



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 eğitimidir.

Ülkemizdeki yer sağlayıcıları, erişim sağlayıcıları ve içerik sağlayıcıları 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 deęil 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. BandwidthD

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

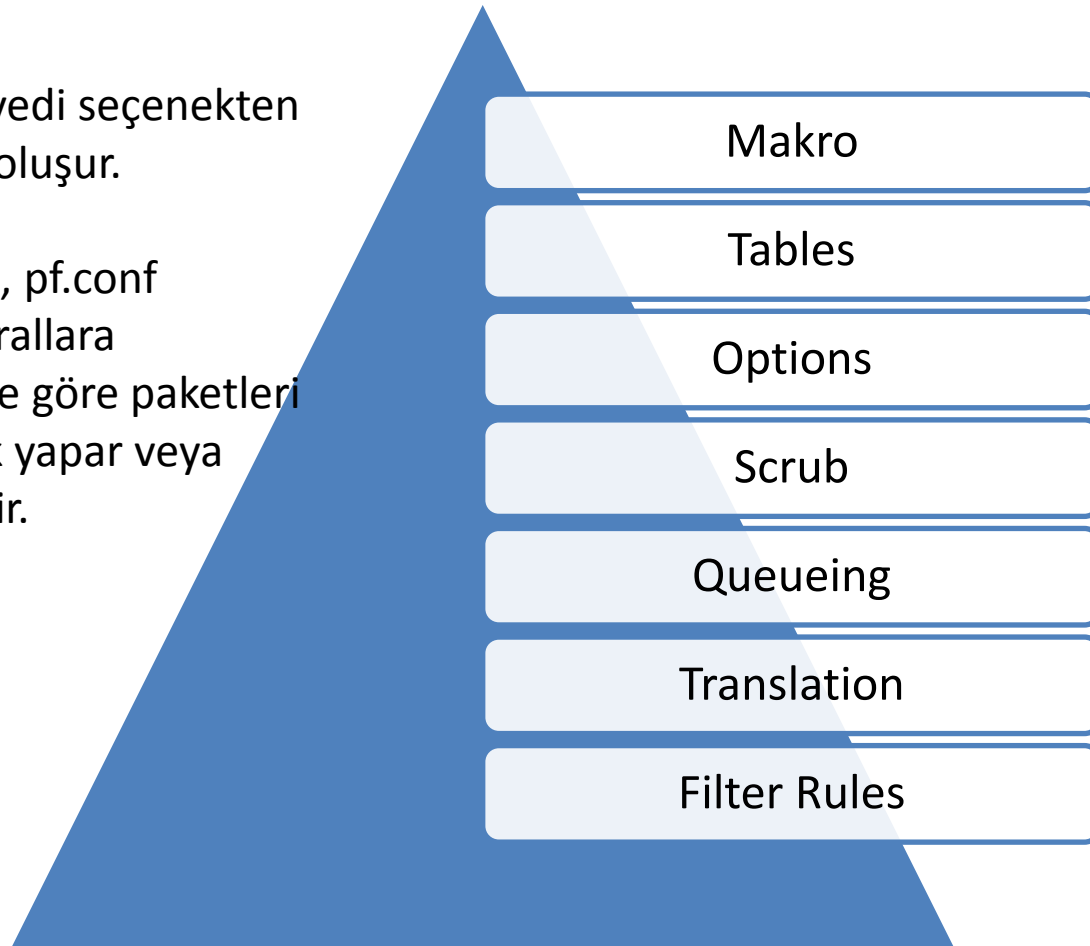
PF Aktif Edilmesi	PF Kontrolü
<ul style="list-style-type: none">▪ OpenBSD için <pre># pf=YES > /etc/rc.conf.local</pre> <ul style="list-style-type: none">▪ FreeBSD için <pre>#kldload pf</pre> <pre>#pf_enable=YES > /etc/rc.conf</pre>	<p>PF Kontrol Edilmesi</p> <ul style="list-style-type: none">▪ pf kaptılması <pre>#pfctl -d</pre> <ul style="list-style-type: none">▪ pf.conf yüklemek <pre>#pfctl -f /etc/pf.conf</pre> <ul style="list-style-type: none">▪ Parse et, fakat yükleme <pre>#pfctl -nf /etc/pf.conf</pre> <ul style="list-style-type: none">▪ Sadece NAT kurallarını yükle <pre>#pfctl -Nf /etc/pf.conf</pre> <ul style="list-style-type: none">▪ Geçerli Filtreleme kurallarını listele <pre>#pfctl -sr</pre> <ul style="list-style-type: none">▪ Durum tablosunu listele <pre>#pfctl -ss</pre> <p><i>Not:Daha fazla bilgi için pfctl(8) man sayfasına bakınız.</i></p>

Bölüm 3:

pf.conf dosyası

pf.conf dosyası yedi seçenekten ve sıralamadan oluşur.

packet filter (pf), pf.conf dosyasındaki kurallara veya seçeneklere göre paketleri dururur, değişiklik 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:

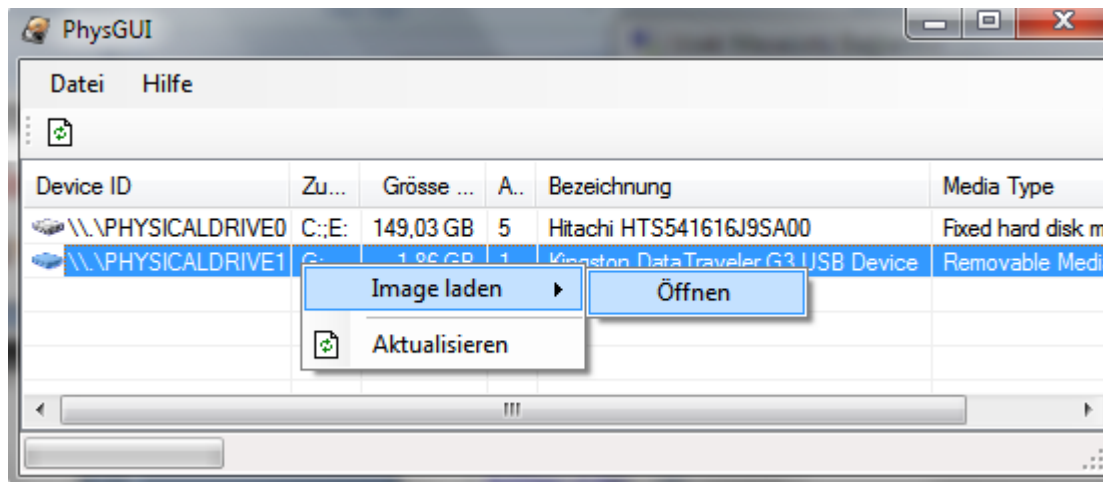
Embedded Kurulum

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.

```
Trying to mount root from ufs:/dev/ad1s1a
Trying to mount root from ufs:/dev/ad1s1a
Trying to mount root from ufs:/dev/ad1s1a

Manual root filesystem specification:
  <fstype>:<device>  Mount <device> using filesystem <fstype>
                    eg. ufs:da0s1a
  ?                  List valid disk boot devices
  <empty line>       Abort manual input

mountroot> ?

List of GEOM managed disk devices:
  ufsid/4c67e254a70d9a5b ad0s1c ad0s1b ad0s1a iso9660/pfSense acd0t01 ad0s1 acd0
  ad0 fd0

Manual root filesystem specification:
  <fstype>:<device>  Mount <device> using filesystem <fstype>
                    eg. ufs:da0s1a
  ?                  List valid disk boot devices
  <empty line>       Abort manual input

mountroot> ufs:/dev/ad0s1a
Trying to mount root from ufs:/dev/ad0s1a
```

Bölüm 7:

Kurtarma Operasyonu

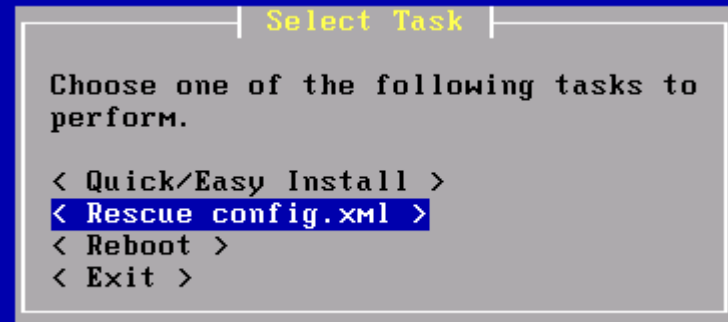
- Config.xml kurtarma operasyonu

```
[ 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)ontinues 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 yüksek ve sade, gelişmiş bir yönetim arabirimi. Servis ve sistem ayarlarını web tabanlı yönetir.

Bölüm 8:

Konfigurasyon | Yönetim Arabirimleri

Konsole Arabirimi	Web Arabirimi
<ul style="list-style-type: none">0) Logout (SSH only)1) Assign Interfaces2) Set LAN IP address3) Reset webConfigurator password4) Reset to factory defaults5) Reboot system6) Halt system7) Ping host8) Shell9) PFtop10) Filter Logs11) Restart webConfigurator12) pfSense Developer Shell13) Upgrade from console14) Disable Secure Shell (sshd)	<ul style="list-style-type: none">SystemInterfacesFirewallServicesVPNStatusDiagnosticsHelp

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	0	6.6.6.106:6806	6.6.6.1:0	0:0	668	9	1308	83712
udp	0	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	0	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	0	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

```
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
5) Reboot system               13) Upgrade
6) Halt system                 14) Enable
7) Ping host
```

Enter an option: 8

```
[2.0-RC3][root@pfsense.fabrikam.com]/root(1): pwd
/root
[2.0-RC3][root@pfsense.fabrikam.com]/root(2): ls
.cshrc                .hushlogin            .profile
.first_time           .login                .shrc
.gitsync_merge.sample .part_mount           .tcshrc
[2.0-RC3][root@pfsense.fabrikam.com]/root(3): uname -a
FreeBSD pfsense.fabrikam.com 8.1-RELEASE-p4 FreeBSD 8.1-RELEASE-p4 #0: Tue Jun 2
1 16:48:23 EDT 2011    sullrich@FreeBSD_8.0_pfsense_2.0-snaps.pfsense.org:/usr/
obj.pfSense/usr/pfSensesrc/src/sys/pfSense_SMP.8  i386
[2.0-RC3][root@pfsense.fabrikam.com]/root(4): mkdir dizin
[2.0-RC3][root@pfsense.fabrikam.com]/root(5):
```



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

Bölüm 8:

Konfigurasyon | Web Arabirimi

Sense ▶ System ▶ Interfaces ▶ Firewall ▶ Services ▶ VPN ▶ Status ▶ Diagnostics ▶ Help **pfsense.fabrikam.com**



Status: Dashboard

System Information

Name	pfsense.fabrikam.com
Version	2.0-RC3 (i386) built on Tue Jun 21 16:50:25 EDT 2011 Update available. Click Here to view update.
Platform	pfSense
CPU Type	Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz
Uptime	00:23
Current date/time	Thu Sep 15 16:11:37 UTC 2011
DNS server(s)	195.175.39.40 195.175.39.39
Last config change	Thu Sep 15 16:11:13 UTC 2011
State table size	27/22000 Show states
MBUF Usage	515 /1290
CPU usage	<div><div></div></div> 1%
Memory usage	<div><div></div></div> 29%
SWAP usage	<div><div></div></div> 0%
Disk usage	<div><div></div></div> 0%






Interfaces

 WAN (DHCP)	↑ 6.6.6.106 1000baseT <full-duplex>
 LAN	↑ 192.168.1.1 1000baseT <full-duplex>

Gateways

Name	Gateway	RTT	Loss	Status
WAN	6.6.6.1	0.963ms	0.0%	Online

Firewall Logs

Act	IF	Source	Destination	Prot
	WAN	6.6.6.66:138	6.6.6.255:138	UDP
	WAN	6.6.6.66:138	6.6.6.255:138	UDP
	WAN	6.6.6.66:138	6.6.6.255:138	UDP
	WAN	6.6.6.66:138	6.6.6.255:138	UDP
	WAN	6.6.6.66:138	6.6.6.255:138	UDP

Bölüm 8:

Konfigurasyon | Genel Ayarlar

System: General Setup



System

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

Domain
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
<input type="text" value="8.8.8.8"/>	WAN
<input type="text" value="4.2.2.2"/>	WAN
<input type="text"/>	None
<input type="text"/>	None

IP addresses: these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.
In addition, select the gateway for each DNS server. You should have a 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.

Time zone
Select the location closest to you

NTP time server
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 **This will change the look and feel of pfsense.**

Save

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 otomatik olarak ortamdaki bir DHCP sunucudan alınır. DHCP sunucunun hostname adresi ve ailesi olarak 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

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spooF") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and duplex - Show advanced option

Static IP configuration

IP address /

Gateway -or- add a new one.

Add new gateway:

Default gateway: ☒

Gateway Name:

Gateway IP:

Description:

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

Ağ Geçidi

Bölüm 9:

Ağ Ayarları | WAN | DHCP

General configuration

☒ **Enable Interface**

Description

Enter a description (name) for the interface here.

Type

DHCP

MAC address

This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU

If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS

If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

- Show advanced option

DHCP client configuration

Hostname

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease (for client identification).

Alias IP address

The value in this field is used as a fixed alias IP address by the DHCP client.

DHCP sunucudan ikinci ip adresi istenebilir.

Opsiyonel olarak, DHCP sunucunun hostname adresi

Bölüm 9:

Ağ Ayarları | WAN | DHCP Kirası

Status > Interfaces






WAN interface (em1)	
Status	up
DHCP	up <button>Release</button>
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

PPPoE configuration

Username	 ozanucar@ttnet
Password	
Service name	 ttnet Hint: this field can usually be left empty
Dial on demand	<input type="checkbox"/> Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing you to have a <i>virtual full time</i> connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
Idle timeout	 seconds If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
Periodic reset	Disabled  Select a reset timing type

PPoE erişim
sağlayıcısı bilgileri

Bölüm 9:

Ağ Ayarları | WAN | PPP

PPP configuration

Service Provider	Country: <input type="text" value="Turkey"/>
	Provider: <input type="text" value="Turkcell"/>
	Plan: <input type="text" value="Turkcell - internet"/>
Select to fill in data for your service provider.	

PPP 3G Bağlantı Ayarları

Username	<input type="text" value="gprs"/>
Password	<input type="password" value="...."/>
Phone Number	<input type="text" value="*99#"/>
Access Point Name (APN)	<input type="text" value="mgb"/>
Modem Port	<input type="text" value="/dev/cuau0"/>
Advanced PPP	Click here to create a PPP configuration.

Bölüm 9:

Ağ Ayarları | Arabirim Ekleme

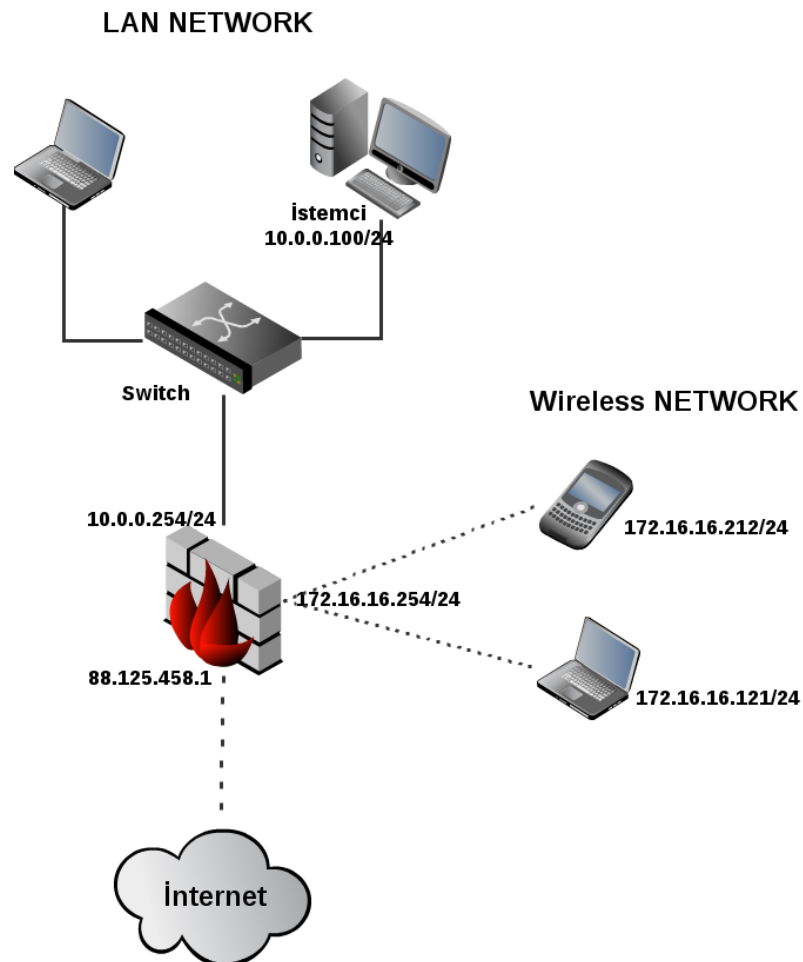
- Interfaces > Assign sekmesinden yeni ağ arabirimi eklenebilir ve kaldırılabilir.

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

Interface	Network port
WAN	em1 (00:0c:29:f7:69:8b) ▼
LAN	em0 (00:0c:29:f7:69:81) ▼
OPT1	em2 (00:0c:29:f7:69:95) ▼
OPT2	em3 (00:0c:29:f7:69:9f) ▼ em0 (00:0c:29:f7:69:81) em1 (00:0c:29:f7:69:8b) em2 (00:0c:29:f7:69:95) em3 (00:0c:29:f7:69:9f)

butonuna tıklayarak yeni ağ arabirim eklenir. Interface > OP1 ile yeni arabirim yapılandırılır.




Bölüm 10: Wireless



Bölüm 10:

Wireless | Arabirim Ayarları

Access Point Olarak Yapılandırmak

Network-specific wireless configuration	
Mode	Access Point 
SSID	 localhost
Minimum wireless standard	Any  <small>When operating as an access point, allow only stations capable of the selected wireless standard to associate (stations not capable are not permitted to associate).</small>
Allow intra-BSS communication	<input type="checkbox"/> <small>When operating as an access point, enable this if you want to pass packets between wireless clients directly. Disabling the internal bridging is useful when traffic is to be processed with packet filtering.</small>
Enable WME	<input type="checkbox"/> <small>Setting this option will force the card to use WME (wireless QoS).</small>
Enable Hide SSID	<input type="checkbox"/> <small>Setting this option will force the card to NOT broadcast its SSID (this might create problems for some clients).</small>

Yayın yapacağı isim

Gizli SSID ile yayın yapılabilir

Bölüm 10:

Wireless | Arabirim Ayarları




Şifreleme Türleri

WEP	<input type="checkbox"/> Enable WEP	TX key
Key 1:	<input type="text"/>	<input type="radio"/>
Key 2:	<input type="text"/>	<input type="radio"/>
Key 3:	<input type="text"/>	<input type="radio"/>
Key 4:	<input type="text"/>	<input type="radio"/>
<p>40 (64) bit keys may be entered as 5 ASCII characters or 10 hex digits preceded by '0x'. 104 (128) bit keys may be entered as 13 ASCII characters or 26 hex digits preceded by '0x'.</p>		
WPA	<input checked="" type="checkbox"/> Enable WPA	
WPA Pre Shared Key		
PSK:	<input type="text" value="gizliparolam"/>	
Passphrase must be from 8 to 63 characters.		
WPA Mode	<input type="text" value="WPA"/>	
WPA Key Management Mode	<input type="text" value="Pre Shared Key"/>	
Authentication	<input type="text" value="Open System Authentication"/>	
Note: Shared Key Authentication requires WEP.		
WPA Pairwise	<input type="text" value="Both"/>	
Key Rotation	<input type="text" value="60"/>	
Allowed values are 1-9999 but should not be longer than Master Key Regeneration time.		
Master Key Regeneration	<input type="text" value="3600"/>	
Allowed values are 1-9999 but should not be shorter than Key Rotation time.		

Bölüm 10:

Wireless | Arabirim Ayarları

802.1x

Enable IEEE802.1X Authentication	<input type="checkbox"/> Setting this option will enable 802.1x authentication. NOTE: this option requires checking the "Enable WPA box".
802.1X Authentication Server IP Address	 <input type="text"/> Enter the IP address of the 802.1X Authentication Server. This is commonly a Radius server (FreeRadius, Internet Authentication Services, etc.)
802.1X Authentication Server Port	 <input type="text"/> Leave blank for the default 1812 port.
802.1X Authentication Server Shared Secret	 <input type="text"/>
802.1X Authentication Roaming Preauth	<input type="checkbox"/>

Bölüm 10:

Wireless | Arabirim Ayarları

Wireless ağ arabirimi için DHCPD

Services: DHCP server

S L ?

LAN **WIRELESS**

☒ **Enable DHCP server on WIRELESS interface**

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

Subnet	5.5.5.0
Subnet mask	255.255.255.0
Available range	5.5.5.1 - 5.5.5.254
Range	<input type="text" value="5.5.5.55"/> to <input type="text" value="5.5.5.100"/>

Status: DHCP leases

?

IP address	MAC address	Hostname	Start	End	Online	Lease Type
5.5.5.55	48:5d:60:81:9f:7b	localhost	2000/01/02 03:34:08	2000/01/02 05:34:08	online	active

Show all configured leases

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

LAN DMZ

Birden fazla ağ arabirimini destekler

☒ 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 192.168.1.0

Subnet mask 255.255.255.0

Available range 192.168.1.1 - 192.168.1.254

Range to

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
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
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.

Dağıtılacak IP aralığı

Bölüm 11:

Services | DHCP Server

Cluster yapısı için kullanılır.

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.

Dynamic DNS - Show Dynamic DNS

NTP servers - Show NTP configuration

TFTP server - Show TFTP configuration

LDAP URI - Show LDAP configuration

Enable network booting - Show Network booting

Additional BOOTP/DHCP Options - 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.

Statik dhcp kiralari

MAC address	IP address	Hostname	Description
00:1f:d0:8d:86:db	192.168.1.11	muhasabe	muhasabe bilgisayari

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

Status: DHCP leases



Sep 16 11:59:
Sep 16 11:59:
Sep 16 11:59:
Sep 16 11:59:
Sep 16 11:59:

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	muhassebe	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 process 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 iletilir. Router'lar DHCP isteklerini geçirmezler. DHCP isteklerini wan ağından, lan ağına aktarması (relay) için DHCP Relay servisi kullanılır.

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

DHCP Relay configuration

Enable ☒ **Enable DHCP relay on interface**

Interface(s)

WAN
LAN
DMZ

Interfaces without an ip address will not be shown.

☐ **Append circuit ID and agent ID to requests**
If this is checked, the DHCP relay will append the circuit ID (pfsense interface number) and the agent ID to the DHCP request.

Destination server

✎

 1.1.1.1

This is the IP address of the server to which the DHCP packet is relayed. You can enter multiple ip address server entries separated by commas. Select "Proxy requests to DHCP server on WAN subnet" to relay DHCP packets to the server that was used on the WAN interface.

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

☒ Enable DNS forwarder

☒ 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.

☒ 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.

Save

Note:

If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in **System: General setup** or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on specify at least one DNS server on the **System: General setup** page.

You may enter records that override the results from the forwarders below.

Host	Domain	IP	Description
qmail	fabrikam.com	172.16.16.100	Qmail Server

Below you can override an entire domain by specifying an authoritative DNS server to be queried for that domain.

Domain	IP	Description
fabrikam.com	172.16.16.16	fabrikam.com dns server






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

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

Bölüm 11:

Services | Dynamic DNS

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

Dynamic DNS client	
Disable	<input type="checkbox"/>
Service type	DynDNS (dynamic) ▼
Interface to monitor	WAN ▼
Hostname	 pfSense.dyndns.net 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	<input checked="" type="checkbox"/> Enable Wildcard
Username	 pfSense Username is required for all types except Namecheap and FreeDNS.
Password	 FreeDNS (freedns.afraid.org): Enter your "Authentication Token" provided by FreeDNS.
Description	 fabrikam.com pfSense Firewall

Note:

You must configure a DNS server in System: General setup or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work.

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

Services: SNMP

SNMP Daemon <input checked="" type="checkbox"/> Enable	
Polling Port	<input type="text" value="161"/> Enter the port to accept polling events on (default 161)
System location	<input type="text" value="tr"/>
System contact	<input type="text" value="mail@ozanucar.com"/>
Read Community String	<input type="text" value="public"/> In most cases, "public" is used here

SNMP Traps <input type="checkbox"/> Enable	
Trap server	<input type="text"/> Enter trap server name
Trap server port	<input type="text" value="162"/> Enter the port to send the traps to (default 162)
Enter the SNMP trap string	<input type="text"/> Trap string

Modules	
SNMP Modules	<input checked="" type="checkbox"/> MibII <input checked="" type="checkbox"/> Netgraph <input checked="" type="checkbox"/> PF <input checked="" type="checkbox"/> Host Resources
<input type="checkbox"/> Bind to LAN interface only This option can be useful when trying to access the SNMP agent by the LAN interface's IP address through a VPN tunnel terminated on the WAN interface.	
<input type="button" value="Save"/>	

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

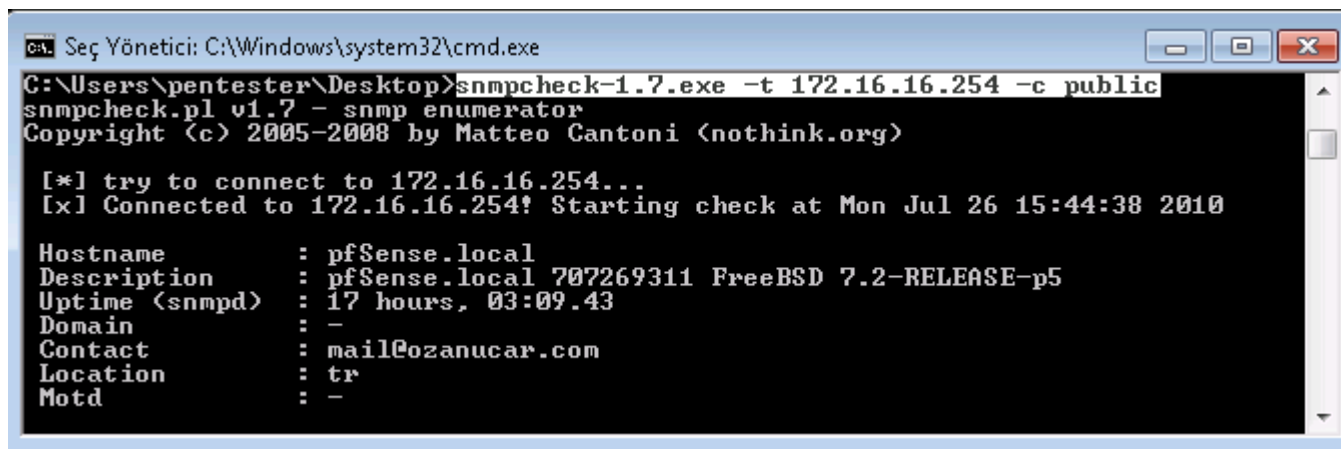
Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
Aventail	HTTPS	OK	03-01-2010 10:01:58	0d 15h 44m 2s	1/3	HTTP OK: HTTP/1.1 302 Found - 717 bytes in 0.455 second response time
SNWL-LASSO	HTTP URL	OK	03-01-2010 10:09:07	1d 3h 36m 53s	1/3	HTTP OK: HTTP/1.1 200 OK - 3267 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



```
Seç Yönetici: C:\Windows\system32\cmd.exe
C:\Users\pentester\Desktop>snmpcheck-1.7.exe -t 172.16.16.254 -c public
snmpcheck.pl v1.7 - snmp enumerator
Copyright (c) 2005-2008 by Matteo Cantoni (nothink.org)

[*] try to connect to 172.16.16.254...
[x] Connected to 172.16.16.254! Starting check at Mon Jul 26 15:44:38 2010

Hostname      : pfSense.local
Description   : pfSense.local 707269311 FreeBSD 7.2-RELEASE-p5
Uptime (snmpd): 17 hours, 03:09.43
Domain        : -
Contact       : mail@ozanucar.com
Location      : tr
Motd          : -
```

Bölüm 11:

Services | OpenNTPD

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

ntp.nasa.gov misali ...

NTP server

Enable	<input checked="" type="checkbox"/> Check this to enable the NTP server.
Interface	<div><div>LAN</div><div>WAN</div></div> Select the interface(s) the NTP server will listen on.
<div>Save</div>	

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.


Wake on LAN

Interface

WAN

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

MAC address

 00:1f:d0:8d:86:db

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	00:1f:d0:8d:86:db	muhassebe	

Note:

This service can be used to wake up (power on) computers by sending special "Magic Packets". The NIC in the computer that is to be woken up must support Wake on LAN and has to be configured properly (WOL cable, BIOS settings).

Bölüm 11:

Services | OLSRD

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

OLSRD Settings

Enable OLSR	<input checked="" type="checkbox"/>	Enables the dynamic mesh linking daemon
Link Quality Level	2	
Interfaces	<div>WAN LAN SYNC loopback</div>	Select the interfaces that OLSR will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.
Enable HTTPInfo Plugin	<input checked="" type="checkbox"/>	Enables the OLSR stats web server
HTTPInfo Port	1989	Port that HTTPInfo will listen on
Allowed host(s)	10.0.0.10	Hosts that are allowed to access the HTTPInfo web service.
Allowed host(s) subnet	255.255.255.0	Enter the subnet mask in form 255.255.255.0

Bölüm 11:

Services | OLSRD

← → X 10.0.0.1:1989 ☆

olsr.org OLSR daemon



Configuration Routes Links/Topology All About

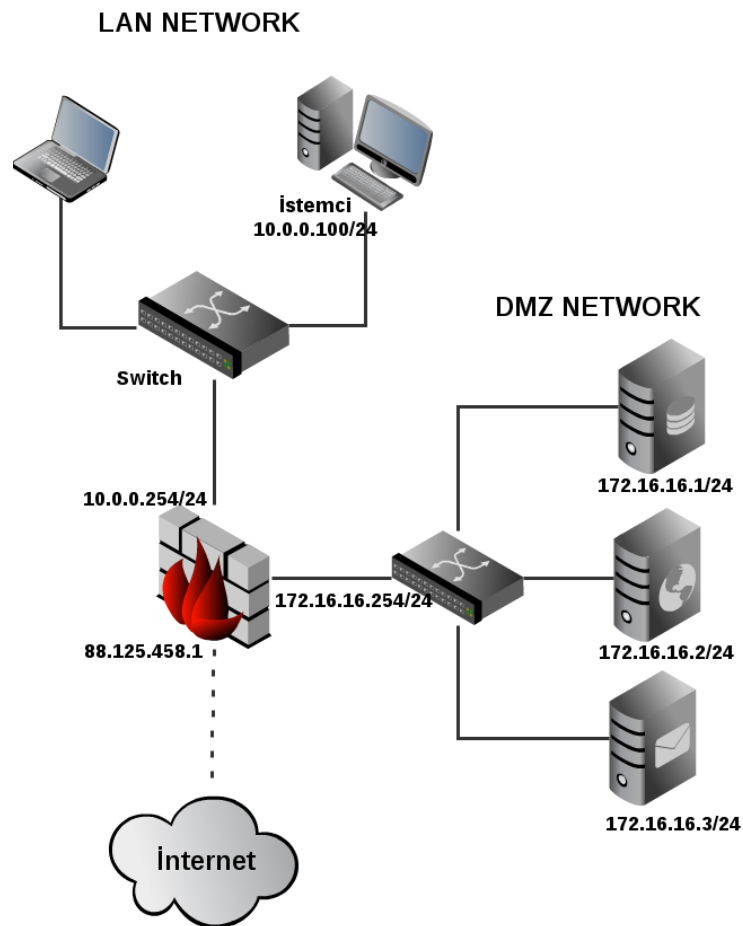
Version: olsr.org - 0.5.6-r7 (built on 2011-08-11 13:58:32 on FreeBSD_8.0_pfSense_2.0-snaps.pfsense.org)
OS: FreeBSD
System time: Wed, 05 Oct 2011 08:40:39
Olsrd uptime: 00 hours 01 minutes 54 seconds
HTTP stats(ok/dyn/error/illegal): 26/0/1/0
Click [here](#) to generate a configuration file for this node.

Variables				
Main address: 10.0.0.1	IP version: 4	Debug level: 2	FIB Metrics: flat	
Pollrate: 0.05	TC redundancy: 2	MPR coverage: 3	NAT threshold: 1.000000	
Fisheye: Disabled	TOS: 0x0010	RtTable: 0x00fe/254	RtTableDefault: 0x0000/0	Willingness: 3
LQ extension: Enabled	LQ level: 2	LQ aging: 0.100000		

Interfaces		
em0		
IP: 10.0.0.1	MASK: 255.255.255.0	BCAST: 10.0.0.255
MTU: 1472	WLAN: No	STATUS: UP

Olsrd is configured to run even if no interfaces are available

Bölüm 12: Firewall



Bölüm 12:

Firewall | Rules I

Edit Firewall rule	
Action	<div>Pass ▾</div> <p>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.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any ▾</div></p> <p>Address: <div></div> / <div>31 ▾</div></p>
Source port range	<div>from: <div>(other) ▾</div> <div></div></div> <div>to: <div>(other) ▾</div> <div></div></div> <p>Specify the source port or port range for this rule. This is usually <i>random</i> and almost never equal to the destination port range (and should usually be "any"). Hint: you can leave the <i>to</i> field empty if you only want to filter a single port.</p>

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 uygulanacağı 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

Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text"/> / <input type="text" value="31"/>
Destination port range	from: <input type="text" value="(other)"/> <input type="text" value=""/> to: <input type="text" value="(other)"/> <input type="text" value=""/> 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	<input type="checkbox"/> 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	<input type="text"/> You may enter a description here for your reference.

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	<input type="button" value="Advanced"/> - Show advanced option
Diffserv Code Point	<input type="button" value="Advanced"/> - Show advanced option
Advanced Options	<input type="button" value="Advanced"/> - Show advanced option
TCP flags	<input type="button" value="Advanced"/> - Show advanced option
State Type	<input type="button" value="Advanced"/> - Show advanced option
No XMLRPC Sync	<input type="button" value="Advanced"/> - Show advanced option
Schedule	<input type="button" value="Advanced"/> - Show advanced option
Gateway	<input type="button" value="Advanced"/> - Show advanced option
In/Out	<input type="button" value="Advanced"/> - Show advanced option
Ackqueue/Queue	<input type="button" value="Advanced"/> - Show advanced option
Layer7	<input type="button" value="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 bağlantı sınırı
- 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.

Firewall: Aliases: Edit

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

Bölüm 12:

Firewall | Alias | Host

Firewall: Aliases: Edit



Alias Edit							
Name	<div> muhasebe</div> <p>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</p>						
Description	<div> Muhasebe ve Finans</div> <p>You may enter a description here for your reference (not parsed).</p>						
Type	Host(s)						
Host(s)	<div>Enter as many hosts as you would like. Hosts must be specified by their IP address.</div> <table><thead><tr><th>IP</th><th>Description</th></tr></thead><tbody><tr><td>1.1.1.11 </td><td><div> Muhasebe Ayse Hanım</div></td></tr><tr><td>1.1.1.12 </td><td><div> Finans Mehmet Bey</div></td></tr></tbody></table>	IP	Description	1.1.1.11	<div> Muhasebe Ayse Hanım</div>	1.1.1.12	<div> Finans Mehmet Bey</div>
IP	Description						
1.1.1.11	<div> Muhasebe Ayse Hanım</div>						
1.1.1.12	<div> Finans Mehmet Bey</div>						

Bölüm 12:

Firewall | Alias | Network

Firewall: Aliases: Edit



Alias Edit										
Name	<div> ARGE</div> <p>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</p>									
Description	<div> ARGE Departmani</div> <p>You may enter a description here for your reference (not parsed).</p>									
Type	Network(s)									
Network(s)	<div><p>Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single host, /24 specifies 255.255.255.0, etc. Hostnames (FQDNs) may also be specified, using a /32 mask. You may also enter an IP range such as 192.168.1.1-192.168.1.254 and a list of CIDR networks will be derived to fill the range.</p><table><thead><tr><th>Network</th><th>CIDR</th><th>Description</th><th></th></tr></thead><tbody><tr><td>172.16.16.0</td><td>24 </td><td><div> ARGE</div></td><td></td></tr></tbody></table><div></div></div>		Network	CIDR	Description		172.16.16.0	24	<div> ARGE</div>	
Network	CIDR	Description								
172.16.16.0	24	<div> ARGE</div>								

Bölüm 12:

Firewall | Alias | Port

Firewall: Aliases: Edit



Alias Edit

Name	<div> izinliportlar</div> <p>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</p>																												
Description	<div> İzinli Port Numaraları</div> <p>You may enter a description here for your reference (not parsed).</p>																												
Type	Port(s)																												
Port(s)	<div>Enter as many ports as you wish. Port ranges can be expressed by seperating with a colon.</div> <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> <div></div>	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																											

Bölüm 12:

Firewall | Alias | Urltable

Firewall: Aliases: Edit



Alias Edit					
Name	<div> turkiye</div> <p>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</p>				
Description	<div> Turkiye IP Araligi</div> <p>You may enter a description here for your reference (not parsed).</p>				
Type	URL Table				
URL	<div><p>Enter a single URL containing a large number of IPs and/or Subnets. After saving pfSense will download the URL and create a table file containing these addresses. This will work with large numbers of addresses (30,000+) or small numbers.</p><table><thead><tr><th>URL</th><th>Update Freq.</th></tr></thead><tbody><tr><td>et/e_country_data/TR_cidr.txt</td><td>7 </td></tr></tbody></table><div></div></div>	URL	Update Freq.	et/e_country_data/TR_cidr.txt	7
URL	Update Freq.				
et/e_country_data/TR_cidr.txt	7				

Bölüm 12:

Firewall | Schedules

Zaman bazlı firewall kuralları yazmayı sağlar.

Firewall: Schedules: Edit



Schedule information

Schedule 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).

Month

October 2011

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
31						

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**

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
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
Mon - Sun	12:59	13:59	

Bölüm 12:

Firewall | Schedules | Uygulama

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

Firewall: Schedules

Name	Time Range(s)	Description
personel	Mon - Sun 0:59-23:59 öğlen saati	personel grubu

Firewall: Rules

FloatingWANLANBURSA

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
	*	personel	*	*	*	*	none	personel	personel grubu

personel grubu

Mon - Sun; 0:59 - 23:59

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'l 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 timeout süresi 6 saniyeye olsun. Spoof edilmiş ip adreslerine karşı Synproxy koruması da aktif olsun.

Firewall: Rules

S L ?

Floating

WAN

LAN

DMZ

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<div><div></div><div></div><div></div></div>	TCP	<u>! turkiye</u>	*	*	*	*	none		ddos saldırıları durumunda

pass

pass (disabled)

block

block (disabled)

reject

reject (disabled)

log

log (disabled)

Bölüm 12:

Firewall | Rules | Uygulama I

Firewall: Rules: Edit

S L ?

Edit Firewall rule

Action	<div>1</div> <div>Block</div> <p>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.</p>								
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>								
Interface	<div>WAN</div> <p>Choose on which interface packets must come in to match this rule.</p>								
Protocol	<div>TCP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>								
Source	<div><input checked="" type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias</div></p> <p>Address: <div>turkiye</div> / <div>31</div></p>								
State Type	<div>2</div> <div>synproxy state</div> <p>Hint: Select which type of state tracking mechanism to use.</p> <table><tr><td>keep state</td><td>Works with all IP protocols</td></tr><tr><td>sloppy state</td><td>Works with all IP protocols</td></tr><tr><td>synproxy state</td><td>Proxies incoming TCP connections. This option includes connection tracking.</td></tr><tr><td>none</td><td>Do not use state mechanism</td></tr></table>	keep state	Works with all IP protocols	sloppy state	Works with all IP protocols	synproxy state	Proxies incoming TCP connections. This option includes connection tracking.	none	Do not use state mechanism
keep state	Works with all IP protocols								
sloppy state	Works with all IP protocols								
synproxy state	Proxies incoming TCP connections. This option includes connection tracking.								
none	Do not use state mechanism								

Advanced Options

☒

This allows packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.

☐

This will disable auto generated reply-to for this rule.

You can mark a packet matching this rule and use this mark to match on other NAT/filter rules. It is called **Policy filtering**

You can match packet on a mark placed before on another rule.

Maximum state entries this rule can create

Maximum number of unique source hosts

Maximum number of established connections per host

Maximum state entries per host

Maximum new connections / per second(s)

6

State Timeout in seconds

3

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

S L ?

Floating WAN LAN DMZ

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
		*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>		TCP/UDP	<u>muhassebe</u>	*	*	<u>izinliportlar</u>	*	none		Muhasebe ve Finans	
<input type="checkbox"/>		*	1.1.1.100	*	<u>ARGE</u>	*	*	none		Accept for ARGE	

pass
 pass (disabled)

block
 block (disabled)

reject
 reject (disabled)

log
 log (disabled)

Bölüm 12:

Firewall | Rules | Uygulama II

Edit Firewall rule	
Action	<div>Pass</div> <p>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.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>TCP/UDP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias</div></p> <p>Address: <div>muhassebe</div> / <div>31</div></p> <p><div>Advanced</div> - Show source port range</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any</div></p> <p>Address: <div></div> / <div>31</div></p>
Destination port range	<p>from: <div>(other)</div> <div>izinliport</div></p> <p>to: <div>(other)</div> <div>izinliport</div></p>

Bölüm 12:







Firewall | Rules | Uygulama IV

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



Firewall: Rules



S L ?



Floating WAN LAN DMZ



	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/> 		TCP/UDP	ARGE	*	*	80 (HTTP)	*	none		ARGE Departmani	 
<input type="checkbox"/> 		TCP/UDP	ARGE	*	*	443 (HTTPS)	*	none		ARGE Departmani	 

ARGE Departmani:
172.16.16.0/24 - ARGE

 pass
 pass (disabled)

 block
 block (disabled)

 reject
 reject (disabled)

 log
 log (disabled)

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.

Firewall: Virtual IP Address: Edit



Edit Virtual IP	
Type	<input checked="" type="radio"/> Proxy ARP <input type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	<input type="text" value="WAN"/>
IP Address(es)	Type: <input type="text" value="Single address"/> Address: <input type="text" value=""/> <input type="text" value="32"/> This is a CIDR block of proxy ARP addresses.
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	<input type="text" value="3"/> Enter the VHID group that the machines will share
Advertising Frequency	Base: <input type="text" value="1"/> Skew: <input type="text" value="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	<input type="text"/> You may enter a description here for your reference (not parsed).

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 incelemeye ve sorun çözmede sıkça ihtiyaç duyulur. Diagnostics | System logs | Firewall sayfasından şu bilgiler edinilebilir;

Status: System logs: Firewall

System	Firewall	DHCP	Portal Auth	IPsec	PPP	VPN	Load Balancer	OpenVPN	OpenNTPD	Settings
Normal View Dynamic View Summary View										
Last 50 firewall log entries. Max(50)										
Act	Time	If	Source	Destination						
	Oct 4 16:46:22	LAN	6.6.6.104	224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s,						
	Oct 4 16:46:22	WAN	10.0.0.1	224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s,						
	Oct 4 16:46:23	LAN	6.6.6.104	224.0.0.18: VRRPv2, Advertisement, vrid 1, prio 0, authtype none, intvl 1s,						
	Oct 4 16:46:23	WAN	10.0.0.1	224.0.0.18: VRRPv2, Advertisement, vrid 2, prio 0, authtype none, intvl 1s,						

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

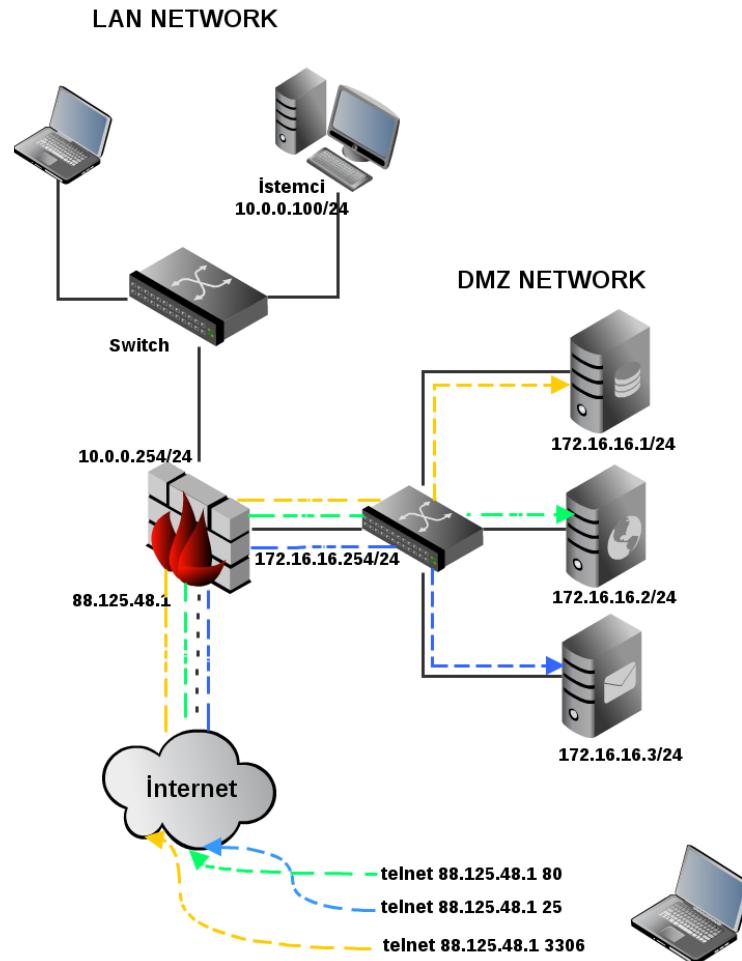
```
# clog /var/log/filter.log  
# clog -f /var/log/filter.log (logları canlı izlemek için)  
# clog /var/log/filter.log | php /usr/local/www/filterparser.php
```

Tcpdump ile izleme

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

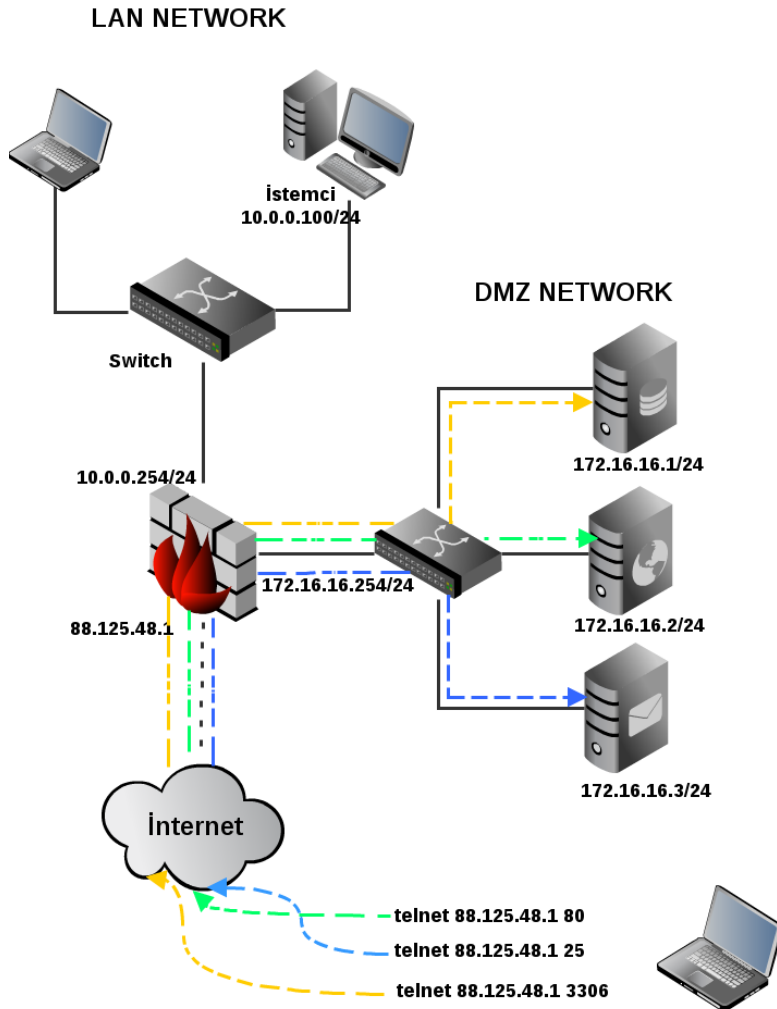

Bölüm 13:

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.

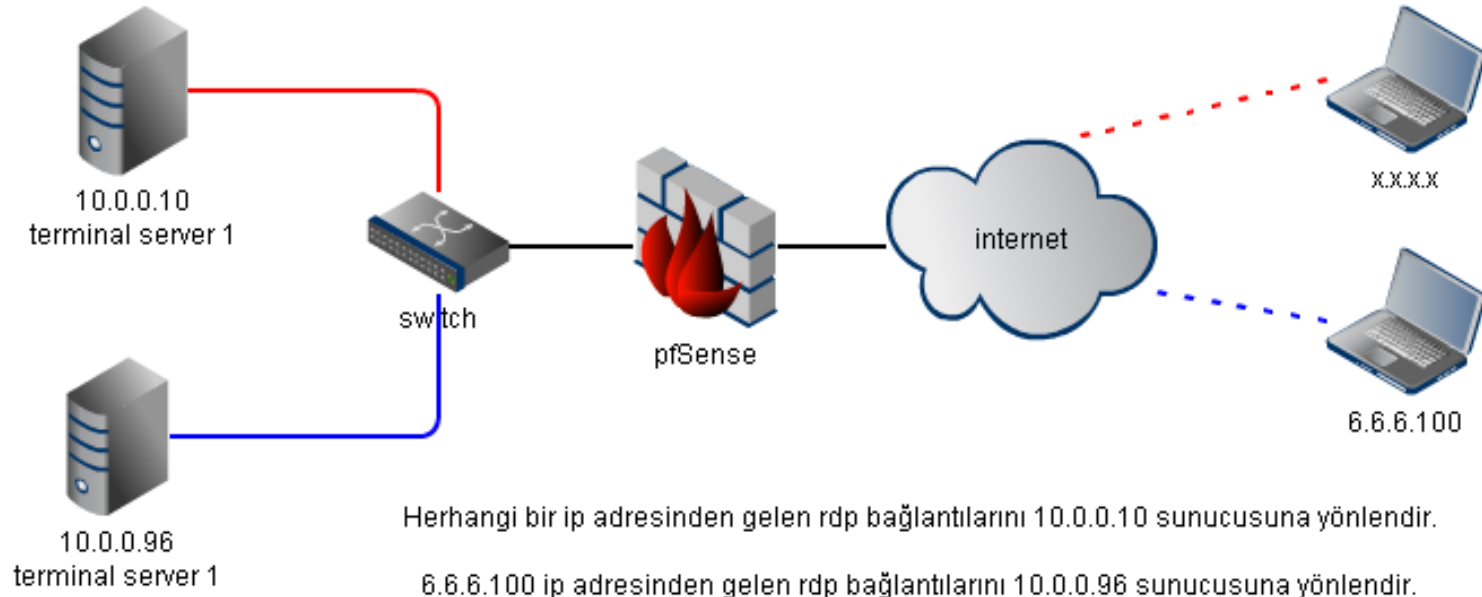
Bölüm 13:

NAT | Port Forwarding

Destination port range	<div>from: <input type="text" value="MS RDP"/></div> <div>to: <input type="text" value="MS RDP"/></div> <p>Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port</p>
Redirect target IP	<div><input type="text" value="10.0.0.10"/></div> <p>Enter the internal IP address of the server on which you want to map the ports. e.g. 192.168.1.12</p>
Redirect target port	<div><input type="text" value="MS RDP"/></div> <p>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above</p>
Description	<div><input type="text" value="rdp"/></div> <p>You may enter a description here for your reference (not parsed).</p>
No XMLRPC Sync	<div><input type="checkbox"/></div> <p>HINT: This prevents the rule from automatically syncing to other CARP members.</p>
NAT reflection	<div><input type="text" value="use system default"/></div>
Filter rule association	<div><input type="text" value="Add associated filter rule"/></div>

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.

Firewall: NAT: Port Forward



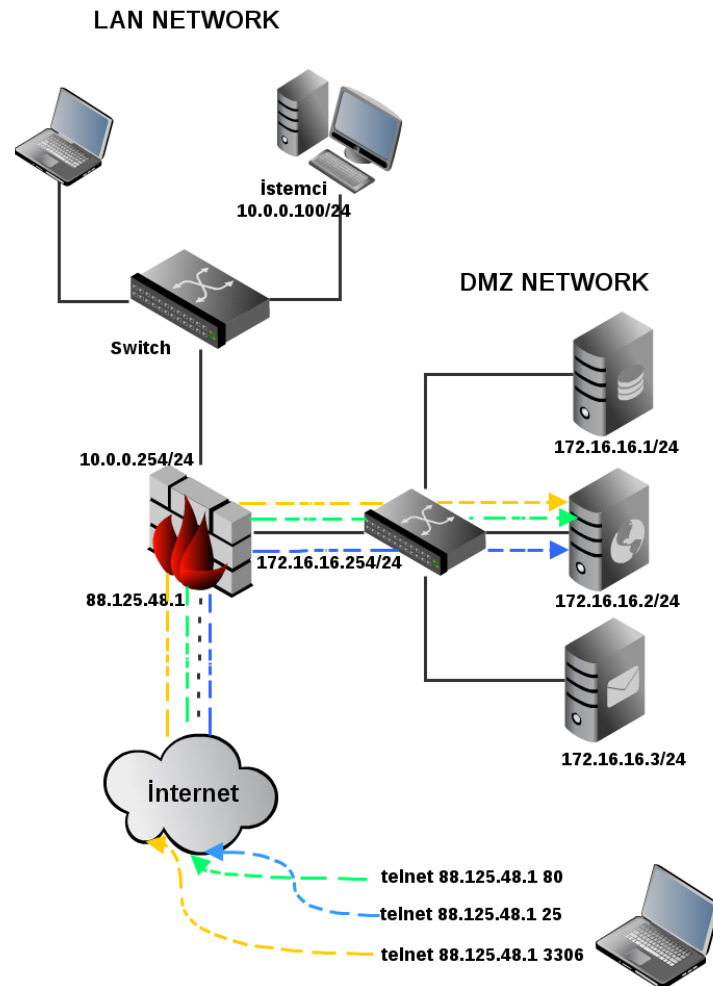
Port Forward 1:1 Outbound

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description	
<input type="checkbox"/>	WAN	TCP	6.6.6.100	*	WAN address	3389 (MS RDP)	10.0.0.96	3389 (MS RDP)	rdp 2	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	3389 (MS RDP)	10.0.0.10	3389 (MS RDP)	rdp	

pass
 linked rule

Bölüm 13:

1:1 NAT



Bölüm 13:

1:1 NAT

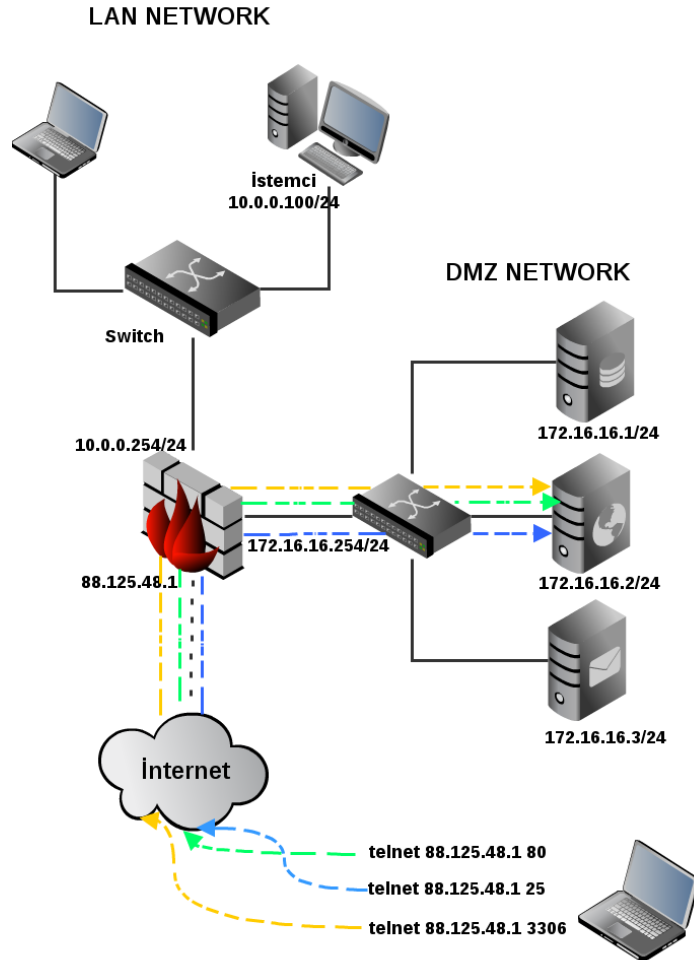
Belirtilen IP adresine gelen bütün trafiği bir hedef ip adresine iletir.

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

Edit NAT 1:1 entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
External subnet IP	<div>6.6.6.106</div> <div>Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address. Hint: this is generally an address owned by the router itself on the selected interface.</div>
Internal IP	<div><input type="checkbox"/> not Use this option to invert the sense of the match.</div> <div>Type: <div>Single host</div></div> <div>Address: <div>10.0.0.96</div> / <div>31</div></div> <div>Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.</div>
Destination	<div><input type="checkbox"/> not Use this option to invert the sense of the match.</div> <div>Type: <div>any</div></div> <div>Address: <div></div> / <div>31</div></div>

Bölüm 13:

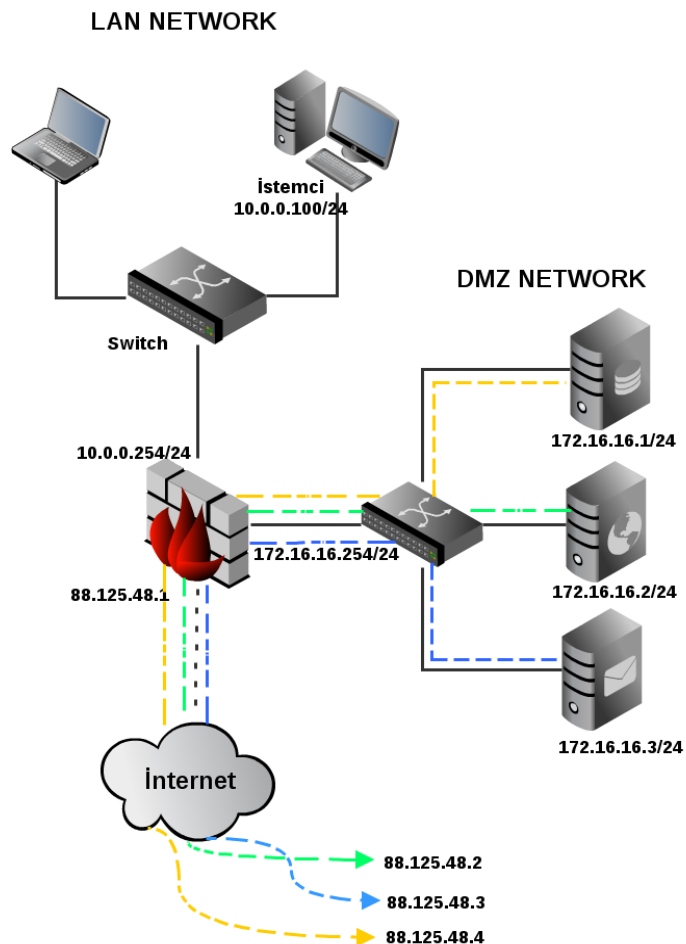
1:1 NAT | Uygulama



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

Bölüm 13:

NAT | Outbound NAT



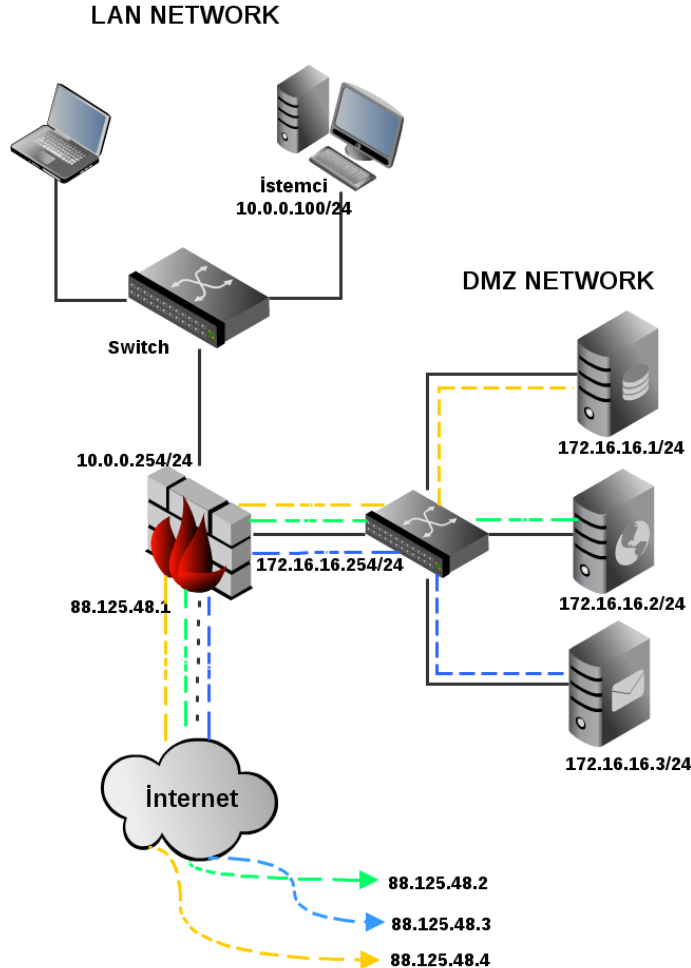
Bölüm 13:

NAT | Outbound NAT

Interface	<div>WAN ▾</div> <p>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</p>
Protocol	<div>any ▾</div> <p>Choose which protocol this rule should match. Hint: in most cases, you should specify <i>any</i> here.</p>
Source	<div>Type: Network ▾</div> <div>Address: 172.16.16.1 / 32 ▾</div> <p>Enter the source network for the outbound NAT mapping.</p> <div>Source port: (leave blank for any)</div>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <div>Type: any ▾</div> <div>Address: / 24 ▾</div> <p>Enter the destination network for the outbound NAT mapping.</p> <div>Destination port: (leave blank for any)</div>
Translation	<div>Address: 88.125.48.2 (http) ▾</div> <p>Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first). Also note that if you are trying to redirect connections on the LAN select the "any" option.</p>

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

Port Forward 1:1 Outbound

Mode: ☐ Automatic outbound NAT rule generation (IPsec passthrough included) ☒ Manual Outbound NAT rule generation (AON - Advanced Outbound NAT) Save

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input type="checkbox"/>	WAN	172.16.16.1/32	*	*	*	88.125.48.2	*	NO	for webserver
<input type="checkbox"/>	WAN	10.0.0.0/24	*	*	*	6.6.6.106	*	NO	Auto created rule for LAN to WAN

172.16.16.1 ip adresi
88.125.48.2 olarak
yönlendirilsin

LAN networkü
6.6.6.106 ip
adresini ile
yönlendirilsin

Bölüm 13:

NAT Reflection

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

Network Address Translation

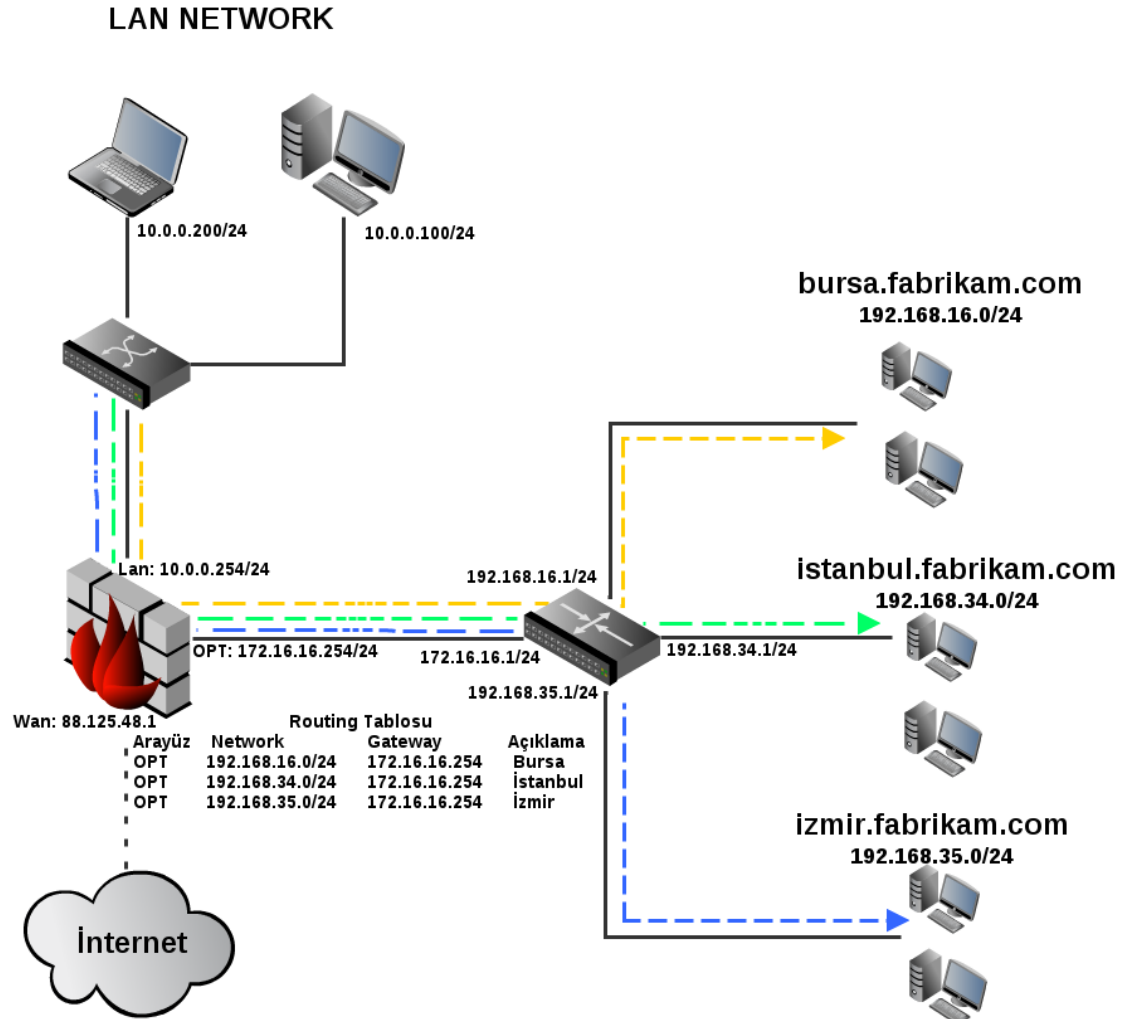
Disable NAT Reflection

☐ Disables the automatic creation of NAT redirect rules for access to your public IP addresses from within your internal networks. Note: Reflection only works on port forward type items and does not work for large ranges > 500 ports.

Save

[http://doc.pfsense.org/index.php/Why_can%27t I access forwarded ports on my WAN IP from my LAN/OPTx networks%3F](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



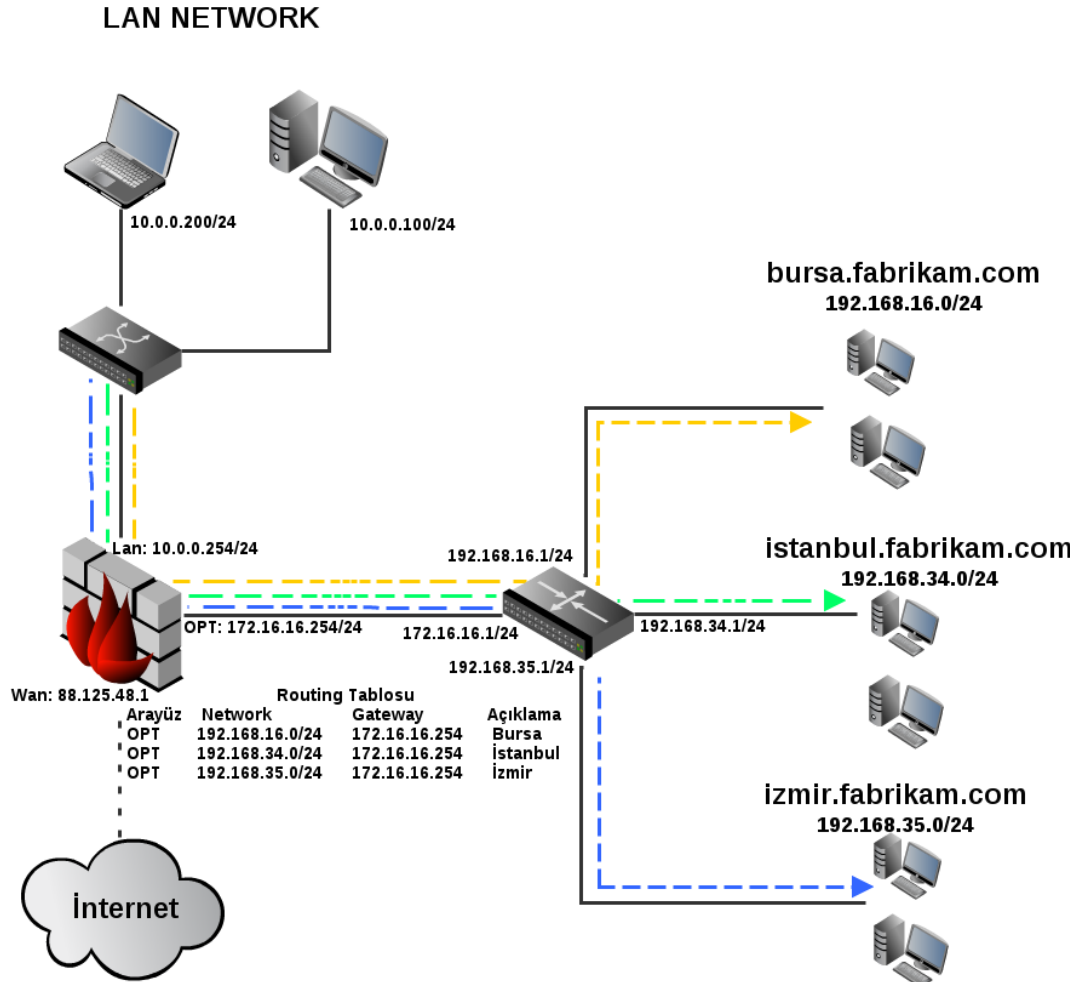
Bölüm 14:

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.

System: Static Routes: Edit route

Edit route entry	
Destination network	<div> 192.168.16.0 / 24 </div> <p>Destination network for this static route</p>
Gateway	<div>bursaGW - 172.16.16.1 </div> <p>Choose which gateway this route applies to or add a new one.</p>
Description	<div> Bu yol bursa'ya gider</div> <p>You may enter a description here for your reference (not parsed).</p>
<div><div>Save</div><div>Cancel</div></div>	

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.

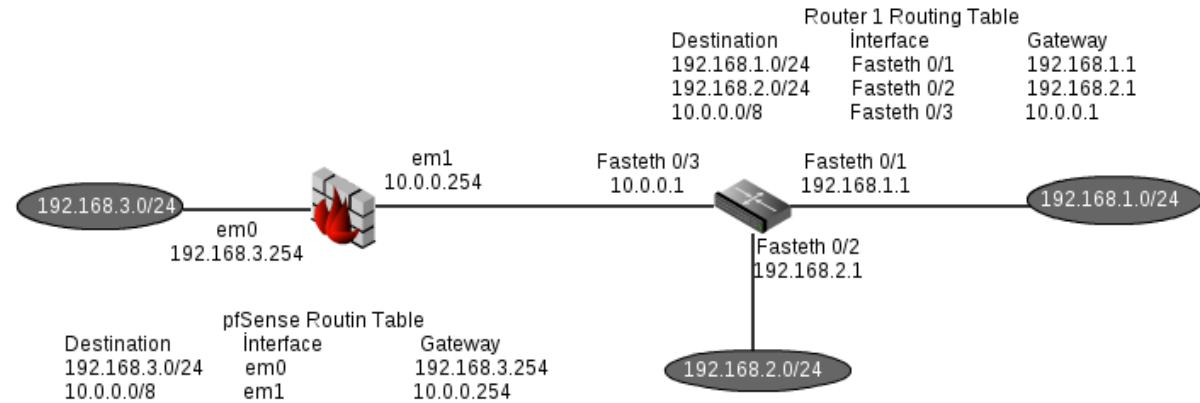
IPv4

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	

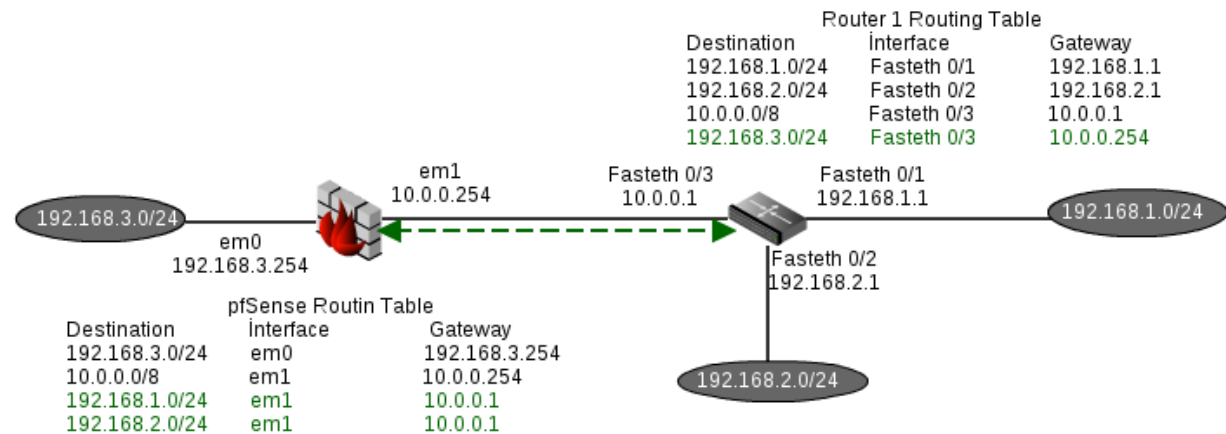
Bölüm 14:

RIP (Router Information Protokol)

RIP Öncesi



RIP Sonrası



Bölüm 14:

RIP (Router Information Protokol)

Services: RIP



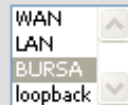
ROUTED Settings

Enable RIP



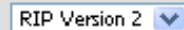
Enables the Routing Information Protocol daemon

Interfaces



Select the interfaces that RIP will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.

RIP Version



Select which RIP version the daemon will listen/advertise using.

RIPv2 password

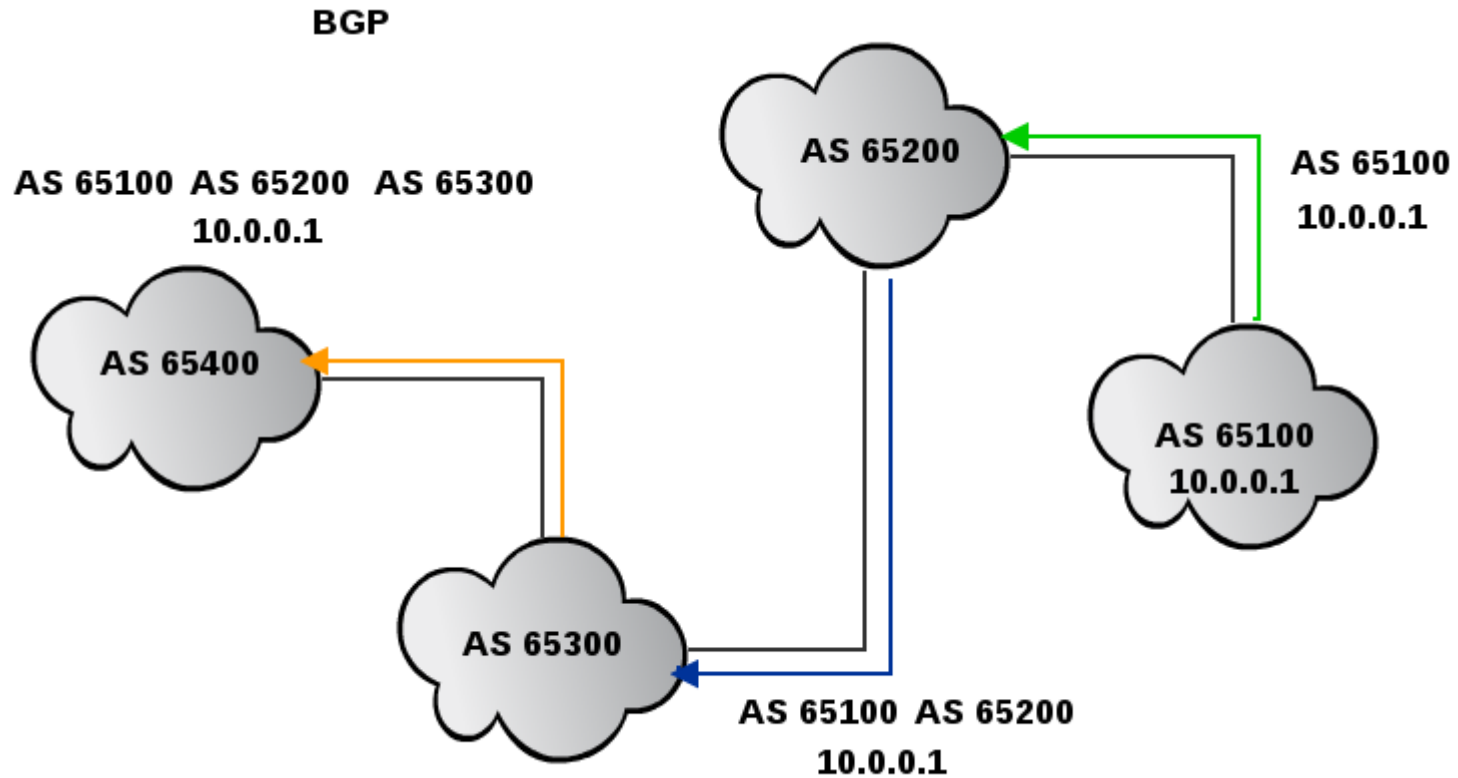


Specify a RIPv2 password. This password will be sent in the clear on all RIPv2 responses received and sent.

Bölüm 14:

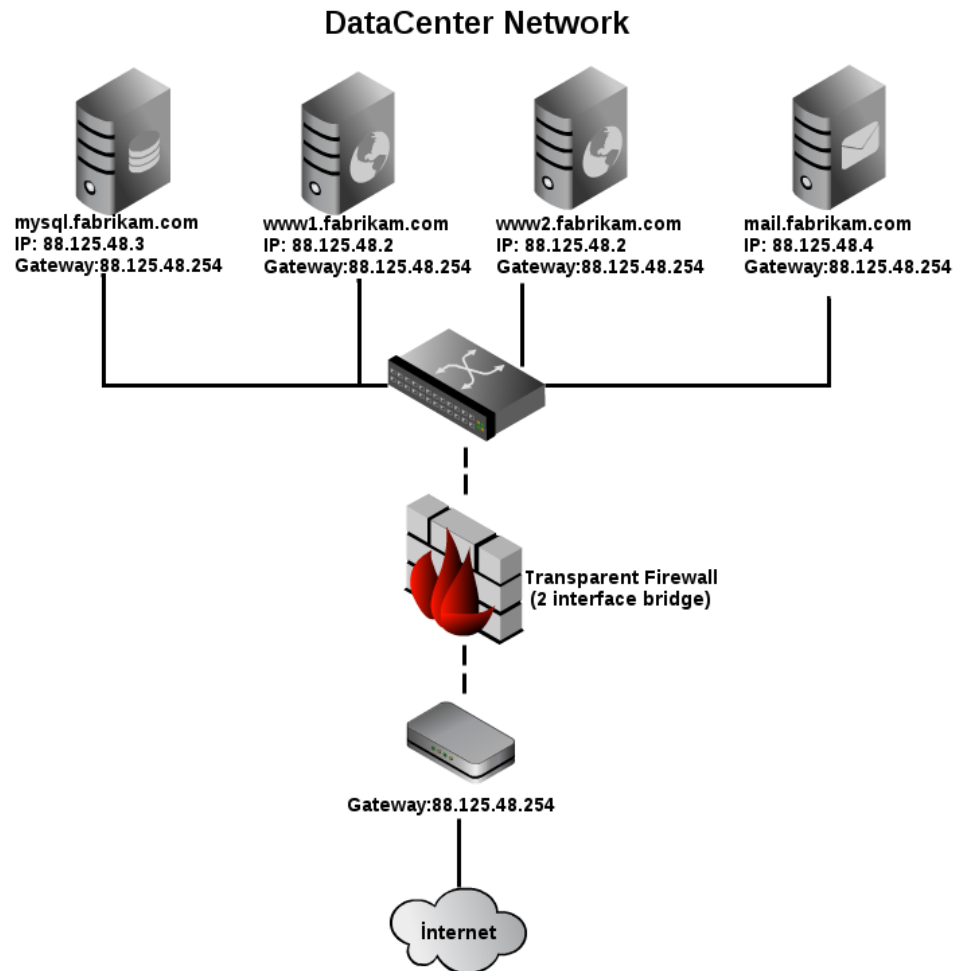
BGP (Border Gateway Protokol)

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.

Interfaces: Bridge: Edit

Bridge configuration

Member interfaces	<div><div>WAN</div><div>LAN</div><div>SYNC</div></div> <div>Interfaces participating in the bridge.</div>
Description	<div><div></div> LAN SYNC Bridge</div>

Show advanced options

Save

Cancel

1.
Adım

OPT2

BRIDGE0 (LAN SYNC Bridge) ▼

em0 (00:0c:29:cf:a1:5d)

em1 (00:0c:29:cf:a1:67)

em2 (00:0c:29:cf:a1:71)

BRIDGE0 (LAN SYNC Bridge)

2.
Adım

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

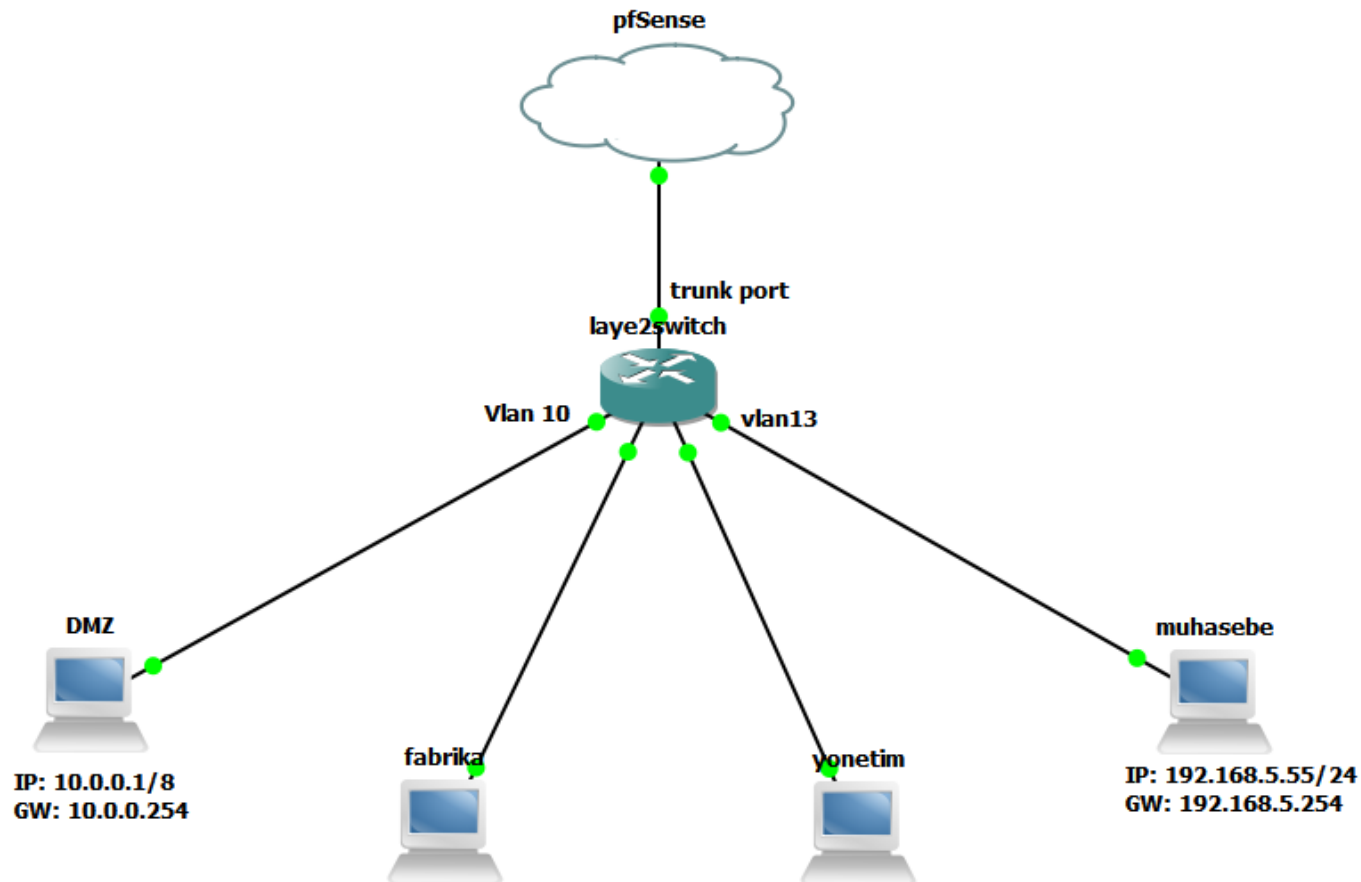
Sanal yerel alan ağı (VLAN), bir yerel alan ağı (LAN) üzerindeki ağ kullanıcılarının ve kaynakların mantıksal olarak gruplandırılması ve switch üzerinde port'lara atanmasıyla yapılır. VLAN kullanılmasıyla her VLAN sadece kendi broadcast'ini alacağından, broadcast trafiği azaltılarak bant genişliği artırılmış olur. VLAN tanımlamaları, bulunan 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

Firewall: VLAN: Edit

Parent interface	<input type="text" value="em0 (00:0c:29:48:45:c9)"/>	<div>Dot1q (802.1q) Vlan Etiketi</div>
	<small>Only VLAN capable interfaces will be shown.</small>	
VLAN tag	<input type="text" value="10"/>	
	<small>802.1Q VLAN tag (between 1 and 4094)</small>	
Description	<input type="text"/>	
	<small>You may enter a description here for your reference (not parsed).</small>	
<div>Save Cancel</div>		

Interfaces: VLAN

Interface assignments		VLANs
Interface	VLAN tag	Description
em0	1	
em0	10	
em0	11	
em0	12	
em0	13	

Bölüm 15:

pfSense Vlan Yapılandırması

Interfaces: Assign

Interface assignments VLANs

Interface	Network port
LAN	em0 (00:0c:29:48:45:c9) ▼
WAN	em1 (00:0c:29:48:45:d3) ▼
Vlan10	VLAN 10 on em0 ▼
Vlan13	VLAN 13 on em0 ▼

Vlan'lar gerçek ağ arabirimleri gibi kullanılabilir.

Vlan arabirimlerinin bilgileri

Vlan10 interface (vlan1)	
Status	up
MAC address	00:0c:29:48:45:c9
IP address	10.0.0.254
Subnet mask	255.0.0.0
Media	1000baseTX <full-duplex>
In/out packets	203/69 (17 KB/11 KB)
In/out errors	0/0
Collisions	0

Vlan13 interface (vlan4)	
Status	up
MAC address	00:0c:29:48:45:c9
IP address	192.168.5.254
Subnet mask	255.255.255.0
Media	1000baseTX <full-duplex>
In/out packets	30/11 (3 KB/849 bytes)
In/out errors	0/0
Collisions	0

Bölüm 15:

pfSense Vlan Firewall Kuralları

Firewall: Rules

LAN

WAN

Vlan10

Vlan13

Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
*	10.0.0.1	*	*	*	*		

</

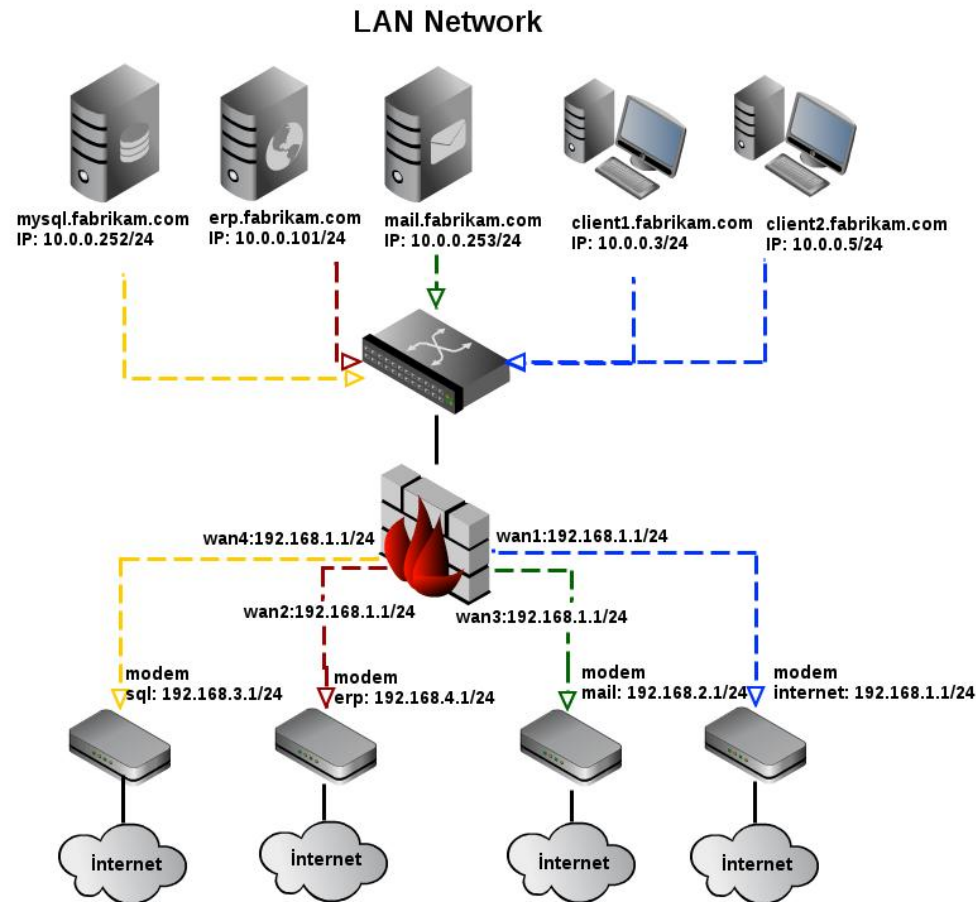
Bölüm 16:

Multiple WAN

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

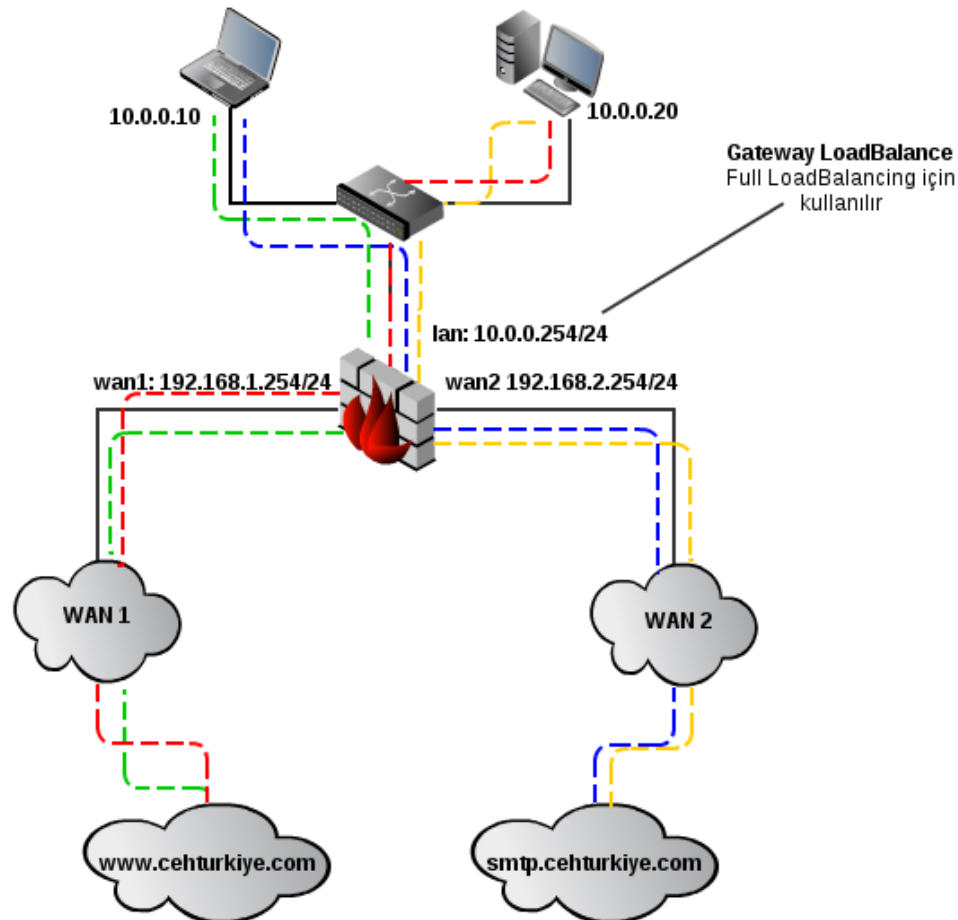
Bölüm 16:

Multiple WAN | Policy Based Routing



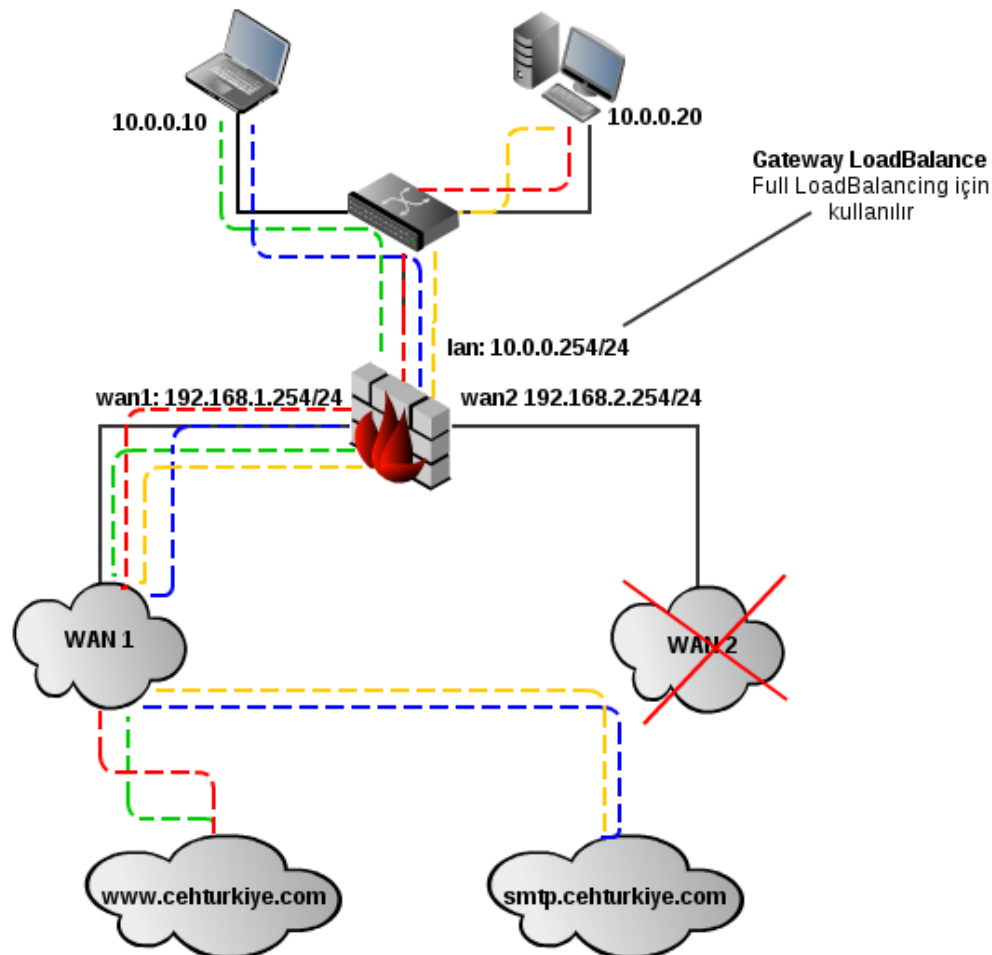
Bölüm 16:

Multiple WAN | Load Balancing



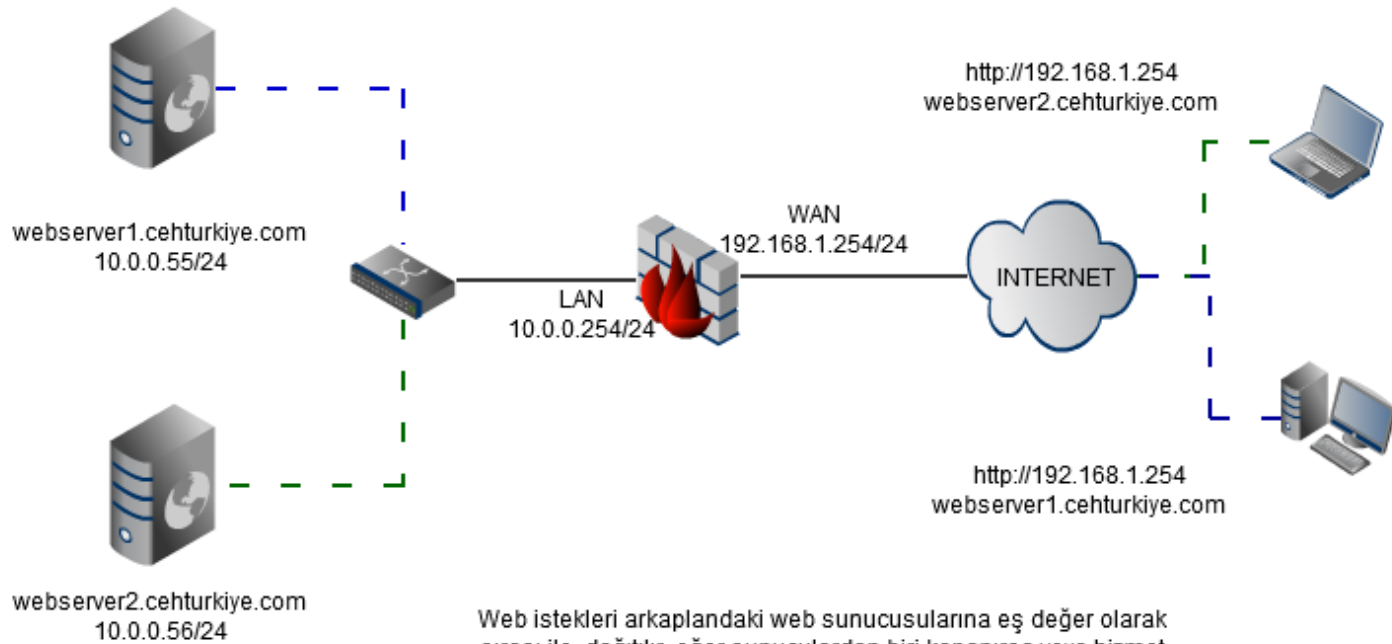
Bölüm 16:

Multiple WAN | Failover



Bölüm 17:

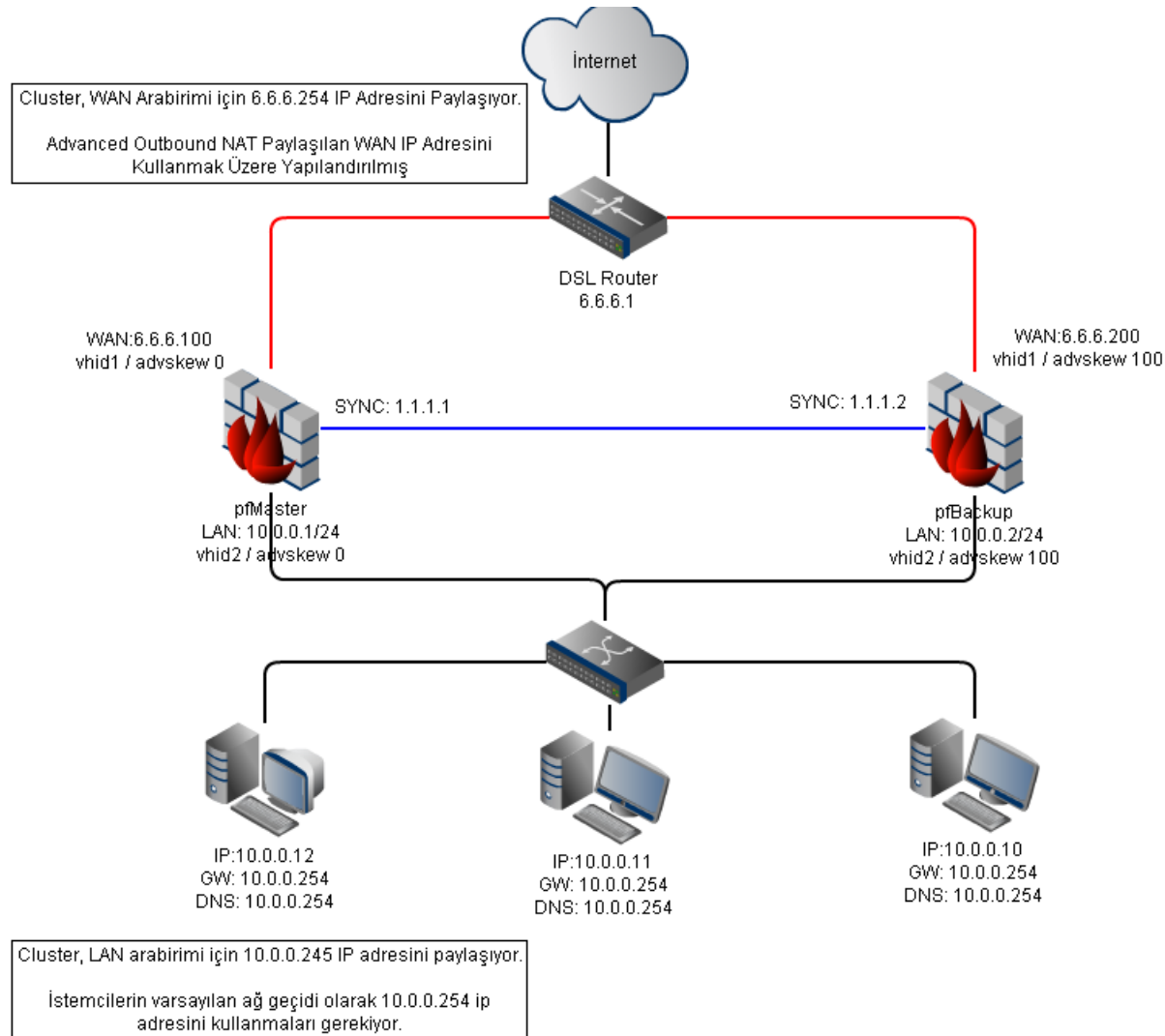
Incoming Server Load Balancing



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

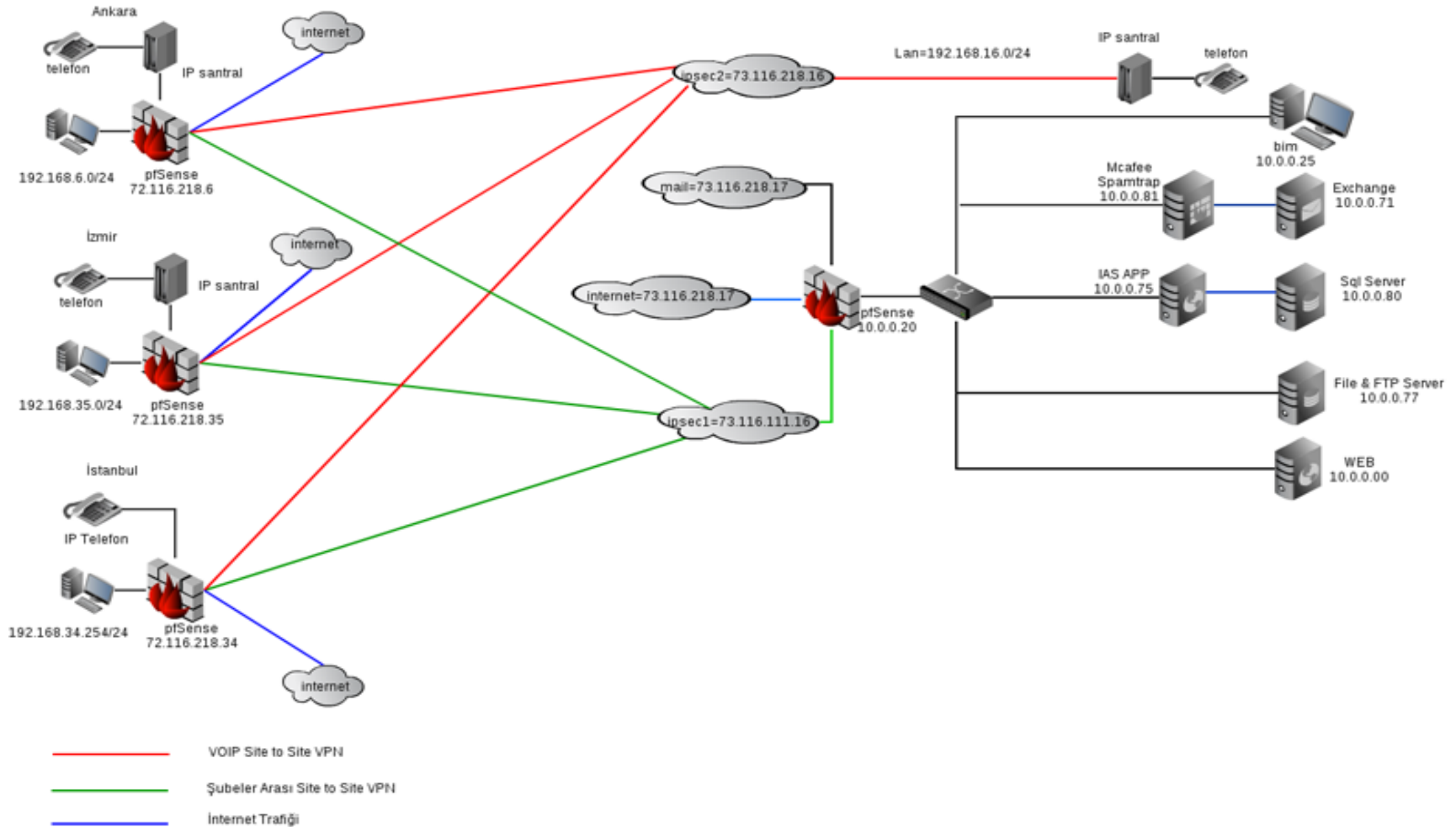
TCP Port 1723
GRE protokolünü kullanır
Radius Auth. Destekler

OpenVPN

TCP Port 1194

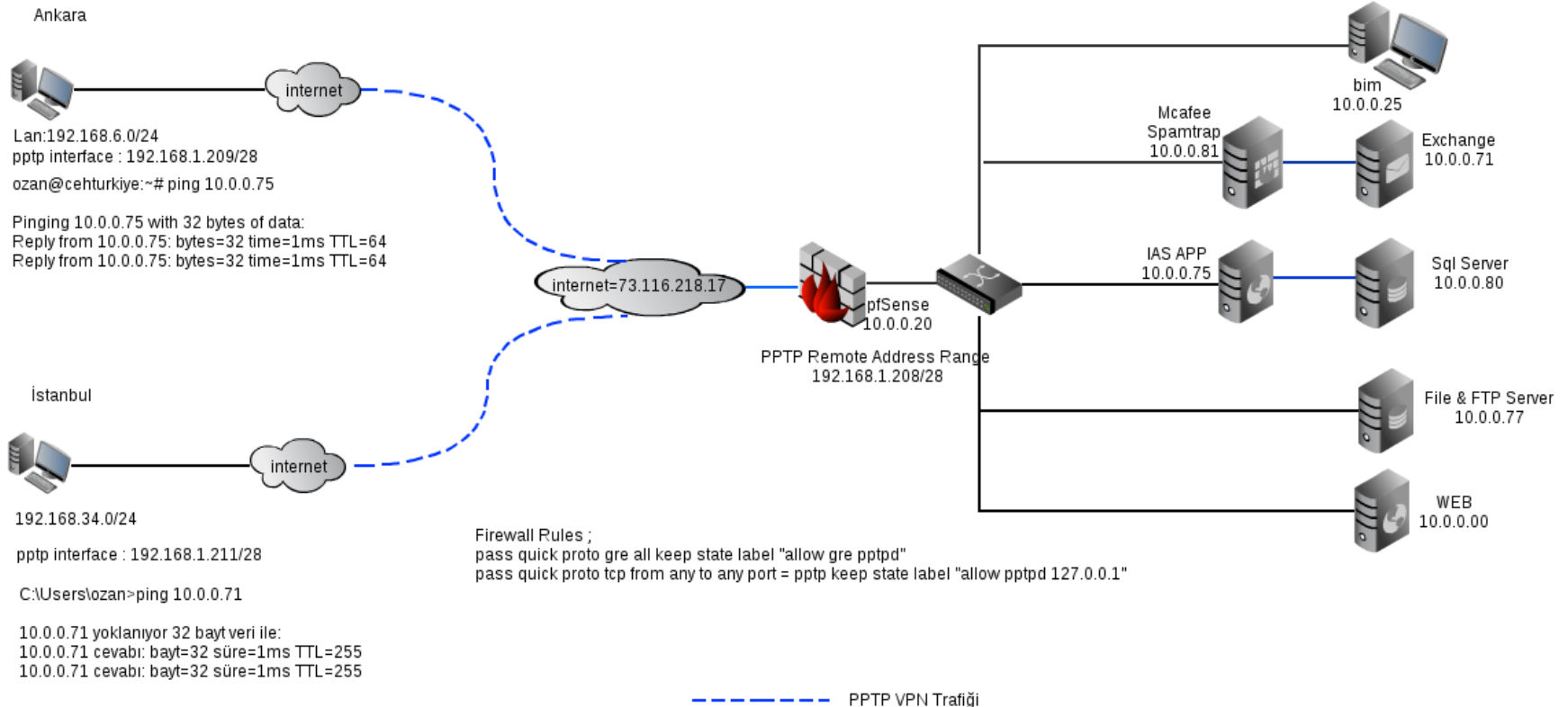
Bölüm 19:

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

Aslen ağ protokollerini analiz için tasarlanmış olmasada, 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

Network Games

pfSense Traffic Shaper Wizard

Enable: ☒ Prioritize network gaming traffic
This will raise the priority of gaming traffic to higher than most traffic.

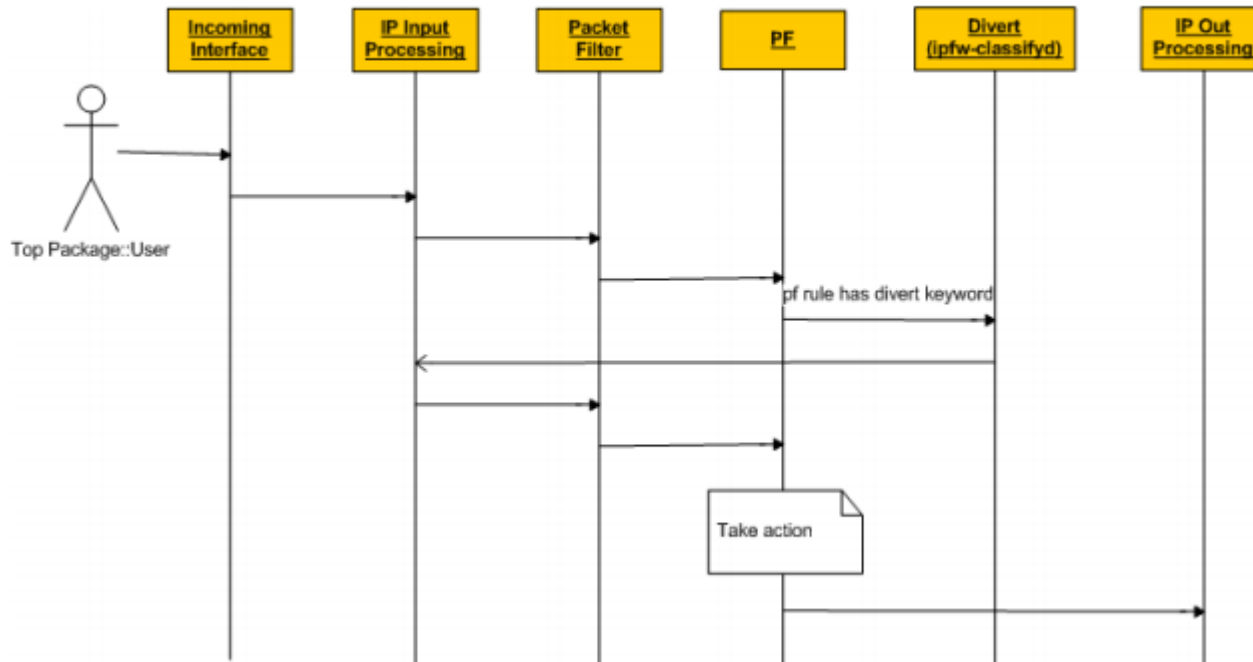
Next

Enable/Disable specific games

BattleNET:	<input type="checkbox"/> Battle.net - Virtually every game from Blizzard publishing should match this. This includes the following game series: Starcraft, Diablo, Warcraft. Guild Wars also uses this port.
Battlefield2:	<input type="checkbox"/> Battlefield 2 - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
CallOfDuty:	<input type="checkbox"/> Call Of Duty (United Offensive)
Counterstrike:	<input type="checkbox"/> Counterstrike. The ultimate 1st person shooter.
DeltaForce:	<input type="checkbox"/> Delta Force
DOOM3:	<input checked="" type="checkbox"/> DOOM3
EmpireEarth:	<input type="checkbox"/> Empire Earth
Everquest:	<input type="checkbox"/> Everquest - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
Everquest2:	<input type="checkbox"/> Everquest II
GunZOnline:	<input type="checkbox"/> GunZ Online
FarCry:	<input type="checkbox"/> Far Cry

Bölüm 20:

Traffic Shaper



IP paketi ipfw-classifyd ye giriş-çıkış yaparken

Bölüm 20:

Traffic Shaper

Firewall: Traffic Shaper: Layer7

By Interface By Queue Limiter **Layer7** Wizards

wizard
Test
webLim
block_p2p
misc

Create new I7 rules group

Enable/Disable ☒ Enable/Disable layer7 Container

Name block_p2p

Description Block P2P traffic
You may enter a description here for your reference (not parsed).

Rule(s)

Add one or more rules

Protocol	Structure	Behaviour
bittorrent	action	block
gnutella	action	block
edonkey	action	block
soribada	action	block
napster	action	block
fasttrack	action	block

Save Cancel Delete

Layer7 grafik arabirimi

In/Out none / none
Choose the Out queue/Virtual interface only if you have selected In too.
The Out selection is applied to traffic going out the interface the rule is created, In is the incoming one.
If you are creating a rule on the Floating tab if the direction is In then the same rules apply, if the direction is out the selections are reverted Out is for incoming and In is for outgoing and if you do not select any direction use only the In since the Out selection does not make sense in there to prevent oddities.

Ackqueue/Queue none / none
Choose the Acknowledge Queue only if you have selected Queue.

Layer7 block_p2p
Choose a Layer7 container to apply application protocol inspection rules. This rule are valid for tcp and udp protocols for now.

Description Layer7 block: P2P
You may enter a description here for your reference.

Save Cancel

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>&nbsp;</td></tr>
  <tr>
    <td colspan="2">
      <center><input name="accept" type="submit" value="Continue"></center>
    </td>
  </tr>
</table>
</center>
</form>
</body>
</html>
```

Bölüm 21:

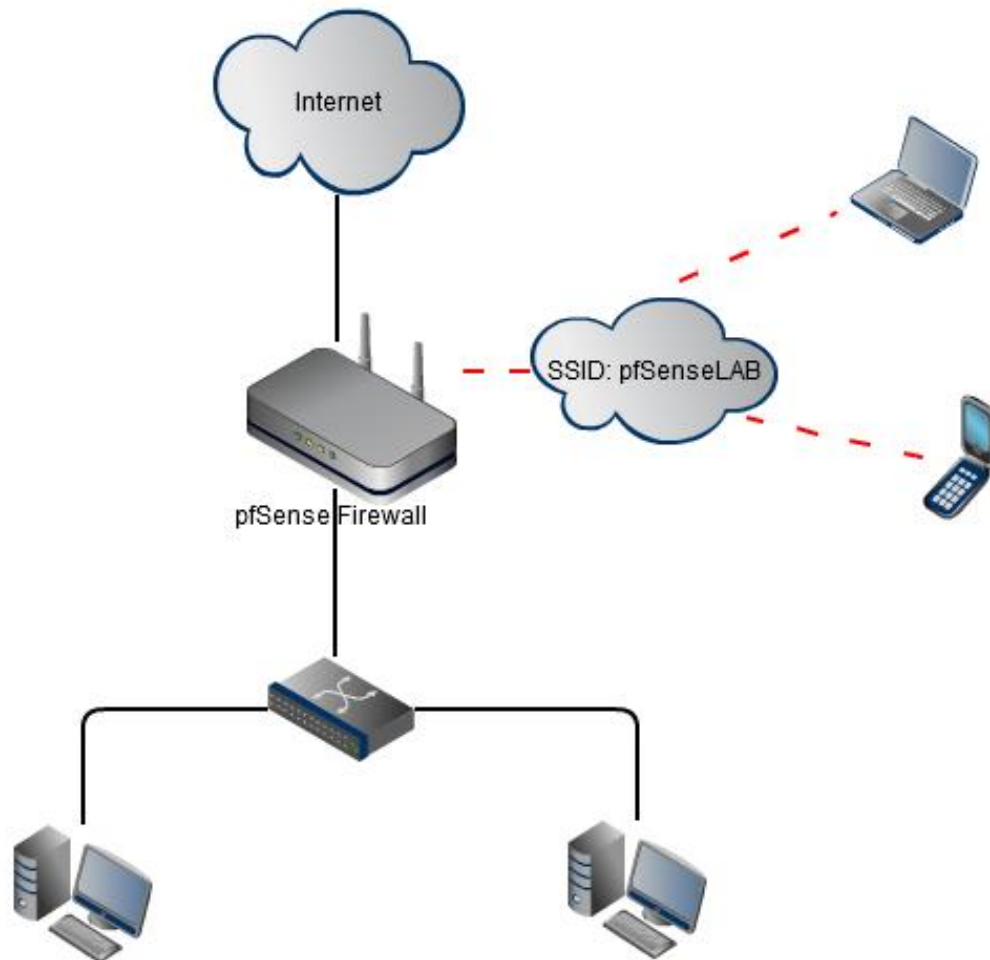
Captive Portal | Özelleştirme

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.

SystemFirewallDHCPPortal AuthIPsec VPNPPTP VPNLoad BalancerOpenVPNOpenNTPDSettings

Last 50 firewall log entries. (Switch to dynamic view)

Act	Time	If	Source	Destination	Proto
✖	Aug 2 12:31:07	WAN	192.168.5.233:137	192.168.5.255:137	UDP
✖	Aug 2 12:31:07	WAN	172.16.16.252:137	172.16.16.255:137	UDP
✖	Aug 2 12:31:07	LAN	192.168.5.233:137	192.168.5.255:137	UDP
✖	Aug 2 12:31:07	WAN	192.168.5.233:137	192.168.5.255:137	UDP
✖	Aug 2 12:31:07	LAN	192.168.5.233:137	192.168.5.255:137	UDP

SystemFirewallDHCPPortal AuthIPsec VPNPPTP VPNLoad BalancerOpenVPN

Last 50 system log entries

Aug 2 12:28:50	kernel: Timecounter "TSC" frequency 2399604399 Hz quality 800
Aug 2 12:28:50	kernel: Timecounters tick every 10.000 msec
Aug 2 12:28:50	kernel: IPsec: Initialized Security Association Processing.
Aug 2 12:28:50	kernel: ad0: 8192MB <VMwa
Aug 2 12:28:50	kernel: acd0: CDROM <VMw.
Aug 2 12:28:50	kernel: Waiting 5 seconds for
Aug 2 12:28:50	kernel: Trying to mount root
Aug 2 12:28:50	kernel: WARNING: / was not properly dismounted

SystemFirewallDHCPPortal AuthIPsec VPNPPTP VPNLoad Balancer

Last 50 Portal Auth log entries

Aug 2 12:35:57	logportalauth[526]: LOGIN: ozanus, 00:04:23:d1:e0:7d, 172.16.16.252
----------------	---

Bölüm 22:

Sistem Monitor | Ağ Arabirimi Durumları

Status: Interfaces

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:

WAN interface (em1)

Status	up
DHCP	up <input type="button" value="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

Status: Services

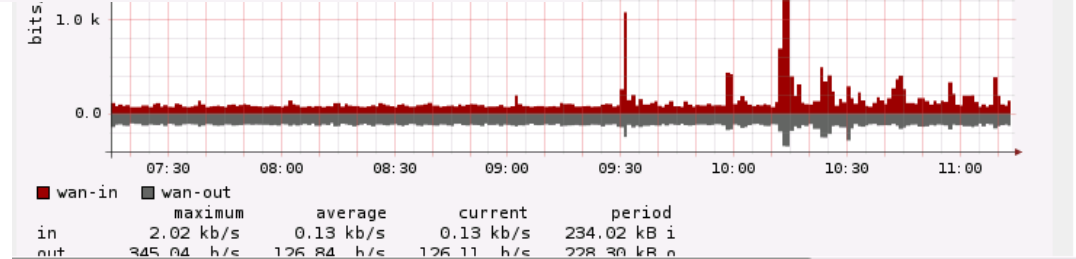
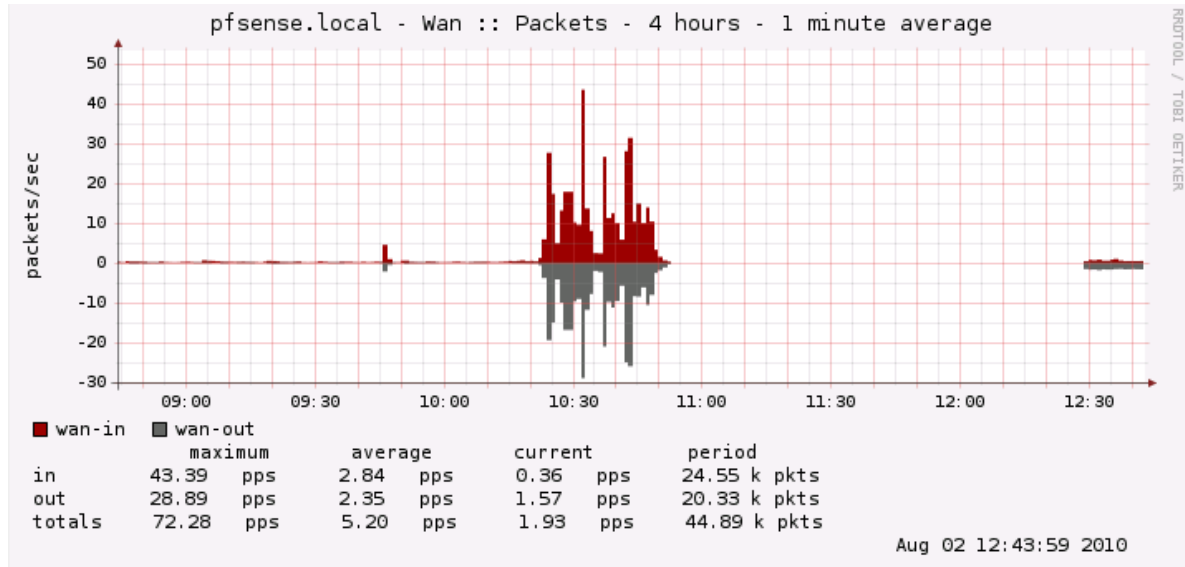
Service	Description	Status	
dnsmasq	DNS Forwarder	▶ Running	 
ntpd	NTP clock sync	✖ Stopped	
lighttpd	Captive Portal	▶ Running	 
dhcpcd	DHCP Service	▶ Running	 
bsnmpd	SNMP Service	▶ Running	 

-  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 | Bağlantı 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.

Status: System logs: Settings

☐ Show log entries in reverse order (newest entries on top)

Number of log entries to show: 50

☒ Log packets blocked by the default rule
Hint: packets that are blocked by the implicit default block rule will not be logged anymore if you uncheck this option. Per-rule logging options are not affected.

☐ Show raw filter logs
Hint: If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information.

☐ Disable writing log files to the local RAM disk

☒ Enable syslog'ing to remote syslog server

Remote syslog servers

Server 1: 85.95.238.71

Server 2: 192.168.1.5

Server 3:

IP addresses of remote syslog servers

☒ system events

☒ firewall events

☒ DHCP service events

☒ Portal Auth

☐ PPTP VPN events

☐ Everything

Save

Bölüm 22:

Sistem Monitor | pflInfo

- Packet Filter istatistikliğini 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.

Diagnostics: pfTop



Sort type:

pfTop: Up State 1-5/5, View: default, Order: bytes

PR	D	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
tcp	I	10.0.0.8:1680	10.0.0.1:80	9:9	91	31	357	257K
tcp	I	10.0.0.8:1681	10.0.0.1:80	9:9	57	64	356	257K
tcp	I	10.0.0.8:1682	10.0.0.1:80	4:4	24	86400	232	163K
icmp	O	6.6.6.104:41059	6.6.6.1:0	0:0	319	10	624	39936
udp	O	6.6.6.104:5525	178.63.102.198:123	2:2	316	35	30	2280

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

System: Package Manager

Kullanılabilir Paket Listesi

1.2.3-RELEASE packages

Installed Packages

Package Name	Category	Status	Package Info	Description
AutoConfigBackup	Services	Stable 1.18 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
Avahi	Network Management	ALPHA 0.6.25_1 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.
Backup	System	Stable 0.1.7 platform: 1.2	No info, check the forum	Tool to Backup and Restore files and directories.
Country Block	Firewall	Beta 0.1.9 platform: 1.2.2	Package Info	Block countries
Cron	Services	Beta 0.2 platform: 1.2	No info, check the forum	The cron utility is used to manage commands on a schedule.
DNS Blacklist	Services	Beta 0.2.4 platform: 1.2.2	No info, check the forum	DNS Blacklist uses dnsmasq entries to block domain names by category.

Paket kur









Bölüm 23:




Paket Sistemi | Paket Yükseltme/Kaldırma

System: Package Manager

1.2.3-RELEASE packages

Installed packages

Package Name	Category	Package Info	Package Version	Description	
Cron	Services	No info, check the forum	0.2	The cron utility is used to manage commands on a schedule.	 
rate	Network Management	No info, check the forum	0.9	This package adds a table of realtime bandwidth usage by IP address to Status -> Traffic Graphs	 
squid	Network	No info, check the forum	2.7.9_4	High performance web proxy cache.	 
squidGuard	Network Management	No info, check the forum	1.3-03	High performance web proxy URL filter. Requires proxy Squid package.	 

-  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



Blog VRT Community Docs Education and Consulting About My Account Sign Out SOURCEfire

My Oinkcode

Oinkcode

011f5a1a18e34ea5b1bb363ed5252415527a248a
1315b868cdfa794abc91ad99ea4045b82a7dd99a
1315b868cdfa794abc91ad99ea4045b82a7dd99a
011f5a1a18e34ea5b1bb363ed5252415527a248a
b51e1b8de6aaf341d9d7a6d3e9bbf51b37ff7cb2
b51e1b8de6aaf341d9d7a6d3e9bbf51b37ff7cb2

Downloading with your Oinkcode

Important Note

In June 2010 we stopped offering rules in the "snortrules-snapshot-CURRENT" format. Instead, rules are released for specific versions of Snort. You will be responsible for downloading the correct rules release for your version of Snort. The new versioning mechanism will require a four digit version in the file name.

Subscriber Release

`http://www.snort.org/sub-rules/<filename>/<oinkcode here>`

e.g. `http://www.snort.org/sub-rules/snortrules-snapshot-2900.tar.gz/011f5a1a18e34ea5b1bb363ed5252415527a248a`

Registered User Release

`http://www.snort.org/reg-rules/<filename>/<oinkcode here>`

e.g. `http://www.snort.org/reg-rules/snortrules-snapshot-2900.tar.gz/011f5a1a18e34ea5b1bb363ed5252415527a248a`

Configuring Oinkmaster

In order to use Oinkmaster to update Snort with VRT rules you must edit oinkmaster.conf

In the oinkmaster.conf modify "url" to:

`url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode here>/<filename>`

e.g. `url = http://www.snort.org/pub-bin/oinkmaster.cgi/011f5a1a18e34ea5b1bb363ed5252415527a248a/snortrules-snapshot-2900.tar.gz`

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

Bölüm 24:

Snort IDS/IPS | Genel Ayarlar

Services: Snort: Global Settings

Snort Interfaces Global Settings Updates Alerts Blocked Whitelists Suppress Help

Please Choose The Type Of Rules You Wish To Download

Install Snort.org rules

☐ Do NOT Install

☒ Install Basic Rules or Premium rules

Sign Up for a Basic Rule Account

Sign Up for Sourcefire VRT Certified Premium Rules. This Is Highly Recommended

Oinkmaster code

Code: b51e1b8de6aaf341d9d7a6d3e9bbf51b37ff7cb2

Obtain a snort.org Oinkmaster code and paste here.

Install Emergingthreats rules ☒

Emerging Threats is an open source community that produces fastest moving and diverse Snort Rules.

Update rules automatically: 6 HOURS

Please select the update times for rules.

Hint: In most cases, every 12 hours is a good choice.

General Settings

Log Directory Size Limit

☒ Enable directory size limit (Default)

☐ Disable directory size limit

Warnings: PfSense NanoBSD should use no more than 10MB of space.

Notes: Available space is 6387MB

Size in MB: 1404 Default is 20% of available space.

Remove blocked hosts every: 3 HOURS

Please select the amount of time you would like hosts to be blocked for.

Hint: In most cases, 1 hour is a good choice.

Alerts file description type: SHORT

Please choose the type of Alert logging you will like see in your alert file.

Hint: Best practice is to chose full logging. **WARNING: On change, alert file will be cleared.**

Keep snort settings after deinstall ☒

Settings will not be removed during deinstall.

Reset **WARNING:** This will reset all global and interface settings.

Save Cancel

Kurallar hangi aralıklarla güncellenecek ?

Kuralları yükle. Bunun için Oinkmaster koda ihtiyaç var.

Kayıtlar için ne kadar alan kullansın

Kayıt türü


Eğer Snort'u sistemden kaldıracak olursam ayarlarını sakla.

Bölüm 24:

Snort IDS/IPS | İmzalar

Services: Snort: Update Rules

Snort imzaları




There is a new set of Snort.org rules posted. Downloading...

Snort download in progress

Downloaded : 5587835

Services: Snort: Update Rules

Emergingthreats imzaları



There is a new set of Emergingthreats rules posted. Downloading...

70%

Bölüm 24:

Snort IDS/IPS| Ağ Ayarları

Snort: Interface Edit: 0 28112 em0

Snort Interfaces **If Settings** **Categories** **Rules** **Servers** **Preprocessors** **Barneyard2**

General Settings

Interface	<input checked="" type="checkbox"/> Enable or Disable
Interface	<div>LAN</div> <div>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</div>
Description	<div>Lan Network</div> <div>You may enter a description here for your reference.</div>
Memory Performance	<div>AC-BNFA</div> <div>Lowmem and ac-bnfa are recommended for low end systems, Ac: high memory, best performance, ac-std: moderate memory, high performance, acs: small memory, moderate performance, ac-banded: small memory, moderate performance, ac-sparsebands: small memory, high performance.</div>

Hafıza için Performans Ayarı

Choose the networks snort should inspect and whitelist.

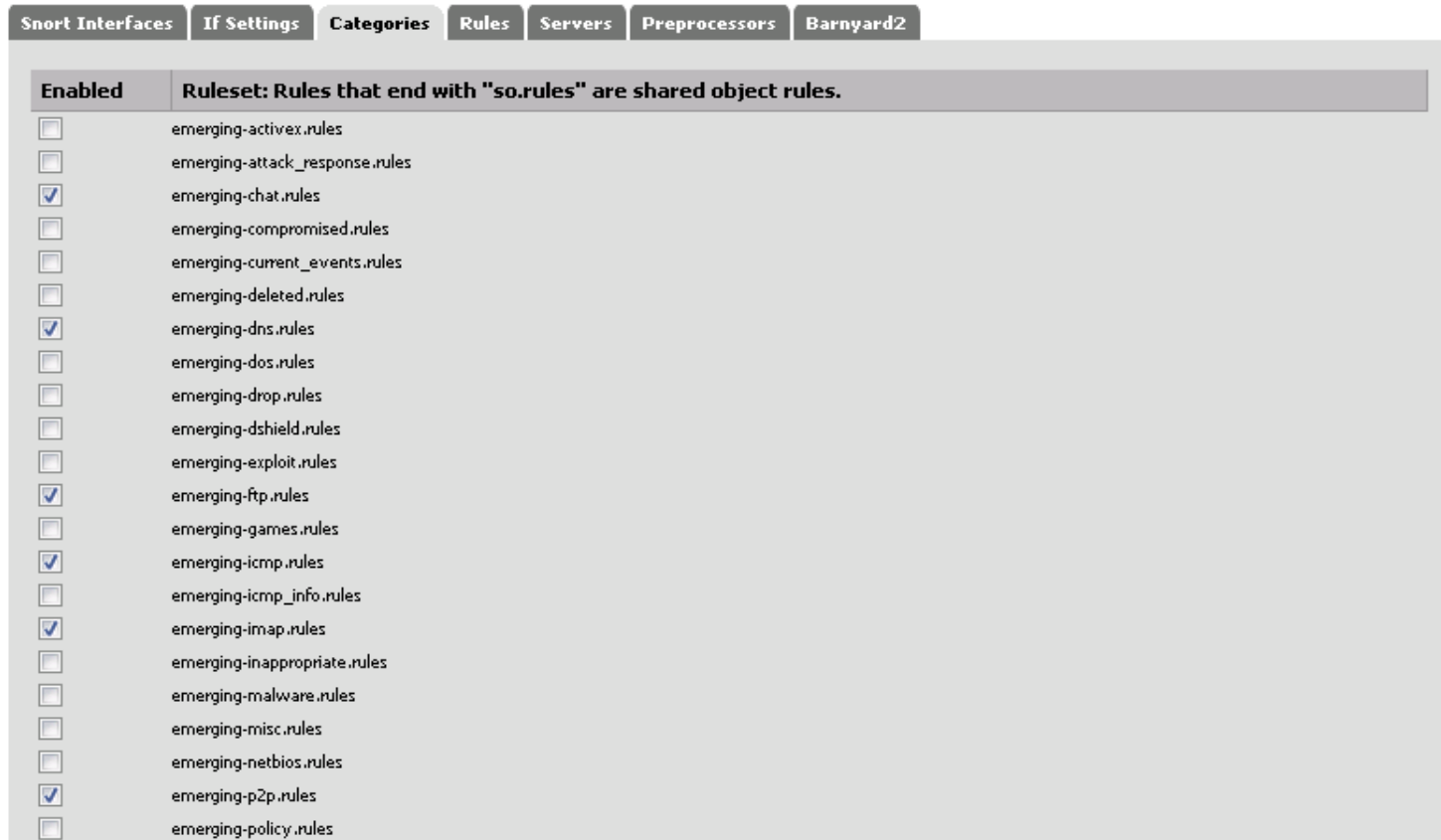
Home net	<div>default</div> <div>Choose the home net you will like this rule to use. Note: Default home net adds only local networks. Hint: Most users add a list of friendly ips that the firewall cant see.</div>
External net	<div>default</div> <div>Choose the external net you will like this rule to use. Note: Default external net, networks that are not home net. Hint: Most users should leave this setting at default.</div>
Block offenders	<div><input type="checkbox"/></div> <div>Checking this option will automatically block hosts that generate a Snort alert.</div>
Whitelist	<div>default</div> <div>Choose the whitelist you will like this rule to use. Note: Default whitelist adds only local networks.</div>

Snort bir saldırı girişimi veya anormallik tespit ederse, ilgili kurala göre block uygula. Bu özellik Snort'a IPS özelliği kazandırır

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

Snort: 0 28112 em0 Category: snort_p2p.rules

Snort Interfaces If Settings Categories Rules Servers Preprocessors Barnyard2

Category: snort_p2p.rules There are 17 rules in this category.

SID	Destination	Port	Message
1432	\$EXTERNAL_NET	any	P2P GNUTella client request
556	\$EXTERNAL_NET	any	P2P Outbound GNUTella client request
557	\$EXTERNAL_NET	any	P2P GNUTella client request
2180	\$EXTERNAL_NET	any	P2P BitTorrent announce request
2181	\$EXTERNAL_NET	any	P2P BitTorrent transfer
2587	\$EXTERNAL_NET	any	P2P eDonkey server response
3459	\$EXTERNAL_NET	41170	P2P Manolito Search Query
3681	\$EXTERNAL_NET	5190	P2P AOL Instant Messenger file receive attempt
3680	\$HOME_NET	any	P2P AOL Instant Messenger file send attempt
5694	\$EXTERNAL_NET	\$HTTP_PORTS	P2P Skype client setup get newest version attempt
5695	\$EXTERNAL_NET	\$HTTP_PORTS	P2P Skype client start up get latest version attempt



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

```
save Cancel
Disable original rule : ☐ ☒
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ET POLICY Possible External Ultrasurf Anonymizer DNS Query"; c
# Emerging Threats
#
# This distribution may contain rules under two different licenses.
#
# Rules with sids 1 through 3464, and 100000000 through 100000908 are under the GPLv2.
# A copy of that license is available at http://www.gnu.org/licenses/gpl-2.0.html
#
# Rules with sids 2000000 through 2799999 are from Emerging Threats and are covered under the BSD License
# as follows:
#
# *****
# Copyright (c) 2003-2010, Emerging Threats
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without modification, are permitted provided the
# following conditions are met:
#
# * Redistributions of source code must retain the above copyright notice, this list of conditions and the fo
# disclaimer.
# * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
# following disclaimer in the documentation and/or other materials provided with the distribution.
# * Neither the name of the nor the names of its contributors may be used to endorse or promote products deri
```



Kural pasif durumda, tıklandığında kuralı aktif yapar



Kural aktif durumda, tıklandığında kuralı pasif yapar



Kuralı düzenle

Bölüm 24:

Snort IDS/IPS | Kural Yönetimi

Snort: Interface 0em0 Define Servers

Snort Interfaces **If Settings** **Categories** **Rules** **Servers** **Preprocessors** **Barnyard2**

Note:
Please save your settings before you click start.
Please make sure there are **no spaces** in your definitions.

Define Servers

Define DNS_SERVERS	<input type="text" value="8.8.8.8"/> Example: "192.168.1.3/24,192.168.1.4/24". Leave blank to scan all networks.
Define DNS_PORTS	<input type="text"/> Example: Specific ports "25,443" or All ports between "5060:5090". Default is 53.
Define SMTP_SERVERS	<input type="text" value="192.168.1.25"/> Example: "192.168.1.3/24,192.168.1.4/24". Leave blank to scan all networks.
Define SMTP_PORTS	<input type="text"/> Example: Specific ports "25,443" or All ports between "5060:5090". Default is 25.
Define Mail_Ports	<input type="text"/> Example: Specific ports "25,443" or All ports between "5060:5090". Default is 25,143,465,691.
Define HTTP_SERVERS	<input type="text" value="192.168.1.100"/> Example: "192.168.1.3/24,192.168.1.4/24". Leave blank to scan all networks.
Define WWW_SERVERS	<input type="text"/> Example: "192.168.1.3/24,192.168.1.4/24". Leave blank to scan all networks.
Define HTTP_PORTS	<input type="text" value="8080,443,4444"/> Example: Specific ports "25,443" or All ports between "5060:5090". Default is 80.

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.

Snort Interfaces

If Settings

Categories

Rules

Servers

Preprocessors

Barnyard2

Note:
Rules may be dependent on preprocessors!
Defaults will be used when there is no user input.

Performance Statistics

Enable

☒ Performance Statistics for this interface.

HTTP Inspect Settings

Enable

☒ Use HTTP Inspect to Normalize/Decode and detect HTTP traffic and protocol anomalies.

HTTP server flow depth

-1 to 1460 (-1 disables HTTP inspect, 0 enables all HTTP inspect)
Amount of HTTP server response payload to inspect. Snort's performance may increase by adjusting this value. Setting this value too low may cause false negatives. Values above 0 are specified in bytes. Default value is 0

Stream5 Settings

Max Queued Bytes

Minimum is 1024, Maximum is 1073741824 (default value is 1048576, 0 means Maximum)
The number of bytes to be queued for reassembly for TCP sessions in memory. Default value is 1048576

Max Queued Segs

Minimum is 2, Maximum is 1073741824 (default value is 2621, 0 means Maximum)
The number of segments to be queued for reassembly for TCP sessions in memory. Default value is 2621

General Preprocessor Settings

Enable
RPC Decode and Back Orifice
detector

☒
Normalize/Decode RPC traffic and detects Back Orifice traffic on the network.

Enable
FTP and Telnet Normalizer

☐
Normalize/Decode FTP and Telnet traffic and protocol anomalies.

Enable
SMTP Normalizer

☒
Normalize/Decode SMTP protocol for enforcement and buffer overflows.

Enable
Portscan Detection

☐
Detects various types of portscans and portsweeps.

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.

Snort Interfaces	If Settings	Categories	Rules	Servers	Preprocessors	Barnyard2
General Barnyard2 Settings						
Enable	<input checked="" type="checkbox"/> Enable Barnyard2 on this Interface This will enable barnyard2 for this interface. You will also have to set the database credentials.					
Interface	<div>LAN ▼</div> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.					
Mysql Settings						
Log to a Mysql Database	alert, mysql, dbname=snort user=snort host=192.168.1.88 password=snortcuk Example: output database: alert, mysql, dbname=snort user=snort host=localhost password=xyz Example: output database: log, mysql, dbname=snort user=snort host=localhost password=xyz					
Advanced Settings						
Advanced configuration pass through	<div></div> Arguments here will be automatically inserted into the running barnyard2 configuration.					
<div>Save Cancel</div>						

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

Services: Snort 2.8.6.1 pkg v. 1.34

Snort Interfaces Global Settings Updates Alerts Blocked Whitelists Suppress Help

	If	Snort	Performance	Block	Barnyard2	Description	
	LAN	ENABLED	AC-BNFA	DISABLED	ENABLED	Lan Network	  


Note:


This is the **Snort Menu** where you can see an over view of all your interface settings.
Please edit the **Global Settings** tab before adding an interface.


Warning:


New settings will not take effect until interface restart.

Click on the  icon to add a interface.

Click on the  icon to edit a interface and settings.

Click on the  icon to delete a interface and settings.

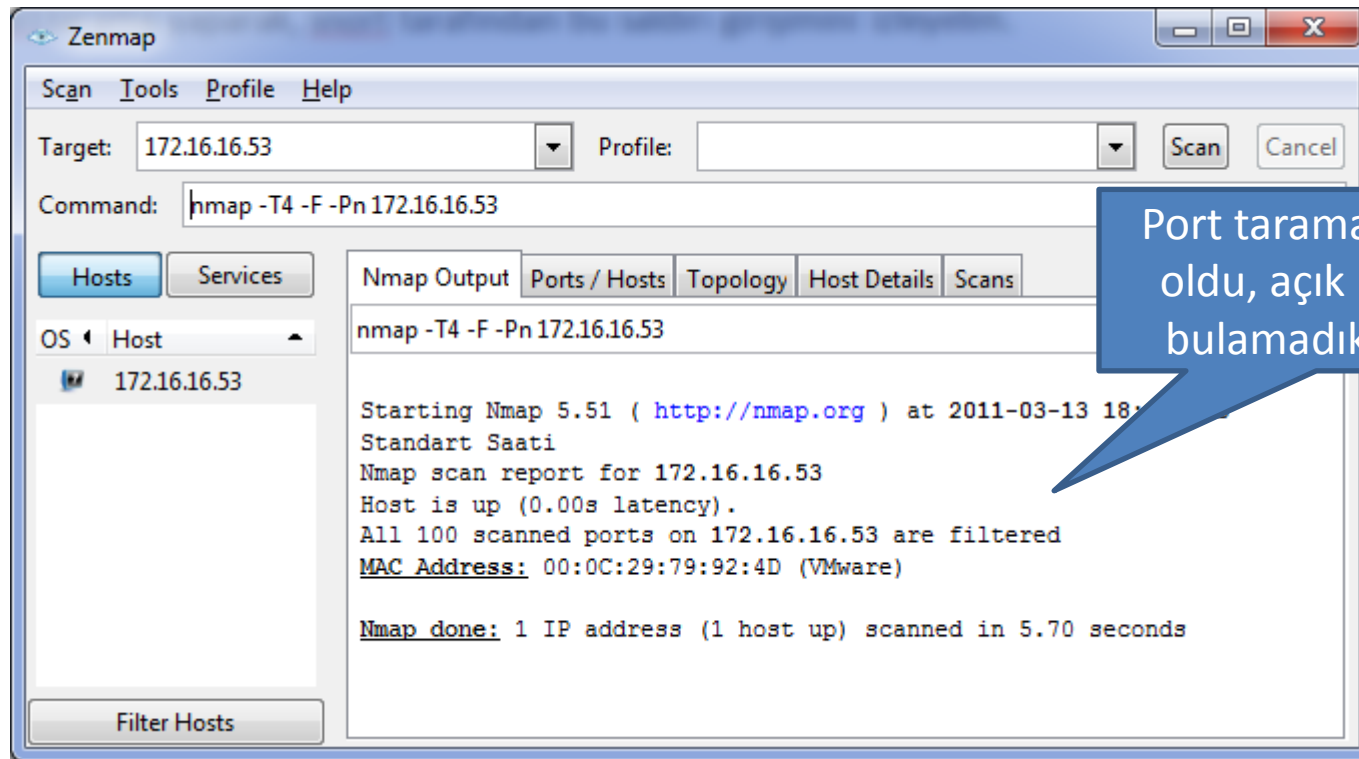
Click on the  icon to **start** snort and barnyard2.

Click on the  icon to **stop** snort and barnyard2.

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.

Services: Snort: Snort Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Whitelists Suppress Help

Last 250 Alert Entries.

Save or Remove Logs

Latest Alert Entries Are Listed First.

Download All log files will be saved. Clear **Warning:** all log files will be deleted.

Auto Refresh and Log View

Save Refresh ☐ **Default is ON.** Enter the number of log entries to view. **Default is 250.**

Filter: PRIORITY Submit Clear

#	PRI	PROTO	DESCRIPTION	CLASS	SRC	SPORT	FLOW	DST	DPORT	SID	Date
1	3	PROTO:255	(portscan) TCP Filtered Portscan	Prep	1.1.1.5	empty	->	172.16.16.53	empty	122:5:0	03/13-18:21:51
2	3	PROTO:255	(portscan) TCP Filtered Portscan	Prep	1.1.1.5	empty	->	172.16.16.53	empty	122:5:0	03/13-18:20:22

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.

Services: Snort Blocked Hosts

[Snort Interfaces](#) [Global Settings](#) [Updates](#) [Alerts](#) [Blocked](#) [Whitelists](#) [Suppress](#) [Help](#)

Last 500 Blocked.


This page lists hosts that have been blocked by Snort. Settings are set to never remove hosts.

Save or Remove Hosts

[Download](#) All blocked hosts will be saved. [Clear](#) **Warning:** all hosts will be removed.

Auto Refresh and Log View

[Save](#) Refresh ☒ **Default is ON.** Enter the number of blocked entries to view. **Default is 500.**

Remove	#	IP	Alert Description
	1	1.1.1.5	(portscan) TCP Filtered Portscan

1 items listed.

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
```

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Proxy interface		<div>LAN WAN DMZ WAN2</div> <div>The interface(s) the proxy server will bind to.</div>				
Allow users on interface		<input checked="" type="checkbox"/> If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.				
Transparent proxy		<input checked="" type="checkbox"/> If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.				
Bypass proxy for Private Address Space (RFC 1918) destination		<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918) destination through the proxy server but directly through the firewall.				
Bypass proxy for these source IPs		<input type="text"/> Do not forward traffic from these source IPs, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;).				
Bypass proxy for these destination IPs		<input type="text"/> Do not proxy traffic going to these destination IPs, hostnames, or aliases, but let it pass directly through the firewall. Separate by semi-colons (;).				

Bölüm 25:

Squid | Upstream Proxy

Proxy server: Upstream proxy settings

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Enable forwarding		<input checked="" type="checkbox"/>				
		This option enables the proxy server to forward requests to an upstream server.				
Hostname		<input type="text" value="192.168.1.99"/>				
		Enter here the IP address or host name of the upstream proxy.				
TCP port		<input type="text" value="3128"/>				
		Enter the port to use to connect to the upstream proxy.				
ICP port		<input type="text" value="7"/>				
		Enter the port to connect to the upstream proxy for the ICP protocol. Use port number 7 to disable ICP communication between the proxies.				
Username		<input type="text" value="squids"/>				
		If the upstream proxy requires a username, specify it here.				
Password		<input type="password" value="•••••"/>				
		If the upstream proxy requires a password, specify it here.				

Bölüm 25:

Squid | Önbellek Yönetimi

Proxy server: Cache management

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Hard disk cache size <input type="text" value="100"/>						
This is the amount of disk space (in megabytes) to use for						
Hard disk cache system <input type="text" value="ufs"/>						
This specifies the kind of storage system to use.						
ufs is the old well-known Squid storage format that has always been there.						
aufs uses POSIX-threads to avoid blocking the main Squid process on disk-I/O. (Formerly known as async-io .)						
diskd uses a separate process to avoid blocking the main Squid process on disk-I/O.						
null Does not use any storage. Ideal for Embedded/NanoBSD.						
Hard disk cache location <input type="text" value="/var/squid/cache"/>						
This is the directory where the cache will be stored. (note: do not end with a /). If you change this location, squid needs to make a new cache, this could take a while						
Memory cache size <input type="text" value="8"/>						
This is the amount of physical RAM (in megabytes) to be used for negative cache and in-transit objects. This value should not exceed more than 50% of the installed RAM. The minimum value is 1MB.						
Minimum object size <input type="text" value="0"/>						
Objects smaller than the size specified (in kilobytes) will not be saved on disk. The default value is 0, meaning there is no minimum.						
Maximum object size <input type="text" value="4"/>						
Objects larger than the size specified (in kilobytes) will not be saved on disk. If you wish to increase speed more than you want to save bandwidth, this should be set to a low value.						

Önbellek için kullanılacak disk boyutu. Yüksek trafikli ağlarda arttırılması önerilir.

Disk cache methodu

Bölüm 25:

Squid | Önbellek Yönetimi

Level 1 subdirectories	<input type="text" value="16"/> Each level-1 directory contains 256 subdirectories, so a value of 256 level-1 directories will use a total of 65536 directories for the hard disk cache. This will significantly slow down the startup process of the proxy service, but can speed up the caching under certain conditions.
Memory replacement policy	<input type="text" value="Heap GDSF"/> The memory replacement policy determines which objects are purged from memory when space is needed. The default policy for memory replacement is GDSF. LRU: Last Recently Used Policy - The LRU policies keep recently referenced objects. i.e., it replaces the object that has not been accessed for the longest time. Heap GDSF: Greedy-Dual Size Frequency - The Heap GDSF policy optimizes object-hit rate by keeping smaller, popular objects in cache. It achieves a lower byte hit rate than LFUDA though, since it evicts larger (possibly popular) objects. Heap LFUDA: Least Frequently Used with Dynamic Aging - The Heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached. Heap LRU: Last Recently Used - Works like LRU, but uses a heap instead. Note: If using the LFUDA replacement policy, the value of Maximum Object Size should be increased above its default of 12KB to maximize the potential byte hit rate improvement of LFUDA.
Cache replacement policy	<input type="text" value="Heap LFUDA"/> The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. The default policy for cache replacement is LFUDA. Please see the type descriptions specified in the memory replacement policy for additional detail.
Low-water-mark in %	<input type="text" value="90"/> Cache replacement begins when the swap usage is above the low-low-water mark and attempts to maintain utilisation near the low-water-mark.
High-water-mark in %	<input type="text" value="95"/> As swap utilisation gets close to the high-water-mark object eviction becomes more aggressive.
Do not cache	<div><div>milliyet.com.tr haber7.com iyibilgi.com</div><div>Enter each domain or IP address on a new line that should never be cached.</div></div>
Enable offline mode	<input type="checkbox"/> Enable this option and the proxy server will never try to validate cached objects. The offline mode gives access to more cached information than the proposed feature would allow (stale cached versions, where the origin server should have been contacted).

Şu kaynakları
önbelleğe alma

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.

Proxy server: Traffic management

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Trafik limitleri için değerler	Maximum download size	<input type="text" value="0"/>	Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.			
	Maximum upload size	<input type="text" value="0"/>	Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.			
	Overall bandwidth throttling	<input type="text" value="0"/>	This value specifies (in kilobytes per second) the bandwidth throttle for downloads. Users will gradually have their download speed increased according to this value. Set to 0 to disable bandwidth throttling.			
	Per-host throttling	<input type="text" value="0"/>	This value specifies the download throttling per host. Set to 0 to disable this.			
Trafığın set edileceği dosya türleri	Throttle only specific extensions	<input checked="" type="checkbox"/>	Leave this checked to be able to choose the extensions that throttling will be applied to. Otherwise, all files will be throttled.			
	Throttle binary files	<input type="checkbox"/>	Check this to apply bandwidth throttle to binary files. This includes compressed archives and executables.			
	Throttle CD images	<input type="checkbox"/>	Check this to apply bandwidth throttle to CD image files.			
	Throttle multimedia files	<input type="checkbox"/>	Check this to apply bandwidth throttle to multimedia files, such as movies or songs.			

Bölüm 25:

Squid | Kimlik Doğrulama | Yerel

Yerel kullanıcı veritabanını kullanarak kimlik doğrulama yapar.

Dikkat: Transparent modda kimlik doğrulama yapılamaz !

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt **Auth Settings** Local Users

Authentication method Local
None
Local
LDAP
RADIUS
NT domain

Kimlik doğrulama methodu "Local"

LDAP version

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt **Auth Settings** Local Users

Username ozanucar
Enter the username here.

Password
Enter the password here.

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

Save Cancel

Yerel kullanıcı hesabı oluşturmak

Kullanıcı hesaplarını yönetmek

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt **Auth Settings** Local Users

Username	Description
ozanucar	system admin

+

Bölüm 25:

Squid | Kimlik Doğrulama | Ldap

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

Gerekli Bilgiler



Kimlik doğrulama methodu "Ldap"

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

General	Upstream Proxy	Cache Mgmt	Access Control	Traffic Mgmt	Auth Settings	Local Users
Authentication method LDAP Select an authentication method. Authentication is performed by local or external services.						
LDAP version 3 Enter LDAP protocol version (2 or 3).						
Authentication server 172.16.16.99 Enter here the IP or hostname of the server that will perform the authentication.						
Authentication server port Enter here the port to use to connect to the authentication server. Leave this field blank to use the authentication method's default port.						
NT domain Enter here the NT domain.						
LDAP server user DN cn=administrator,cn=Users,dc=cehturkiye,dc=com Enter here the user DN to use to connect to the LDAP server.						
LDAP password •••••• Enter here the password to use to connect to the LDAP server.						
LDAP base domain dc=cehturkiye,dc=com For LDAP authentication, enter here the base domain in the LDAP server.						
LDAP username DN attribute Enter LDAP username DN attribute.						
LDAP search filter sAMAccountName=%s Enter LDAP search filter.						

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

Proxy filter SquidGuard: General settings

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

Enable	<input checked="" type="checkbox"/> Check this for enable squidGuard For saving configuration YOU need click button 'Save' on bottom of page After changing configuration squidGuard you must apply all changes <input type="button" value="Apply"/> SquidGuard service state: STARTED
Enable GUI log	<input type="checkbox"/> Check this for enable GUI log.
Enable log	<input type="checkbox"/> Check this for enable log of the proxy filter. Usually log used for testing filter settings.
Enable log rotation	<input checked="" type="checkbox"/> Check this for enable daily rotate a log of the proxy filter. Use this option for limit log file size.

Blacklist options

Blacklist	<input checked="" type="checkbox"/> Check this for enable blacklist
Blacklist proxy	<input type="text"/> Blacklist upload proxy - enter here, or leave blank. Format: host:[port login:pass] . Default proxy port 1080. Example: '192.168.0.1:8080 user:pass'
Blacklist URL	<input type="text" value="http://www.shallalist.de/Downloads/shallalist.tar.gz"/> Enter FTP, HTTP or LOCAL (pfSense) URL blacklist archive, or leave blank.

Servis Durumu

Karaliste Kullanımı

Karaliste yüklenecek adres

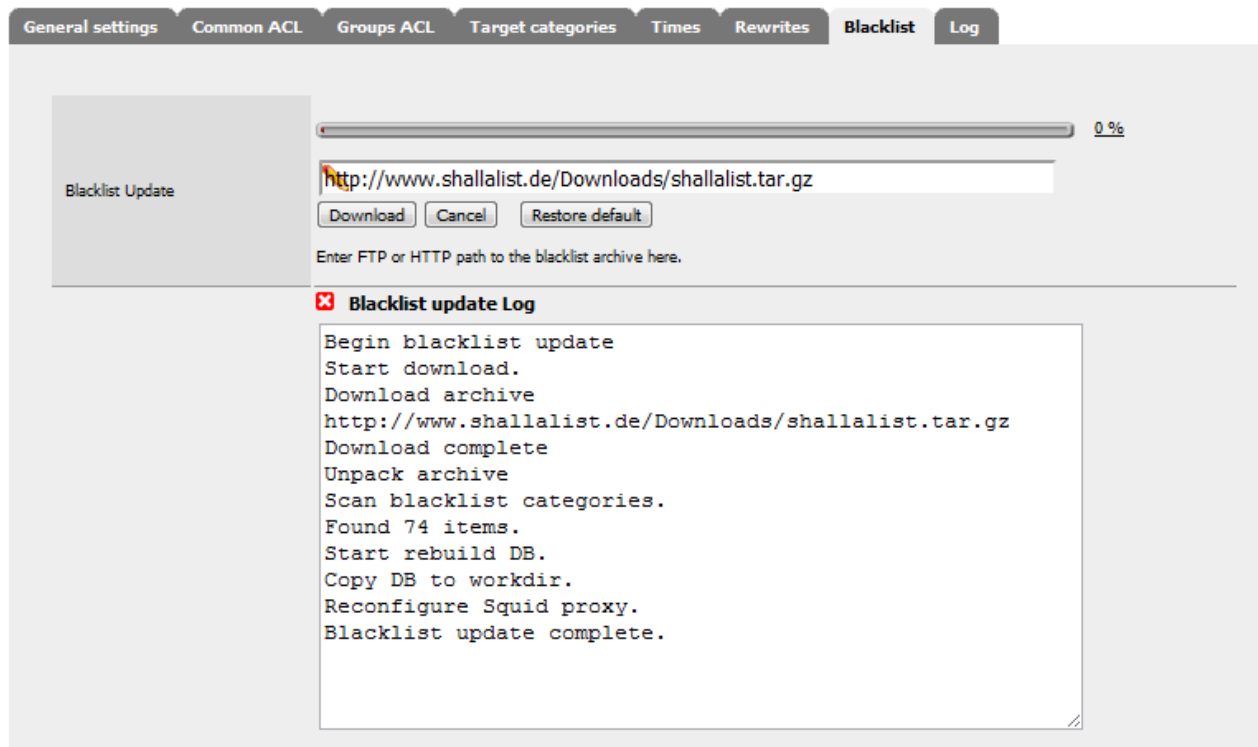
Bölüm 26:

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.

Target Rules List (click here)  

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories	
Fabrikam erişim adresleri [fabrikam]	access <input type="text" value="whitelist"/>
[download_yasak]	access <input type="text" value="deny"/>
[blk_BL_adv]	access <input type="text" value="----"/>
[blk_BL_aggressive]	access <input type="text" value="----"/>
[blk_BL_alcohol]	access <input type="text" value="----"/>
[blk_BL_anonvpn]	access <input type="text" value="----"/>
[blk_BL_automobile_bikes]	access <input type="text" value="whitelist"/>
[blk_BL_automobile_boats]	access <input type="text" value="deny"/>
[blk_BL_automobile_cars]	access <input type="text" value="allow"/>
[blk_BL_automobile_planes]	access <input type="text" value="----"/>
[blk_BL_chat]	access <input type="text" value="----"/>
[blk_BL_costtraps]	access <input type="text" value="----"/>
[blk_BL_dating]	access <input type="text" value="----"/>
[blk_BL_downloads]	access <input type="text" value="----"/>
[blk_BL_drugs]	access <input type="text" value="----"/>

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

Proxy filter SquidGuard: Target categories

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Name	Redirect	Description	 				
fabrikam		fabrikam erisim adresleri	 				
download_yasak	Download Yasak!						

Bölüm 26:

SquidGuard | Yeniden Yönlendirme

URL adresinde geçen bir ifadeyi dönüştürmek için kullanılır.

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

Proxy filter SquidGuard: Rewrites: Edit

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Name	<input type="text" value="bga"/> <small>Enter the unique name here. Name must consist of minimum 2 symbols, first from which letter. All other symbols must be [a-Z_0-9].</small>						
Rewrite rule. Define how url will be replaced.	Target URL or regular expression		Replace to URL	Opt.			
	<input type="text" value="*bga.com.tr"/>		<input type="text" value="http://www.cehturkiye.com"/>	<div><div>no case</div><div>no case</div><div>no case</div><div>no case</div><div>no case + redirect</div></div>			
Log	<input checked="" type="checkbox"/> Check this for log this item.						
Description	<input type="text" value="bga2cehturkiye"/> <small>You may enter a description here for your reference (not parsed).</small> Note: Rewrite rule - define how url will are replaced. Target URL or regular expression - contains destination url or regular expression. Regular expression example: */cc32e46.exe Replace to - contains replacing url.						
<div>Save Cancel</div>							

Bölüm 26:

SquidGuard | Zaman Tanımları

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

Proxy filter SquidGuard: Times: Edit

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

Name	<input type="text" value="mola_saatleri"/> <small>Enter the unique name here. Name must consist of minimum 2 symbols, first from which letter. All other symbols must be [a-Z_0-9].</small>								
Values	<table><tr><td>Time type</td><td>Days</td><td>Date or Date range</td><td>Time range</td></tr><tr><td>Date </td><td>all </td><td>*,*,* <input type="text"/></td><td>12:30-13:30 <input type="text" value=""/></td></tr></table>	Time type	Days	Date or Date range	Time range	Date	all	*,*,* <input type="text"/>	12:30-13:30 <input type="text" value=""/>
Time type	Days	Date or Date range	Time range						
Date	all	*,*,* <input type="text"/>	12:30-13:30 <input type="text" value=""/>						
Description	<input type="text" value="personel mola saati"/> <small>You may enter a description here for your reference (not parsed). Note: Field 'Date or date range' have format 'yyyy.mm.dd'; 'yyyy.mm.dd-yyyy.mm.dd'; or use '*' in format. Example: '2007.05.01'; '2007.04.14-2007.04.17'; '*,12.24'; '2007.*,01'; Field 'Time range' have format 'hh:mm-hh:mm'. Example: '08:00-18:00';</small>								

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 filtreleme 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.

Proxy filter SquidGuard: Common Access Control List (ACL)

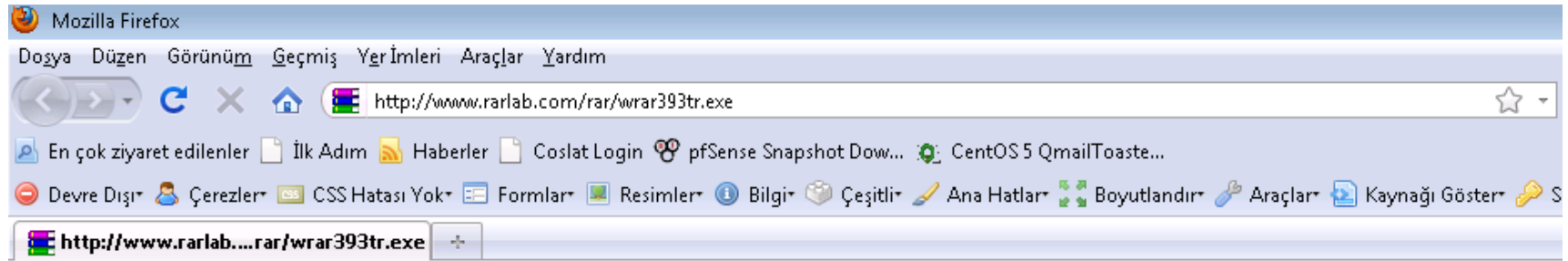
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Target Rules	<input type="text" value="^fabrikam !download_yasak !all"/> Target Rules List (click here)  						
Not to allow IP addresses in URL	<input checked="" type="checkbox"/> To make sure that people don't bypass the URL filter by simply using the IP addresses instead of the fully qualified domain names, you can check this option. This option has no effect on the WhiteList.						
Redirect mode	<input type="text" value="int error page (enter error message)"/> Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.						
Redirect info	<input type="text" value="Yasaklı Adres. Erişiminiz Engellendi."/> Enter external redirection URL, error message or size (bytes) here.						
Use SafeSearch engine	<input checked="" type="checkbox"/> To protect your children from adult content, you can use the protected mode of search engines. Now it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing. Make sure that the search engines can, and others, it is recommended to prohibit. Note: ! This option overrides 'Rewrite' setting. !						
Rewrite	<input type="text" value="bga"/> none (rewrite not defined) for this rule, or leave blank. <input type="text" value="bga"/> <input type="text" value="safesearch"/>						
Log	<input type="checkbox"/> Check this for log this item.						

Bölüm 26:

SquidGuard | Genel ACL | Test

Ön tanımlı tüm istemcilere “download_yasak” kuralı uygulanacaktır. \.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 “Yasaklı Adres. Erişiminiz Engellendi” mesajımız ile cevap verildi 😊



Request denied by pfSense proxy: 403 Forbidden

Reason: Yasaklı Adres. Erişiminiz Engellendi.

Client address: 192.168.1.5

Client group: default

Target group: download_yasak

URL: http://www.rarlab.com/rar/wrar393tr.exe

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 filtreleme 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 192.168.1.1-192.168.1.10. Bu ip aralığına her zaman her şey serbest sadece zararlı içerikli siteler yasak (hacking gibi)

Senaryo 2: Sunucu adreslerim 192.168.1.88, 192.168.1.33, 192.168.1.56.
Sunucularıma her zaman her şey 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 her şey yasak.

Senaryo 4: Sistemimde kimlik doğrulama yapıyorum. “ozan” kullanıcı ile giriş yaptığımda her zaman her şey 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.

Proxy filter SquidGuard: Groups Access Control List (ACL)

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Disabled	Name	Time	Description				
<input type="checkbox"/>	yonetim		Yonetim Birimi				
<input type="checkbox"/>	uretim	mola_saatleri	Mesai saatleri internet yasak, mola saatlerinde izinli				

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

Settings

minute	10
hour	*
mday	*
month	*
wday	*
who	root
command	perl /usr/local/www/lightsquid/lightpsel.pl

Save Cancel

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:

BandwidthD

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:

IMInspector

System > Packages > IMInspector

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 IMInspector protocol plugin
imspector: Protocol Plugin name: Jabber IMInspector protocol plugin
imspector: Protocol Plugin name: MSN IMInspector protocol plugin
imspector: Protocol Plugin name: Yahoo IMInspector 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 IMInspector filter plugin
imspector: Bad-words: Loaded 86 bad-words, replacing with '*' and blocking at 1
imspector: Filter Plugin name: Bad-words IMInspector filter plugin
imspector: Misc: Blocking all file transfers
imspector: Filter Plugin name: Misc IMInspector 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 configuration

Click this button to download the system configuration in XML format.

Backup area:

☐ 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!)

Password:

confirm:

Download configuration

Backup ve Restore işlemlerinde config.xml içeriği şifrelenebilir.

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

Restore configuration

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

Restore area:

config-pfsla...4153653.xml

☒ Configuration file is encrypted.

Password :

confirm :

Restore configuration

Note:

The firewall will reboot after restoring the configuration.

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 oluşturan 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 oluşturan 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:

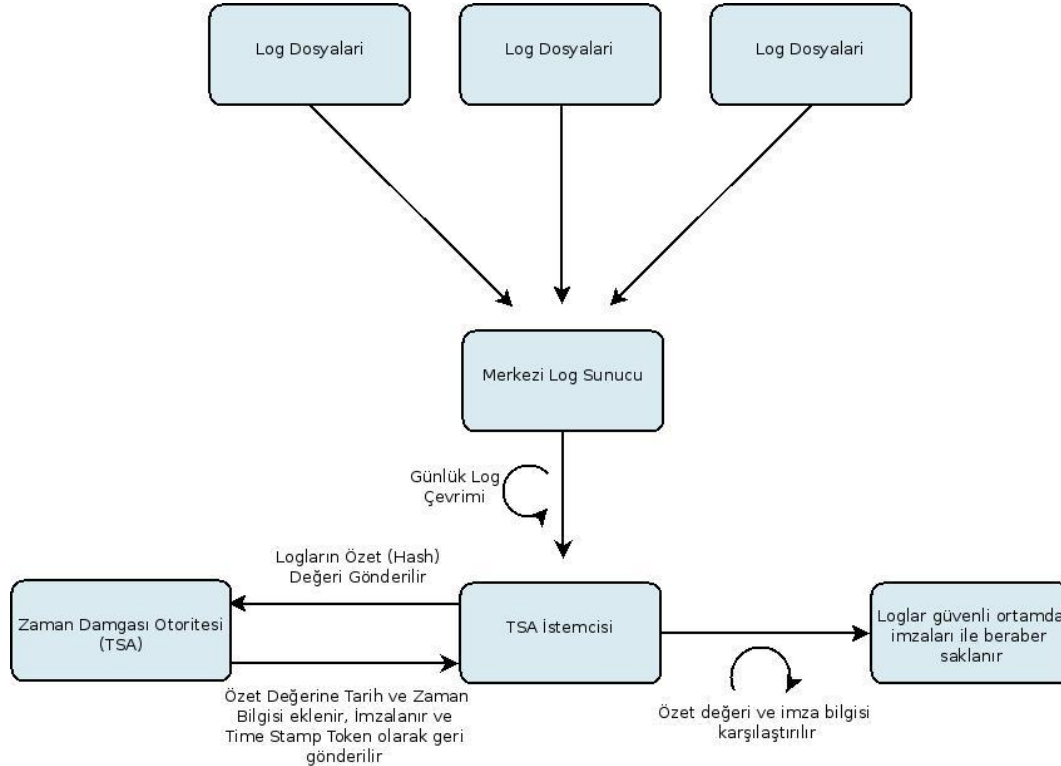
Zaman Damgası Standartlar

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 alındığı tarihte orjinal haliyle var olduğunu, 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 protokolleri 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 konfigürasyon 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

```
cvsup -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 oluşturmak 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 oluşturulur. Kurulum dosyasını test edebilirsiniz.