

İçindekiler

| | |
|---|----|
| PfSense Nedir? | 2 |
| Kurulum | 3 |
| Yerel Ağ ın (LAN) IP Adreslerinin Ayarlanması | 13 |
| İnternet Ç ıkışını Kontrol Etmek..... | 16 |
| pfSense'de Yapılacak Genel Ayarlar | 17 |
| pfSense'de İçerik Filtreleme (Content Filter) | 23 |
| Squid Kurulumu..... | 24 |
| Squid Ayarları | 26 |
| SquidGuard Kurulumu..... | 28 |
| İçerik Filtrelemede Kullanıcıları Gruplandırmak | 35 |
| İçerik Filtrelemede Dosya Uzantılarına Göre Engelleme | 38 |
| pfSense'de MSN Messenger Engelleme | 40 |
| pfSense'de Facebook Engelleme | 44 |
| Facebook'a https://.. üzerinden Erişimi Engelleme | 46 |
| Mac adreslerine göre İp Atama | 50 |
| pfSense Backup/Restore Yapma | 51 |

İsmail Karaca

PfSense Nedir?

PfSense, FreeBSD tabanlı bir dağıtım olarak, BSD sağlamlığını taşıyan, son zamanlarda adından sıkça söz ettiren oldukça gelişmiş ve yetenekli bir güvenlik duvarı dağıtımıdır. BSD lisansı ile dağıtılmaktadır.

Kurulum İçin Neler Gerekli?

Donanım

Kurulum yapmak için; iki ağ arabirimine sahip bir bilgisayara ihtiyacınız olacaktır. PfSense tek ve çok işlemcili bilgisayarlarda çalışabilir.

PfSense Kurulum CD'si

PfSense kurulumu için ihtiyaç duyacağımız CD imajını

<http://www.pfsense.org/mirror.php?section=downloads> adresinde yer alan yansılardan herhangi birinden indirebiliriz.

Bu belgenin hazırlandığı sırada pfSense-2.1.0-LiveCD-Installer.iso isimli 60 MB büyüklüğündeki pfSense iso dosyası kullanılmıştır.

İsmail Karaca

Kurulum

Kurulumu Başlıyoruz

İso dosyasını uygun şekilde bir CD'ye yazdıktan sonra kurulum yapacağınız bilgisayara takmanız ve sistemi CD'den boot etmeniz gerekmektedir. Sistem açıldıktan sonra ilk olarak geçerli ağ arabirimlerini gösterecek ve bunlardan hangisinin LAN hangisinin WAN tarafına bağlı olduğunu belirlemenizi isteyecektir.

Sistemimizde bulunan ağ arabirimleri "Valid interfaces are" başlığı altında ağ arabirimi adı ve MAC adresleri ile gösterilmektedir. Yukarıdaki ekranda le0 ve le1 örnek kurulumu yaptığımız sistemde yer alan Ethernet kartlarıdır.

"Do you want set up VLANs now [y | n]?" soruya n şeklinde cevap verelim ve hemen ardından aşağıdaki ekranda olduğu gibi bize sorulan LAN arabiriminin ismini yazalım.

```
[ 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.

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

Timeout before auto boot continues (seconds): 1

Loading configuration.....done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:
le0      00:0c:29:d1:57:93
le1      00:0c:29:d1:57:9d

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]?
```

Yukarıdaki ekran görüntüsünde görüldüğü gibi sistemde bulunan le0 isimli Ethernet kartının güvenlik duvarımızın yerel ağa bağlı bulunan LAN bacağı olduğunu belirttik. Bir sonraki adımda güvenlik duvarımızın WAN bacağını seçmemiz istenecektir.

"Enter the WAN interface name or 'a' for auto-dedection:" sorusuna WAN bacağı olarak lei olarak isimlendirilen ağ arabirimini girelim. Son olarak ek bir ağ arabirimi seçmek isteyip istemediğimizi soran "Enter the Optional 1 interface name or 'a' for auto-detection (or nothing if finished):" sorusuna yalnızca Enter tuşuna basarak geçelim. "Do you want to proceed [y | n]" sorusuna "y" yanıtını verip pfSense'in işlem yapmasını bekleyelim.

```
Enter the LAN interface name or 'a' for auto-detection: le0
Enter the WAN interface name or 'a' for auto-detection: le1
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN -> le0
WAN -> le1

Do you want to proceed [y:n]?
```

Aşağıdaki pfSense hoş geldiniz ekranını gördüğünüzde pfSense güvenlik duvarınız Çalışan CD olarak hizmetinizdedir. Bu ekranda LAN ve WAN ağ arabirimlerinin hangileri olduğu, bu arabirimlerin hangi IP adreslerini ne olduğu görülebilir. Bu alanın altında pfSense seçenekleri görüntülenir.

```
*** WelcoMe to pfSense 2.0.1 - pfSense ***
WAN(wan) -> sis0 -> 10.115.16.152(DHCP)
LAN(lan) -> sis1 -> 10.0.0.1
pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console
99) Install pfSense to a hard drive, etc.
drive/Memory
Enter an option: |
```

"Enter an option:" sorusuna bu menüde yer alan seçeneklerden birisini seçebilirsiniz. Sistemin daha performanslı çalışabilmesi için pfSense seçeneklerinden "99) Install pfSense to a hard driver/memory drive, etc." seçeneği ile sabit diske kurulum yapılabilir. Diğer seçeneklerden yeri geldikçe bahsedilecektir. Kurulum işlemi başladığında ilk olarak aşağıdaki gibi bir yapılandırma ekranı karşımıza gelecektir.

Eğer standart olarak İngilizce Q düzeninde gelen klavye düzenini değiştirmek isterseniz

"Change Keymap (default)" seçeneği ile değiştirebilirsiniz. Bu ekranda

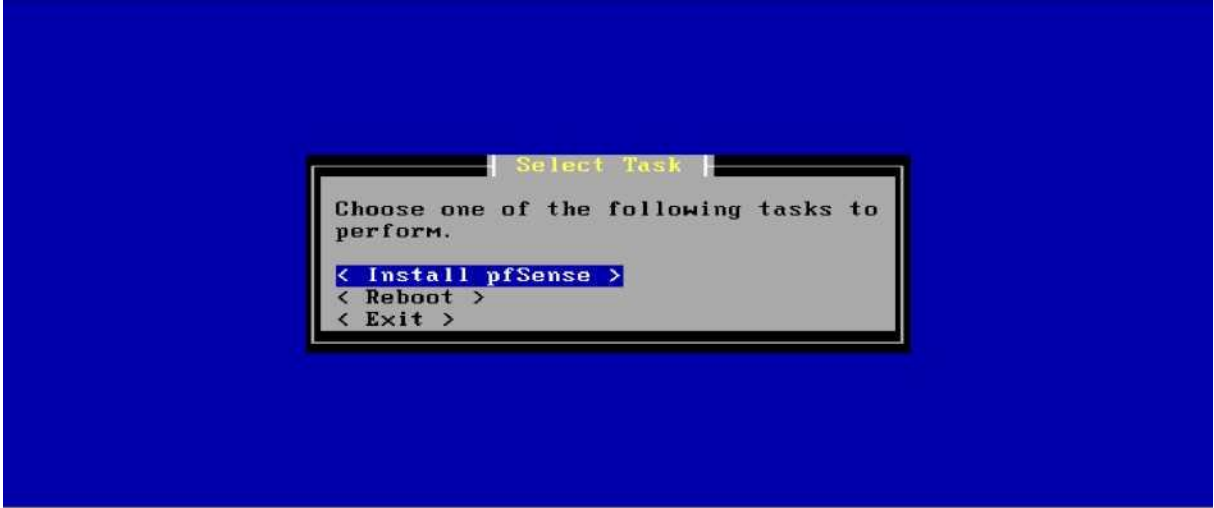
Configure Console

Your selected environment uses the following console settings, shown in parentheses. Select any that you wish to change.

- < Change Video Font (default) >
- < Change Screenmap (default) >
- < Change Keymap (default) >
- < Accept these Settings >

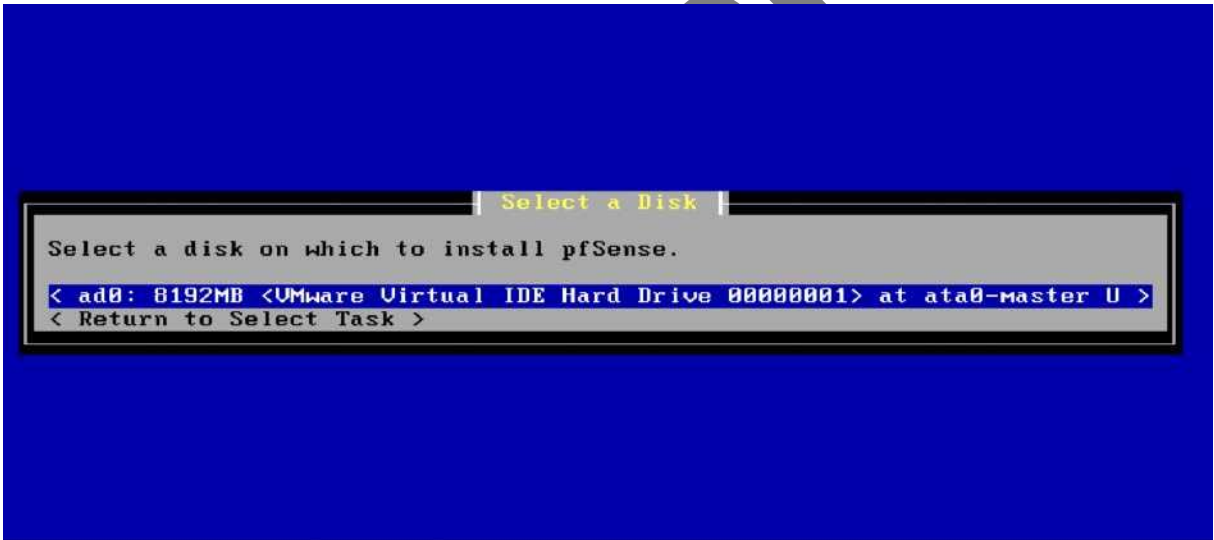
Ismail Karac

"Accept these Settings" seçeneğini kullanarak ön tanımlı ayarları kullanarak kurulumu başlatabiliriz.



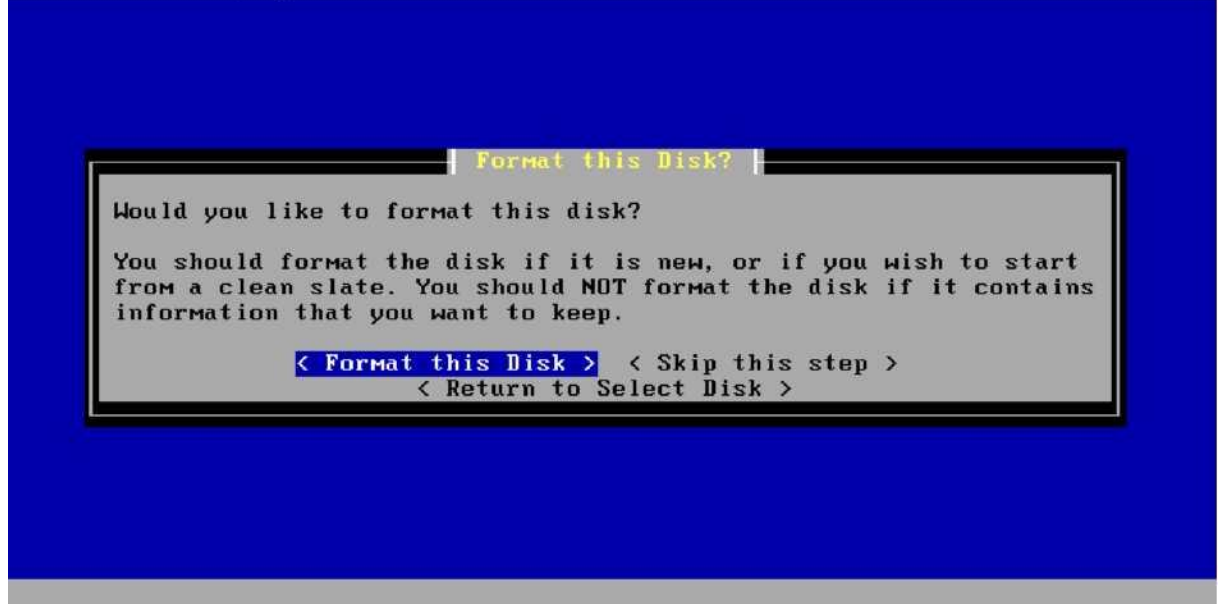
Install pfSense on this computer system

Bu aşamada "Install pfSense" seçeneği ile pfSense kurulumuna başlayabilir, reboot seçeneği ile sistemi yeniden başlatabilir, Exit ile kurulum işleminden çıkabiliriz.



Bu ekranda kurulum için kullanılacak olan sabit diski seçmemiz gerekiyor. Sisteminizde pfSense kurulumu için hazır olan sabit diskimizi seçerek devam ediyoruz.

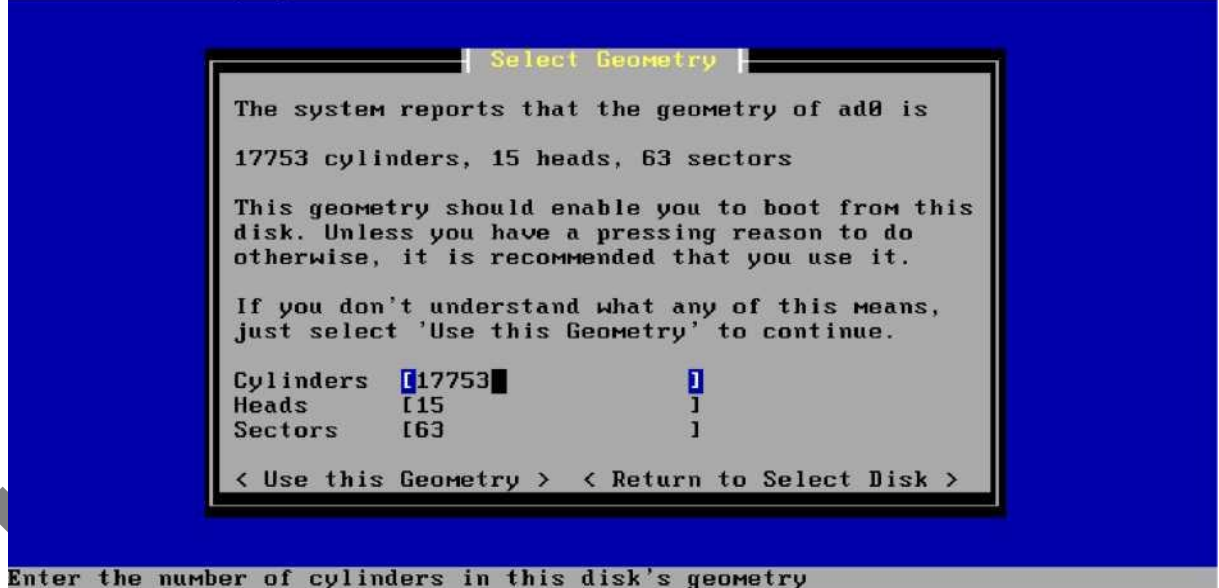
F10=Refresh Display



Bu aşamada seçmiş olduğumuz sabit disk formatlamak isteyip istemediğimiz soruluyor. Eğer daha önceden uygun şekilde biçimlendirilmiş bir diske sahipseniz <Skip this step> seçeneği ile sabit disk biçimlendirme adımını atlayabilirsiniz.

Biz sabit diskimizi formatlayarak devam edeceğimiz için <Format this Disk> seçeneği ile devam ediyoruz.

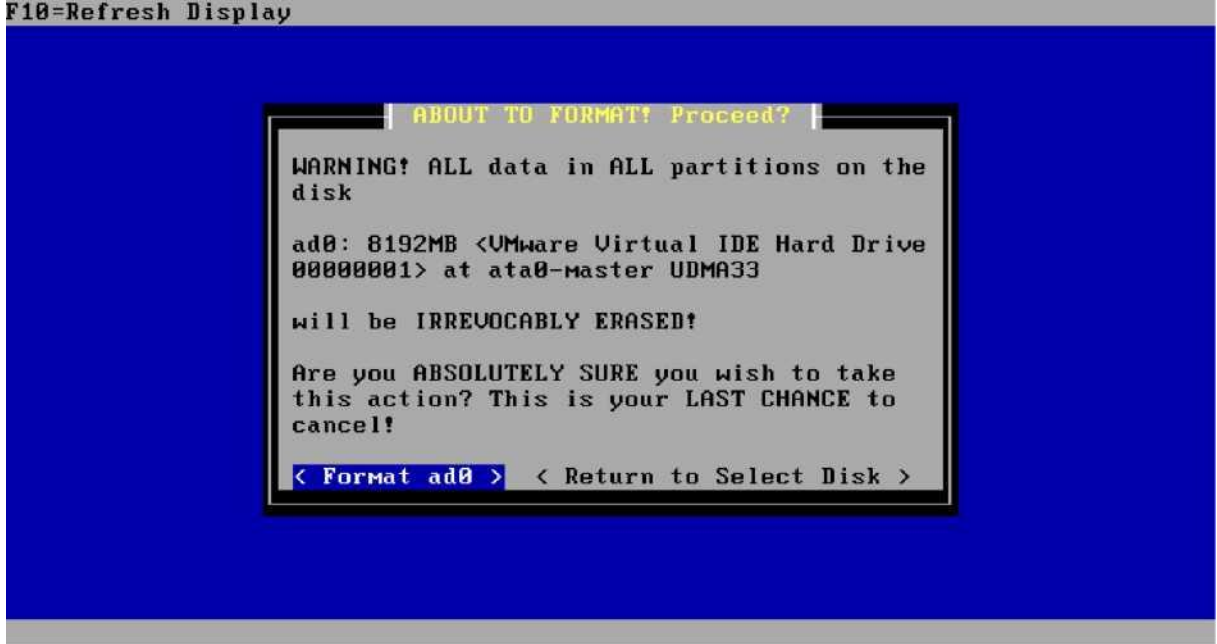
F10=Refresh Display



Enter the number of cylinders in this disk's geometry

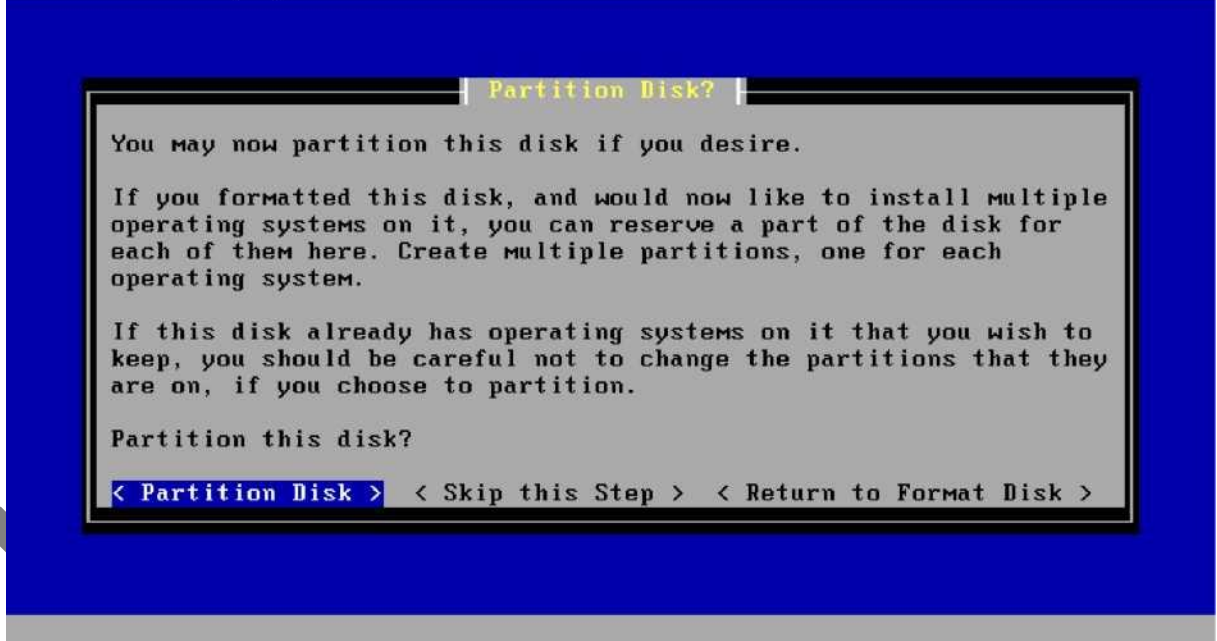
Select Geometry ekranında ne yaptığınız hakkında fikir sahibi değilseniz hiçbir şeyi değiştirmeden <Use this Geometry > diyerek devam edebilirsiniz veya farklı bir disk seçmek için < Return to Select Disk > seçeneği ile sabit disk seçim ekranına dönebilirsiniz.

F10=Refresh Display



Bu ekranda sabit diskimizi biçimlendirmek isteyip istemediğimizi son kez bize soruluyor. Bu işlemden sonra biçimlendirilen diskte yer alan tüm disk bölümlerindeki tüm bilgilerin silineceğine ve kurtarılamayacağına dair bir uyarılıyor. Sabit diskimizi biçimlendirmek istediğimizden emin isek < Format ad0 > seçeneği ile sabit diskimizi formatlıyoruz...

F10=Refresh Display



Sabit diskin biçimlendirilmesinin ardından disk bölümleri oluşturmak için disk bölümlenme aracı bizi karşılıyor. < Partition Disk > seçeneğini kullanarak sabit diskimiz bölümleyeceğiz.

F10=Refresh Display

Edit Partitions

Select the partitions (also known as 'slices' in BSD tradition) you want to have on this disk.

For Size, enter a raw size in sectors (1 gigabyte = 2097152 sectors) or a single '*' to indicate 'use the remaining space on the disk'.

Size (in Sectors) Partition Type Active?

[16776522] [FreeBSD] [X] < Ins > < Del >
< Add >

< Accept and Create > < Return to Format Disk >
< Revert to Partitions on Disk >

Bu aşamada sabit diskimizi istediğimiz gibi bölümleyebiliriz fakat biz en basit şekli ile kurulum yapmak için bize sunulan ilk seçeneği < Accept and Create > diyerek kabul edeceğiz. Tek disk bölümüne basit bir kurulum gerçekleştireceğiz.

F10=Refresh Display

Partition Anyway?

No changes appear to have been made to the partition table layout.

Do you want to execute the commands to partition the disk anyway?

< Yes, partition ad0 > < No, Skip to Next Step >
< No, Return to Edit Partitions >

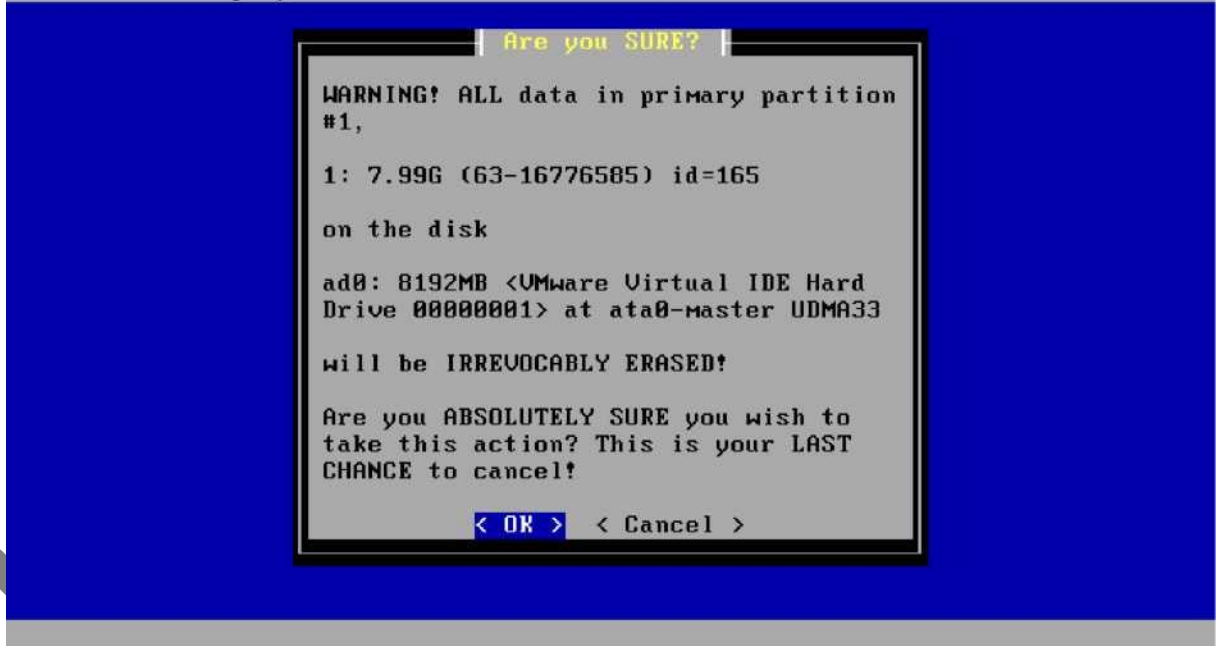
< Yes, partition ad0 > seçeneği ile sabit diskimizi bölümleyerek devam edelim.

F10=Refresh Display



Yukarıdaki "Select a Partition" ekranında kurulumun yapılacağı partiyon listesi seçilecektir. Bir önceki adımda oluşturduğumuz ad0 isimli disk bölümünü seçerek devam edelim.

F10=Refresh Display



Yukarıdaki "Are you SURE?" ekranında, işleme devam etmemiz durumunda birincil disk bölümünün onarılamaz şekilde silineceğini, yapmakta olduğumuz işlemden emin olup olmadığımızı soracaktır. Önemli verilerin bulunduğu bir diske güvenlik duvarı kurma gafletini göstermiyorsanız içiniz rahat bir şekilde < OK > seçeneğini seçerek devam edebilirsiniz. < OK > seçeneğini seçtiğinizde ad0 olarak adlandırılan birincil disk bölümü biçimlendirilecek ve aşağıdaki ekranda olduğu gibi disk bölümün nereye bağlanacağı sorulacaktır.

F10=Refresh Display

Select Subpartitions

Set up the subpartitions (also known as just 'partitions' in BSD tradition) you want to have on this primary partition.

For Capacity, use 'M' to indicate megabytes, 'G' to indicate gigabytes, or a single '*' to indicate 'use the remaining space on the primary partition'.

| Mountpoint | Capacity | | |
|------------|----------|-----------|---------|
| [/ |] [* |] < Ins > | < Del > |
| [swap |] [512M |] < Ins > | < Del > |
| | | < Add > | |

< Accept and Create > < Return to Select Partition >
< Switch to Expert Mode >

Press F1 for Help

Kurulum yazılımını 512 MB büyüklüğüne bir swap alanı ve diskin geri kalanını / (kök dizin) olarak kullanmamızı öneriyor. < Accept and Create > diyerek devam ediyoruz. Daha detaylı disk bölümlenmesi yapılabilirdi ancak şu an için amacımız en temel ve basit şekli ile pfSense kurmak olduğundan seçeneği ile tek disk bölümüne kurulum yapıyoruz.

Install Kernel(s)

You may now wish to install a custom Kernel configuration.

< Uniprocessor kernel (one processor) >

< Symmetric multiprocessing kernel (more than one processor) >

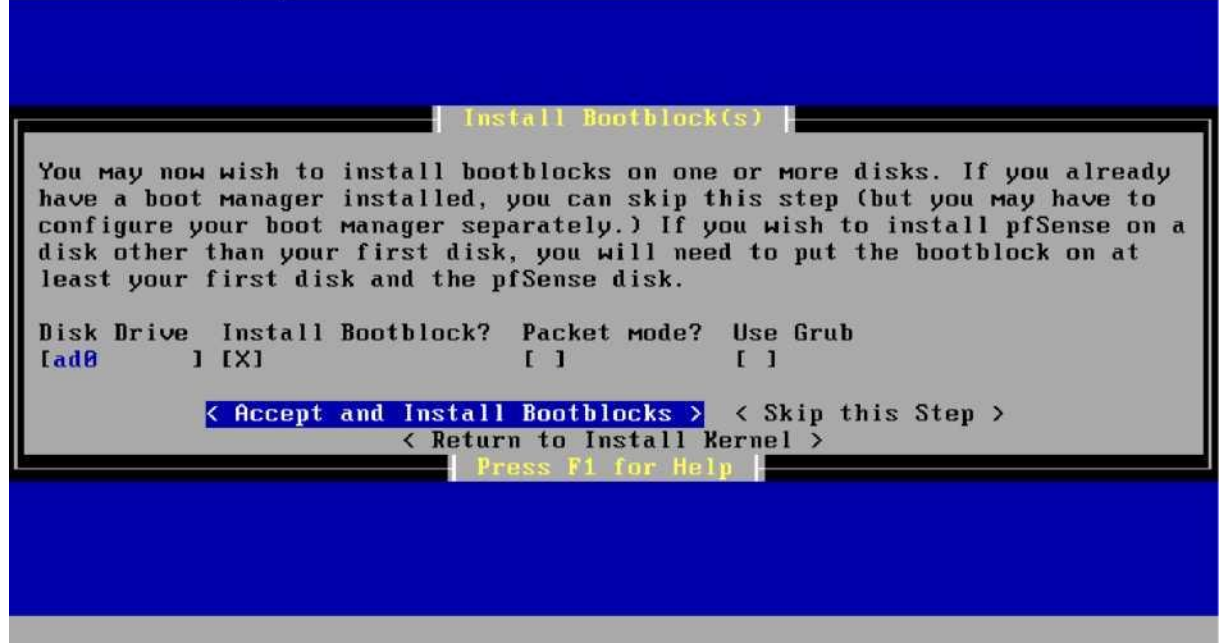
< Embedded kernel (no vga console, keyboard) >

< Developers kernel (includes GDB, etc) >

Press F1 for Help

Kurulum işlemi bittikten sonra kullanılacak olan çekirdek tipi sorulacaktır, tek işlemcili bir bilgisayara sahip iseniz <Uniprocessor kernel (one processor)> kullanabilirsiniz. Çok işlemcili bir donanım üzerinde kurulum yapıyorsanız <Symmetric multiprocessing kernel (more than one processor) > seçeneğini kullanabilirsiniz. Özel bir donanıma gömülü çalışacak bir kurulum söz konusu ise vga konsol ve klavye desteği olmayan <Embedded kernel (no vga console, keyboard)> seçeneğini kullanabilirsiniz. Eğer pfSense geliştiricisi olmaya karar vermişseniz içerisinde geliştirici araçları bulunan <Developers kernel> seçeneğini kullanabilirsiniz. Bizim örneğimizde <Uniprocessor kernel (one processor)> devam ediyoruz.

F10=Refresh Display



Bu adımda açılış yöneticisi kurulumu yapılacaktır. <Accept and Install Bootblocks> seçeneği ile ön tanımlı seçenekleri kullanmanız genellikle yeterli olacaktır. Bu seçeneğin sonrasında çeşitli işlemler otomatik olarak yapılacak ve sistemi reboot etmek isteyip istemediğiniz sorulacaktır. <Reboot> seçeneğini kullanarak yeni kurmuş olduğumuz pfSense sistemimiz başlatılabilir.

Sisteminiz yeniden başladığında aşağıdaki gib bir ekran karşınıza gelmişse pfSense sabit diskinizden çalışıyor olacaktır.



Herhangi bir bilgisayardan pfSense ana makinasına erişmek için size lazım olacak kullanıcı adı ve şifreyi unutmadan. Bunlar default olarak pfSense tarafından atanır. Ancak siz arzu ederseniz daha sonra değiştirebilirsiniz de. Kullanıcı adı: admin Şifreniz: pfsense

Yerel Ağın (LAN) IP Adreslerinin Ayarlanması

Sisteminiz yeniden açıldığında ekrana aşağıdaki gibi bir ekran gelir. Eğer gelmişse problem yok, devam edebilirsiniz. (Dikkat ederseniz bir önceki adımda kullanmış olduğumuz kurulum seçeneği olan 99 artık yok.) Yok eğer daha farklı bir ekranla karşılaşmışsanız bir yerlerde eksik/yanlış yapılan bir işlem var demektir.

```
*** Welcome to pfSense 1.2.3-RELEASE-pfSense on pfSense ***
LAN*      -> em0   -> 192.168.1.1
WAN*      -> em1   -> 10.0.0.249(DHCP)

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

Enter an option: █
```

Sizin yapmış olduğunuz kurulumda LAN ve WAN bacakları için atanan IP numaraları farklı olabilir, sorun değil. Yapacağınız değişikliklerin nereye etkileyeceğini bilmeniz yeterli. LAN sizin yerel ağınız. WAN ise modem aracılığı ile bilgisayarınıza gelen internet ağınız.

İsmail Kalkanca

Yerel ağınız ile ilgili ayarları yapabilmek için "pfSense console setup" menüsünden "Set LAN IP address" komutunu seçmelisiniz. Bunun için "Enter an option:" kısmına 2 yazıp ENTER'a basın.

```
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 2

Enter the new LAN IP address: 10.0.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24
```

Bu ekranda yerel ağımız için pfSense tarafından atanmış olan 192.168.1.1 IP adresini istediğimiz başka bir IP numarasıyla değiştiriyoruz. Burada dikkat etmemiz gereken bir nokta sistemimizin WAN bacağı ile LAN bacağına ait IP aralığı aynı IP takımından olamaz. Örneğin:

| AĞ AYAAĞI | OLMAZ | OLMAZ | OLMAZ | OLUR |
|-----------|------------|---------------|-----------------|-------------|
| LAN | 10.0.0.1 | 192.168.0.1 | 155.155.155.1 | 10.0.0.1 |
| WAN | 10.0.0.150 | 192.168.0.100 | 155.155.155.155 | 192.168.2.1 |

```
Enter an option: 2

Enter the new LAN IP address: 10.0.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN [y;n]? y
Enter the start address of the client address range: 10.0.1.10
Enter the end address of the client address range: 10.0.1.100

The LAN IP address has been set to 10.0.1.1/24.
You can now access the webGUI by opening the following URL
in your web browser:

http://10.0.1.1/

Press ENTER to continue.
█
```

Yukarıdaki resmi analiz edecek olursak:

Yerel ağımızın LAN bacağı için atadığımız yeni IP adresimiz 10.0.1.1, Alt ağ maskesi olarak (24,16 ya da 8 bit seçebiliyordim) 24 seçtim. Böylelikle ağımızdaki bilgisayarlar alt ağ maskesi alırken 255.255.255.0 alacaklar.

Daha sonra yerel ağımızda IP dağıtma işlemini otomatik yaptırabilmek için DHCP server'i "y" yazarak aktif hale getirdim.

Böylelikle her bir kullanıcı bilgisayarını için teker teker IP adresi girme derdim olmayacak.

Enter the start address of the client address range: 10.0.1.10

Enter the end address of the client address range: 10.0.1.100

Burada ise kullanıcı bilgisayarlarına hangi IP aralığından IP atanmasını istiyorsam onu yazdım. Ağımızda dışarıdan gelen misafirlere ait bilgisayarlar da olmak üzere toplamda 80~90 bilgisayar olacağını öngörürsek 10.0.1.10 ile 10.0.1.100 arası bana yetecektir. pfSense'in ilerleyen aşamalarında kısıtlamaları, hakları verirken bu IP aralığına göre tanımlamalar yapıp;"IP'si 10.0.1.10 ile 10.0.1.100 arasında olan bilgisayarlar MSN Messenger'a giremesin" gibi bir kural belirleyebileceğim. 10.0.1.1 adresi pfSense servera ait. Artık bundan sonra pfSense erişmek için http://10.0.1.1 adresini kullanacağım. 10.0.1.2 ile 10.0.1.9 arası ya da 10.0.1.101 ile 10.0.1.255 arası sizin tasarrufunuzda. Mesela kendi bilgisayarınıza ya da ağızda yönetici olarak görev yapan bir başka arkadaşınıza DHCP server için tanımladığınız IP aralığının dışında bir IP vererek tanımlayacağınız kuralların dışında kalmasını sağlayabilirsiniz.

Son olarak ENTER'e bastığınızda pfSense konsolu yeniden açılacak ve yaptığınız ayarlamaların yapıp-yapılmadığını gözlemleyebileceksiniz.

```
*** Welcome to pfSense 1.2.3-RELEASE-pfSense on pfSense ***
LAN* -> em0 -> 10.0.1.1
LAN* -> em1 -> 10.0.0.249 (DHCP)

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

Enter an option: █
```

İnternet Çıkışını Kontrol Etmek

pfSense makine üzerinde yapacaklarımızı tamamladık. Ancak makinamızın LAN ve WAN bacağında bir aksama ya da eksik olup-olmadığını öğrenebilmek için kontrol yapmamız gerekiyor. Bu kontrolü iç ağımızdan modeme, bir internet sitesine ping atarak yapabiliriz.”pfSense console setup” menüsünden”7”’yi seçerek ping atacağımız ekranı açıyoruz.

```
7) Ping host
8) Shell
9) Pftop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 7

Enter a host name or IP address: www.google.com

PING www.l.google.com (74.125.87.104): 56 data bytes
64 bytes from 74.125.87.104: icmp_seq=0 ttl=49 time=297.771 ms
64 bytes from 74.125.87.104: icmp_seq=1 ttl=49 time=288.445 ms
64 bytes from 74.125.87.104: icmp_seq=2 ttl=49 time=478.654 ms

--- www.l.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 288.445/354.957/478.654/87.558 ms

Press ENTER to continue.
█
```

Örneğimizde www.google.com adresini kullandım. Resimde de görüleceği üzere atılan 3 pingte sağlıklı bir şekilde çalıştı. Kayıp yok. Makinamız internete çıkıyor.

Aynı işlemi pfSense'nin yerel ağ üzerindeki olan bir bilgisayara ulaşıp-ulaşamadığını kontrol etmek için de kullanabilirsiniz. Ben örnekte kendi makinamın IP'sine ping atıyorum. Aşağıdaki resimde de görüleceği üzere yerel ağımdaki diğer bilgisayarına sorunsuz bir şekilde ping atabildim.

İsmail KÖK

Sonuç olarak pfSense makinamın LAN ve WAN bacakları sorunsuz bir şekilde çalışıyor.

```
7) Ping host
8) Shell
9) Pftop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 7

Enter a host name or IP address: 10.0.1.2

PING 10.0.1.2 (10.0.1.2): 56 data bytes
64 bytes from 10.0.1.2: icmp_seq=0 ttl=128 time=0.445 ms
64 bytes from 10.0.1.2: icmp_seq=1 ttl=128 time=0.278 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=128 time=0.219 ms

--- 10.0.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.219/0.311/0.445/0.097 ms

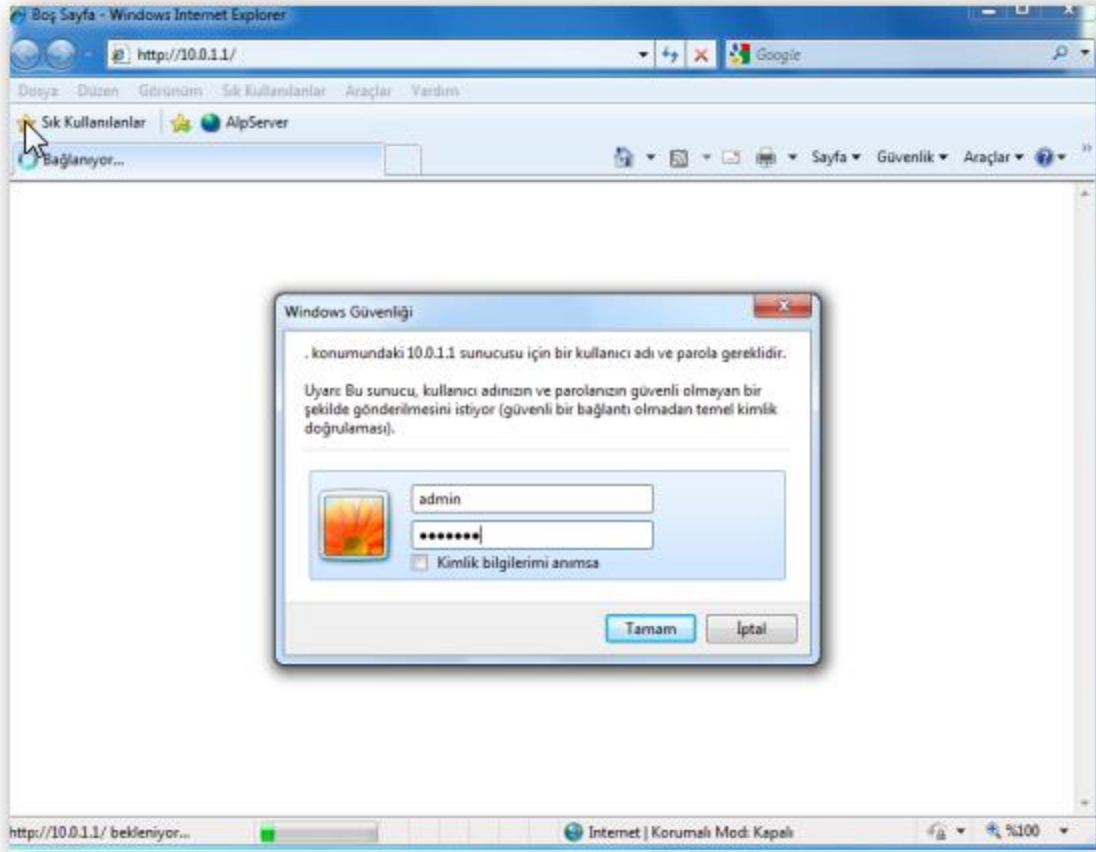
Press ENTER to continue.
█
```

pfSense'de Yapılacak Genel Ayarlar

pfSense'nin kurulumu tamam. Artık pfSense deryasına dalabiliriz. Bunun için yapmamız gereken tarayıcı ekranımızda pfSense'nin IP adresini yazarak ENTER'e basmak olacak. Bu IP adresini, kurulum tamamlandıktan sonra pfSense bize vermişti. Kullanıcı adı ve şifremizi de biliyoruz: admin-pfsense.

```
The GUI IP address has been set to 10.0.1.1
You can now access the webGUI by opening the following URL
in your web browser:
http://10.0.1.1/
Press ENTER to continue
█
```

pfSense makinamızın IP adresini tarayıcı ekranımıza yazıp ENTER'e bastıktan sonra giriş bilgilerimizi isteyen güvenlik penceresi açıldı. Burada pfSense makinanın kullanıcı adı ve şifresini girerek ayarlara başlıyoruz.



pfSense bir sonraki adımda "pfSense Setup Wizard"ı çalıştıracaktır.



'Next'i tıklıyoruz. Bu kez "General Information" penceresi açılacaktır.



Bu pencerede Hostname: kısmına pfSense makinanız için isim atayabilirsiniz. Domain: için bir site adresi verilebileceği gibi boşta bırakılabilir. Primary DNS Server: ve Secondary DNS Server: alanlarına internete çıkış yapacağımız DNS numaralarını girebiliriz. Eğer bu alan boş bırakılacak olursa sistem modemimiz üzerinden atanan DNS'ler ile internete çıkış yapacaktır. "Next"i tıklıyoruz.

Ekranaya gelen ařağıdaki "Time Server Information" penceresinde ise pfSense makine için saat dilimi olarak Timezone: Europe/Istanbul seçilebilir.



The screenshot shows a web browser window titled "FireWall.www.benimsitem.com - Time Server Information - Windows Internet Explorer". The address bar shows "http://10.0.1.1/wizard.php". The page content includes the pfSense logo and a form titled "Time Server Information". The form has a red header bar with the title. Below the header, there is a text input field for "Time server hostname:" with the value "0.pfsense.pool.ntp.org" and a dropdown menu for "Timezone:" with the value "Europe/Istanbul". A "Next" button is located below the form. The page also features a large watermark "ismail-salih" in the background.

Please enter the time, date and time zone.

| Time Server Information | |
|-------------------------|--|
| Time server hostname: | 0.pfsense.pool.ntp.org Enter the name of the time server. |
| Timezone: | Europe/Istanbul |

Next

"Next"i tıktatıyoruz

ismail-salih

Sonra yine "Next"e basarak "Local Area Network Information" penceresinin açılmasını sağlayalım.



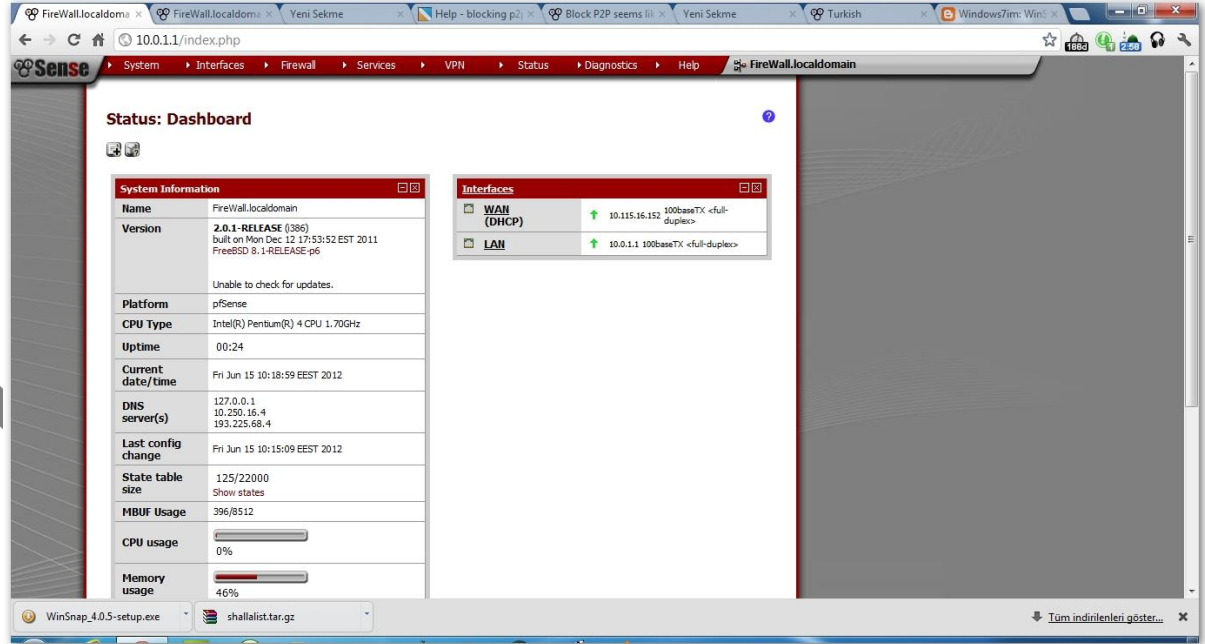
Yine "Next" i tıklıyoruz.



Sonraki "Set Admin WebGUI Password" ekranında yönetici şifremizi değiştirebiliriz. "Next" e tıkladığımızda "Reload configuration" ekranıyla ayarlarımız tamamlanmış olacak.



“Reload”i tıktıyoruz. pfSense sisteme yeniden giriş yapabilmemiz için kullanıcı adını ve şifremizi gireceğimiz ekranı getirir. Artık pfSense'miz kullanıma hazır.



“System Overview” ekranı pfSense'mizin ana sayfası. Bu ekran üzerinden sistemimizde yer alan CPU, RAM ve Disk kullanımları hakkında bilgi sahibi oluruz.

pfSense'de İçerik Filtreleme (Content Filter)

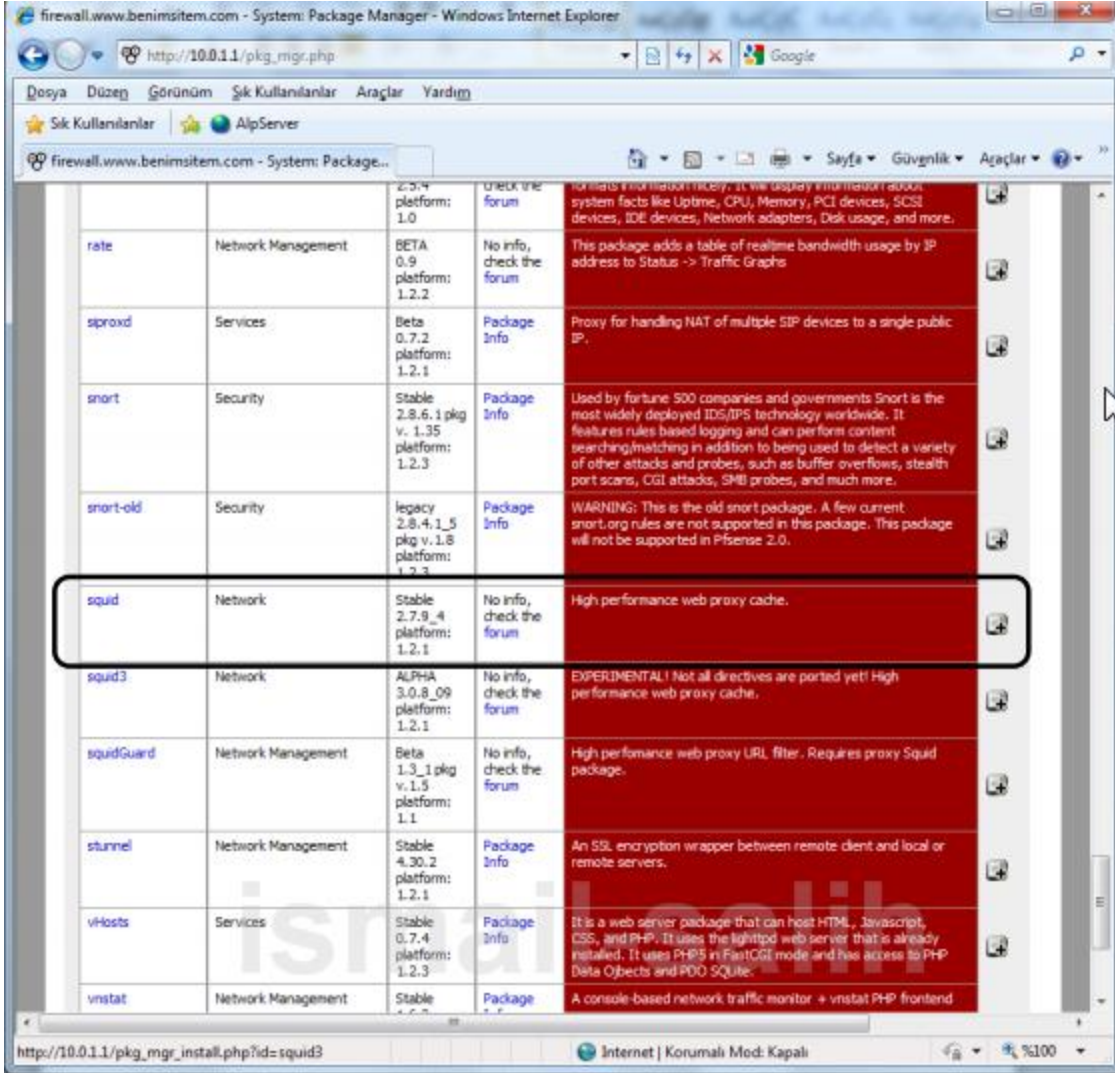
İster pfSense olsun, isterse diğerleri. Bütün güvenlik duvarı kurulumlarının temel amacı interneti paylaşdırmak/filtrelemek yani yönetmektir. Yönetmekle sorumlu olduğumuz ağımda internet dağıtımını kontrol altında tutmak, yoğun trafik çeken siteleri/programları bloklamak, bunun yanında kategorize edilmiş sitelere girişleri zamanlamak ya da tamamen yasaklamak temel amaçtır.

pfSense'de filtreleme yapmak için gelişmiş paketler mevcuttur. Yapılması gereken bu paketleri sisteme eklemek olacaktır. Bu işlem için kullanılacak araçlar squid ve squidGuard'dır. Esas bloklama işlemlerimizi tanımlayacağımız squidGuard'ı sistemimize yükleyebilmek için gerek şart squid'in kurulmasıdır. Squid kurulduktan sonra squidGuard'ın kurulumuna geçilebilir. pfSense'de squid Proxy server olarak çalışırken, squidGuard Proxy filter olarak işlem yapar.

İsmail Karaca

Squid Kurulumu

Bu işlem için önce pfSense'de System menüsü altında yer alan Packages komutunu kullanarak güvenlik duvarının desteklediği, kurulmaya hazır paketleri listeleyebilirsiniz.

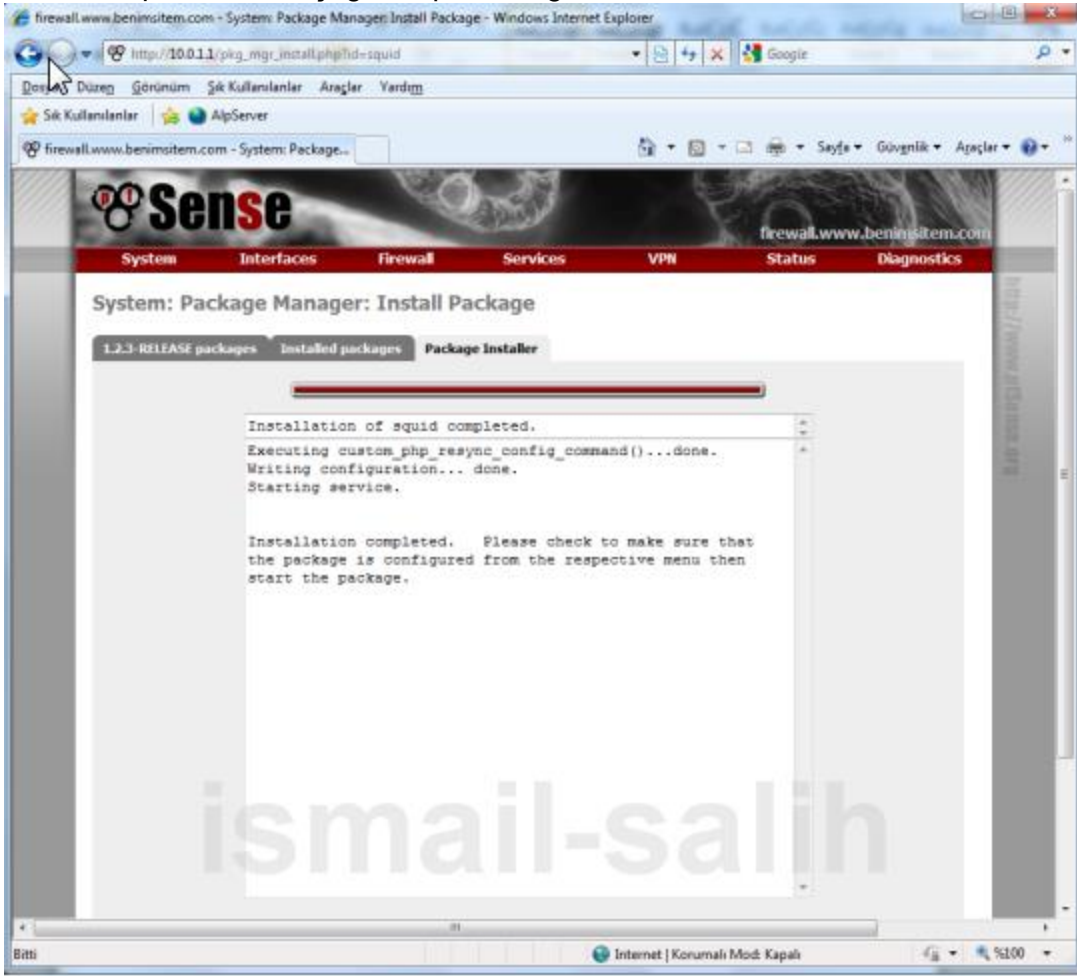


The screenshot shows the pfSense System Package Manager interface. The browser address bar displays 'http://10.0.1.1/pkg_mgr.php'. The page title is 'firewall.www.benimsitem.com - System: Package Manager - Windows Internet Explorer'. The interface includes a menu bar with 'Dosya', 'Düzen', 'Görünüm', 'Sık Kullanılanlar', 'Araçlar', and 'Yardım'. Below the menu is a search bar and a list of packages. The 'squid' package is highlighted with a black box. The table below shows the details of the packages:

| Package Name | Category | Version | Platform | Status | Description |
|--------------|--------------------|-----------------------------|-----------------|--------------------------|---|
| rate | Network Management | BETA 0.9 | platform: 1.2.2 | No info, check the forum | This package adds a table of realtime bandwidth usage by IP address to Status -> Traffic Graphs |
| sproxd | Services | Beta 0.7.2 | platform: 1.2.1 | Package Info | Proxy for handling NAT of multiple SIP devices to a single public IP. |
| snort | Security | Stable 2.8.6.1 pkg v. 1.35 | platform: 1.2.3 | Package Info | Used by fortune 500 companies and governments Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. |
| snort-old | Security | legacy 2.8.4.1_5 pkg v. 1.8 | platform: 1.2.1 | Package Info | WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in PfSense 2.0. |
| squid | Network | Stable 2.7.9_4 | platform: 1.2.1 | No info, check the forum | High performance web proxy cache. |
| squid3 | Network | ALPHA 3.0.8_09 | platform: 1.2.1 | No info, check the forum | EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache. |
| squidGuard | Network Management | Beta 1.3_1 pkg v. 1.5 | platform: 1.1 | No info, check the forum | High performance web proxy URL filter. Requires proxy Squid package. |
| stunnel | Network Management | Stable 4.30.2 | platform: 1.2.1 | Package Info | An SSL encryption wrapper between remote client and local or remote servers. |
| vHosts | Services | Stable 0.7.4 | platform: 1.2.3 | Package Info | It is a web server package that can host HTML, Javascript, CSS, and PHP. It uses the lighttpd web server that is already installed. It uses PHP5 in FastCGI mode and has access to PHP Data Objects and PDO SQLite. |
| vncstat | Network Management | Stable 1.0.0 | platform: 1.2.1 | Package Info | A console-based network traffic monitor + vncstat PHP frontend |

Bu liste içerisinde internet çıkışı cache'leyerek performans arttırımı sağlayacak olan squid'i sistemimize ekleyelim. Bunun için squid satırının hemen sağında yer alan + simgesine tıklamalısınız.

İnternetinizin ve makinanızın hızına göre 1~2 dk. / 3~5 dk. kadar bekleddikten sonra karşınıza kurulum raporu sunan aşağıdaki pencere gelecektir.



Kurulum başarı ile tamamlandı. Squid'e ulaşabilmek için Services menüsü kullanılacak. Ekranı yenilemek için F5'e basılabilir ya da sayfanın sol üst köşesindeki pfSense logosu tıklanabilir. Böylelikle yapılan son değişiklikler de sisteme dâhil edilecek ve biz squid'e ulaşabileceğiz.

Squid Ayarları

Services menüsünden Proxy server komutu seçildiğinde squid çalışacaktır. Bundan sonra sıra squid üzerinde yapılabilecek ayarlara geliyor.

Proxy server: General settings

| General | Upstream Proxy | Cache Mgmt. | Access Control | Traffic Mgmt. | Auth Settings | Local Users |
|---|---|---|----------------|---------------|---------------|-------------|
| Proxy interface | <input type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN | The interface(s) the proxy server will bind to. | | | | |
| 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 (;). | | | | |
| Enabled logging | <input checked="" type="checkbox"/> | This will enable the access log. Don't switch this on if you don't have much disk space left. | | | | |
| Log store directory | <input type="text" value="/var/squid/log"/> | The directory where the log will be stored (note: do not end with a / mark) | | | | |
| Log rotate | <input type="text"/> | Defines how many days of logfiles will be kept. Rotation is disabled if left empty. | | | | |
| Proxy port | <input type="text" value="3128"/> | This is the port the proxy server will listen on. | | | | |
| ICP port | <input type="text"/> | This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP. | | | | |
| Visible hostname | <input type="text"/> | This is the URL to be displayed in proxy server error messages. | | | | |
| Administrator email | <input type="text" value="kmktims@gmail.com"/> | This is the email address displayed in error messages to the users. | | | | |
| Language | <input type="text" value="Turkish"/> | Select the language in which the proxy server will display error messages to users. | | | | |
| Disable X-Forward | <input type="checkbox"/> | If not set, Squid will include your system's IP address or name in the HTTP requests it forwards. | | | | |
| Disable VIA | <input type="checkbox"/> | If not set, Squid will include a Via header in requests and replies as required by RFC2616. | | | | |
| What to do with requests that have whitespace characters in the URI | <input type="text" value="strip"/> | strip: The whitespace characters are stripped out of the URL. This is the behavior recommended by RFC2396. deny: The request is denied. The user receives an "Invalid Request" message. | | | | |

Proxy interface: LAN

Bu ifadeyle proxy serverimiz iç ağıımızı kontrol edeceğini ifade etmiş oluyoruz.

Allow users on interface: seçili

Proxy interface alanında seçilen arayüze ait tüm kullanıcıların proxy üzerinden sisteme dâhil olacağını ifade eder. Daha sonrasında squidGuard ile yapılacak tüm işlemlerin tüm kullanıcıları etkilemesi sağlanır.

Transparent proxy: seçili

Şeffaf proxy modu aktif hale getirildiğinde her bir kullanıcı makinası için tarayıcı ayarlarında teker teker ağ geçidi ve port tanımlamaya gerek kalmayacak, böylelikle külfetten kurtulmuş olacağız. Seçenek aktifken gönderilen tüm istekler 80 portu üzerinden proxy server'e iletilecektir.

Enabled logging: seçili

Bu seçenekle proxy üzerinden yapılan tüm çıkışların kaydı tutulacak.

Log store directory: /var/squid/log

Log'lar için kayıt pozisyonu belirlemiş olduk.

Proxy port: 3128

Administrator email: E-mail adresiniz

Custom Options:

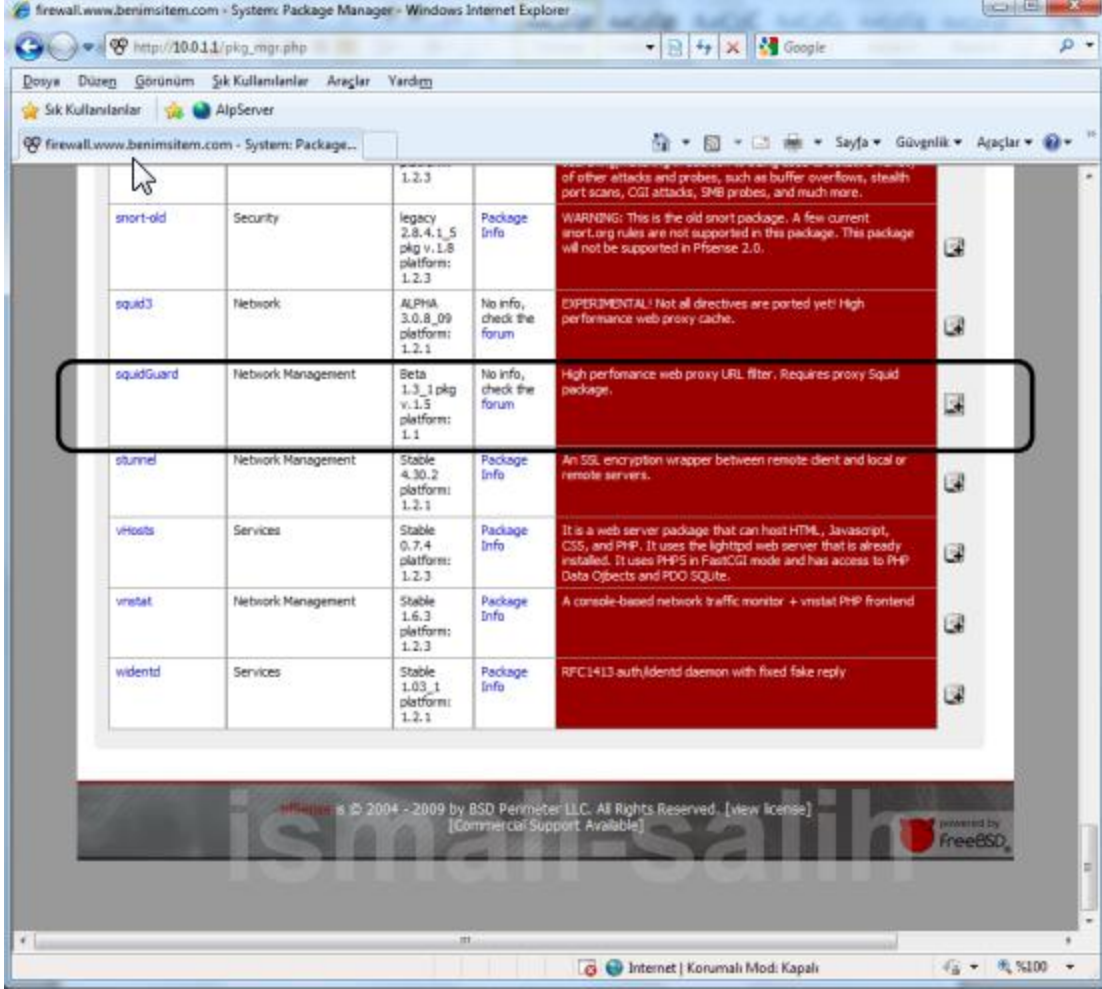
```
refresh_pattern windowsupdate.com/*\.(cab|exe) 4320 100% 43200
reload-into-ims;refresh_pattern
download.microsoft.com/*\.(cab|exe) 4320 100% 43200 reload-into-
ims;refresh_pattern au.download.windowsupdate.com/*\.(cab|exe)
4320 100% 43200 reload-into-ims;range_offset_limit -
1;redirect_program /usr/local/bin/squidGuard -c
/usr/local/etc/squidGuard/squidGuard.conf;redirector_bypass
on;redirect_children 3
```

Bu alana kopyalanacak yukarıdaki kodlarla herhangi bir makinadan yapılacak olan Windows güncellemesi cache'e alınacak ve daha sonra bir başka bilgisayar tarafından yapılacak güncelleme talebi internet üzerinden değil, cache'e alınan dosyalar yardımıyla yapılacaktır.

Böylelikle hem internet hızınızda bir azalma olmayacak, hem de daha hızlı bir güncelleme yapmış olacaksınız. Tercih e-râcidir. Arzu edilmezse yazılmayabilir.

SquidGuard Kurulumu

System menüsü içinde yer alan Packages komutu seçilerek aşağıdaki pencerenin açılması sağlanır.



| Package Name | Category | Version | Platform | Description |
|-------------------|--------------------|-----------------------------|----------|---|
| snort-old | Security | legacy 2.8.4.1_5 pkg v. 1.8 | 1.2.3 | of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in PfSense 2.0. |
| squid3 | Network | ALPHA 3.0.8_09 | 1.2.1 | EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache. |
| squidGuard | Network Management | Beta 1.3_1 pkg v. 1.5 | 1.1 | High performance web proxy URL filter. Requires proxy Squid package. |
| stunnel | Network Management | Stable 4.30.2 | 1.2.1 | An SSL encryption wrapper between remote client and local or remote servers. |
| vhosts | Services | Stable 0.7.4 | 1.2.3 | It is a web server package that can host HTML, Javascript, CSS, and PHP. It uses the lighttpd web server that is already installed. It uses PHP5 in FastCGI mode and has access to PHP Data Objects and PDO SQLite. |
| vrsstat | Network Management | Stable 1.6.3 | 1.2.3 | A console-based network traffic monitor + vrsstat PHP frontend |
| widentd | Services | Stable 1.03_1 | 1.2.1 | RFC1413 auth/identd daemon with fixed fake reply |

Bunun için squidGuard satırının hemen sağında yer alan + simgesine tıklamalısınız.

İsmail

İnternetinizin ve makinanızın hızına göre 1~2 dk. / 3~5 dk. kadar bekleddikten sonra karşınıza kurulum raporu sunan aşağıdaki pencere gelecektir.



Kurulum tamamlandı. Ancak squidGuard'a erişebilmek için ekranı yenilemek gerekecek. Bunun için F5 fonksiyon tuşuna basabileceğiniz gibi ana sayfanın sol üst köşesinde yer alan pfSense logosuna da tıklayabilirsiniz. Bu işlemden sonra squidGuard'a erişmek için Services menüsünde yer alan Proxy filter komutunu kullanabilirsiniz.

System Interfaces Firewall Services VPN Status Diagnostics

Proxy filter SquidGuard: General settings

General settings Default ACL Destinations Times Rewrites Log

Enable
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**

SquidGuard service state: **STOPPED**

Enable GUI log
Check this for enable GUI log.

Enable log
Check this for enable log of the proxy filter. Usually log used for testing filter settings.

Enable log rotation
Check this for enable daily rotate a log of the proxy filter. Use this option for limit log file size.

Blacklist options

Blacklist
Check this for enable blacklist

Blacklist proxy
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
Enter FTP, HTTP or LOCAL (pfSense) URL blacklist archive, or leave blank.

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available] powered by FreeBSD

Enable: squidGuard'i aktif hale getirebilmek için bu seçeneğin aktif olması gerekir. Squid ve squidGuard üzerinde yapılan değişikliklerin sisteme tanıtılabilmesi için 'Apply' düğmesine basılmalıdır. Log tutmayla ilgili olan seçeneklerin aktifleştirilmesi kullanıcıya bağlıdır. Sistemi etkilemez.

Eğer bu noktada sistemi ENABLE edecek olursanız tüm internet bağlantınız kesilecektir. Korkmayın!. Default sekmesinde yer alan Destination ruleset kısmını açarak Default Access [all] seçeneğinin yanında yer alan access açılır menüden allow seçeneğini seçin ve tekrar General settings sekmesine dönerek 'Apply' düğmesine basın. Artık tüm internet çıkışları serbest.

Proxy filter SquidGuard: Default

General settings Default ACL Destinations Times Rewrites Log

Default destination

Destination ruleset: (click)

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

Destination rules

Default access [all] access deny

Not to allow IP addresses in URL:

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: [int error page (enter error message)]

Select redirect mode here.
Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.
Options: ext:url:err page , ext:url:redirect , ext:url:as 'move' , ext:url:as 'found'.

Redirect info:

Enter external redirection URL, error message or size (bytes) here.

Spec: Use safe search engine:

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. Make sure that the search engines can, and others, it is recommended to prohibit.
Note: ! This option overrides 'Rewrite' setting. !

Rewrite: [none (rewrite not defined)]

Enter rewrite condition name for this rule, or leave blank.

Log:

Check this for log this item.

Save

Blacklist options kategorisi sistemimize kara listeleri başlıklar halinde (adult, oyun, şiddet, müzik, video, kumar, vb.) dâhil etmemizi sağlayan yerdir. Blacklist'i aktif hale getirmeden bu kategorileri sistemimize eklemek için Blacklist URL kısmını kullanacağız. Buraya <http://www.shallalist.de/Downloads/shallalist.tar.gz> adresini kopyalayıp **'Upload URL'** düğmesine basalım. Bu dosya sıkıştırılmış bir dosya olarak indirilip pfSense tarafından açılır ve kategoriler eklenir. İşlem biraz uzun sürecektir.

Yükleme işlemi tamamlandıktan sonra Default sekmesindeki kısım düğmesine basılarak açılacak olursa onlarca kategori eklendiği gözlemlenecektir.



Bu kategoriler içinde engellemek istediklerimizin access açılır listesinden “deny” seçeneğini seçmemiz yeterli olacaktır. Örneğin [blk_BL_violence] kategorisi “deny” yaptığımızda şiddet içerikli siteler engellenecektir. Bu listenin en altında bulunan Default access [all] seçeneği “allow” olmalı.

Bunu yapmakla:

Çağrılan internet sitesi squidGuard içinde işletilen kurallara göre yukarıdan aşağıya doğru “deny” yaptığımız kategorilere takılmadan geçtiyse, gösterilmesinde mahzur yok demektir; gösterilsin..

System Interfaces Firewall Services VPN Status Diagnostics

Proxy filter SquidGuard: Default

General settings Default ACL Destinations Times Rewrites Log

| | |
|----------------------------------|--|
| Default destination | <input type="text" value="url"/> Destination ruleset (click) |
| Not to allow IP addresses in URL | <input 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' 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="Bu siteye erişiminiz sistemin yöneticiniz tarafından kısıtlanmıştır. Eğer bu siteye erişmeniz gerekiyorsa sistemin yöneticisiyle iletişime geçin."/> Enter external redirection URL, error message or site (bytes) here. |
| Spec: Use safe search engine | <input 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. 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="none (rewrite not defined)"/> Enter rewrite condition name for this rule, or leave blank. |
| Log | <input checked="" type="checkbox"/> Check this for log this item. |

Save

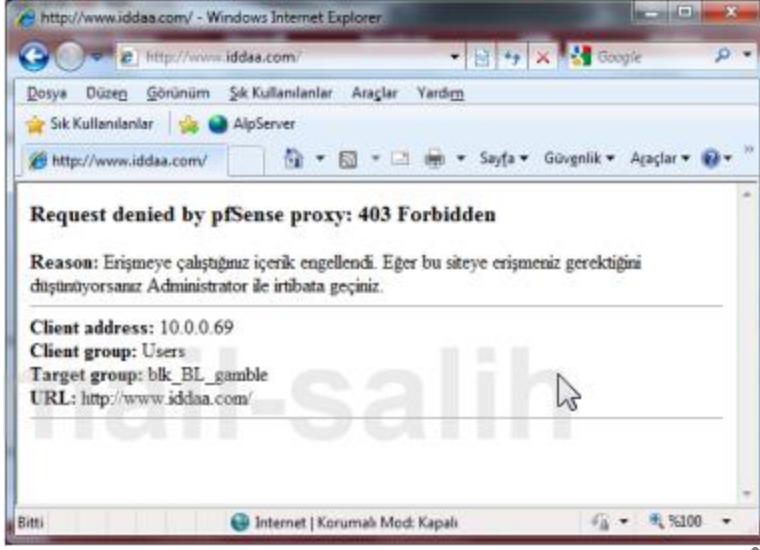
© 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support: Available] powered by freeBSD

Not to allow IP addresses in URL: İnternete girmek isteyen kişiler eğer IP adresi ile girmeye çalışırlarsa engel olacak, izin vermeyecek.

Redirect mode: Engellenen bir içerikle karşılaşıldığında ekranda ne gibi bir işlem yapılması gerektiğini burada belirtiriz. Burada seçebileceğimiz dört farklı seçenek vardır. Bunlar:

- **int error page (enter error message):** Redirect info kısmında belirleyeceğimiz hata mesajının gösterilmesini sağlar.
- * **int blank page:** Engellenen bir içerikle karşılaşıldığında boş bir sayfa görüntüler.
- **ext url err page (enter URL):** Harici bir hata sayfasına yönlendirmek için kullanılır.
- **ext url redirect (enter URL):** Başka bir internet sitesine yönlendirmek için kullanılır. Burada kendi işyerinize/kurumunuza ait web siteniz varsa o adrese yönlendirebilirsiniz.
- **ext url move (enter URL):** İsteği alternatif olarak bir başka sayfaya taşımak için kullanılır.
- **ext url found (enter URL):** Normal istek sayfa açılıyormuş gibi bir başka sayfanın açılmasını sağlar.

İşlem tamamlandıktan sonra aktif sayfanın altında yer alan düğmesine basalım. Bütün bu ayarlamalar ve kayıt işlemi bittikten sonra General settings sekmesinden düğmesine tıklarsak sistemimiz bizim ayarlarımızla iş yapar hale gelecektir. Örneğin mahzurlu bir siteye giriş yapmaya çalıştım ve karşıma gelen pencere şu oldu



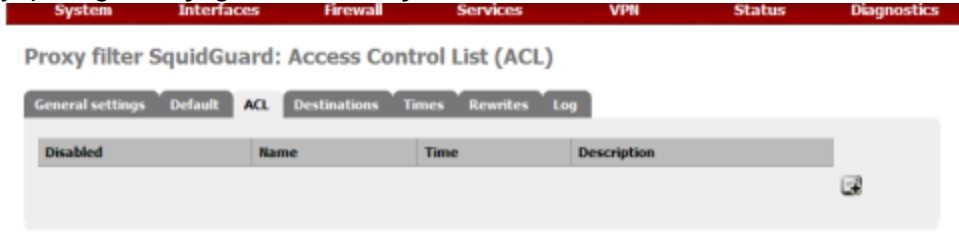
Sistemimiz çalışıyor.

İsmail Karaca

İçerik Filtrelemede Kullanıcıları Gruplandırma

Şu zamana kadar yapmış olduğumuz ayarlar sayesinde internet çıkışlarımızı kontrol altına aldık. Ancak bu durum isteklerimizi tam olarak karşılamaya yetmiyor. İsterim ki; kendim ya da yerel ağımızda yönetici pozisyonunda olanlar internete kısıtlaması olmadan girerken aynı zamanda diğer kullanıcılardan bir kısmı mesai saatleri içinde sohbet, müzik sitelerine giremesin. Diğer kısmı ise video sitelerine erişemesin ama müzik sitelerine girebilsin. Bu ve benzeri kontrolleri pfSense ile yapabilmek oldukça kolay.

Bunun için öncelikle Services menüsünden Proxy filter komutunu çalıştırın. Ekrana gelecek olan pencere üzerinde ACL (Access Control List) sekmesine tıkladığınızda işlemlerinizi yapacağınız aşağıdaki ekran açılacaktır.



İsmail

Bu ekran üzerinde + simgesine tıklayarak grup tanımlamalarımızı başlatabiliriz. Aşağıdaki ekran açılacaktır.

System Interfaces Firewall Services VPN Status Diagnostics

Proxy filter SquidGuard: Access Control List (ACL): Edit

General settings Default **ACL** Destinations Times Rewrites Log

Disabled
Check this for disable this ACL rule.

Name:
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].

Order:
Select the new position for ACL item. ACL are evaluated on a first-match source basis.
Note: Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
For example: ACL with single (or short range) source ip 10.0.0.15, must be placed before ACL with more large ip range 10.0.0.0/24

Source IP addresses and domains:
Enter source IP address or domain or "username" here. For separate use space.
Example:
ip: 192.168.0.1 or subnet 192.168.0.0/24 or subnet 192.168.1.0/255.255.255.0 or range 192.168.1.1-192.168.1.10
domain: foo.bar match foo.bar or *.foo.bar
username: user:1

Time:
none (time not defined)
Enter time name in current which this rule permitted.

Destination:
Destination ruleset (click) [x] [y]

Not to allow IP addresses in URL
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:
none
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:
Enter external redirection URL, error message or size (bytes) here.

Spec: Use safe search engine
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. Make sure that the search engines can, and others, it is recommended to prohibit.
Note: ! This option overrides 'Rewrite' setting. !

Rewrite:
none (rewrite not defined)
Enter rewrite condition name for this rule, or leave blank.

Overtime rewrite:
none (rewrite not defined)
Enter rewrite condition name for this rule, or leave blank.

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

Log
Check this for log this item.

Save Cancel

Disabled: Name kısmında vereceğimiz isim altında saklanacak olan bu ayarları devre dışı bırakmak istediğimizde bu alanı kullanırız. Böylelikle tanımladığımız kuralları silmeye gerek kalmadan devre dışı bırakmış oluruz.

Name: Tanımlayacağımız ACL'e isim atamasını bu alan üzerinden yapacağız. Bu alanda Türkçe karakterler kullanılmamalı.

Source IP addresses and domain: Burada gruba dâhil edeceğimiz IP adreslerini araya boşluk koyarak yazmamız gerekiyor. Eğer bu IP aralığı bir küme oluşturuyorsa araya – koyarak bu işlemi yapabiliriz. Örneğin;
10.0.1.2-10.0.1.9 10.0.1.159-10.0.1.200 10.0.1.220 10.0.1.254

Time: Bu seçenekteki açılır menüde Proxy filter'in (squidGuard'a ait) Times sekmesinde tanımlamış olduğunuz zaman çizelgelerinin bir listesini bulabilirsiniz. (Zaman çizelgesi oluşturma konusu daha sonra işlenecektir.) Mesela mesai saatlerini belirleyebilir, hafta sonu-hafta içi ya da tatil günleri için özel kullanım zamanlamaları oluşturabilirsiniz.

Destination: Burada Default sekmesine yaptığımız ayarlara benzer kısıtlama yada izinler tanımlayabiliriz. Dikkat ederseniz burada kategoriler çift sıra şeklinde sıralanmışlar. Bunlardan Destination rules tanımladığınız zaman dilimlerinde, Destination rules in overtime ise bu zaman dilimleri dışında aktif olacak ayarlardır.

Eğer tanımlamasını yaptığınız bu grubun izin verdiğiniz zaman diliminin dışında kalan zamanlarda internet çıkışlarını kesmek istiyorsanız Destination rules in overtime kısmında yer alan Default Access [alil seçeneğini "deny" yapmanız yeterli olacaktır

Burada aklınıza şöyle bir soru gelebilir:

"Biz Proxy filter'in (squidGuard'a ait) Default sekmesinde bazı kısıtlamalar yapmıştık. Burada da ayrıca bir kısıtlama işlemi yaptık. Acaba bir orda, bir burada yaptığımız tanımlamalar karşılıklıya neden olmaz mı ? pfSense tanımladığım hangi kuralı çalıştıracak ?"

pfSense için her zaman tanımladığınız ACL'lerin önceliği vardır. Öncelikle burada yaptığınız ayarlar uygulanır. Dolayısı ile ACL içinde kısıtlanmış bir kategoride yer alan herhangi bir site Default sekmesinde izin verilmiş de olsa gösterilmeyecektir. İşte bundan dolayı Default sekmesinde yer alan Destination ruleset kısmındaki yer alan tüm kısıtlama işlemleri iptal edilebilir.

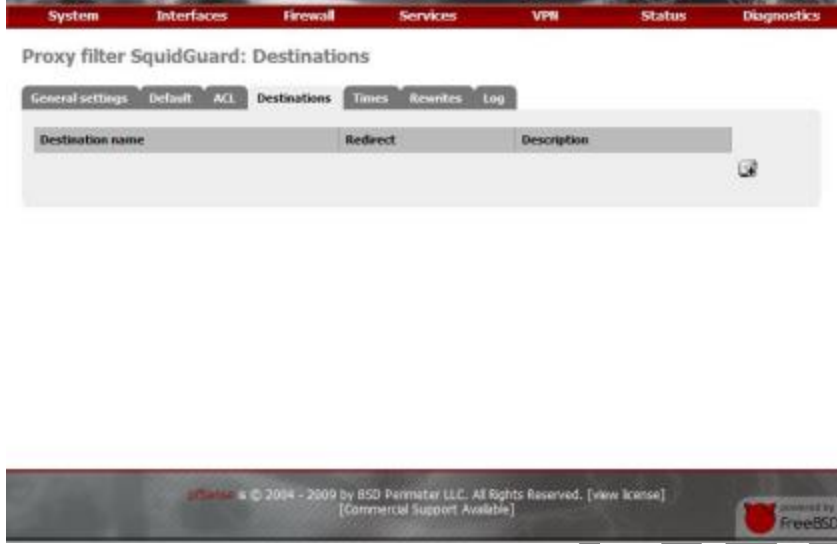
Not to allow IP addresses in URL: İnternete girmek isteyen kişiler eğer IP adresi ile girmeye çalışırlarsa engel olacak, izin vermeyecek.

Redirect mode: Engellenen bir içerikle karşılaşıldığında ekranda ne gibi bir işlem yapılması gerektiğini burada belirtiriz. Burada seçebileceğimiz altı farklı seçenek vardır. Bunlar:

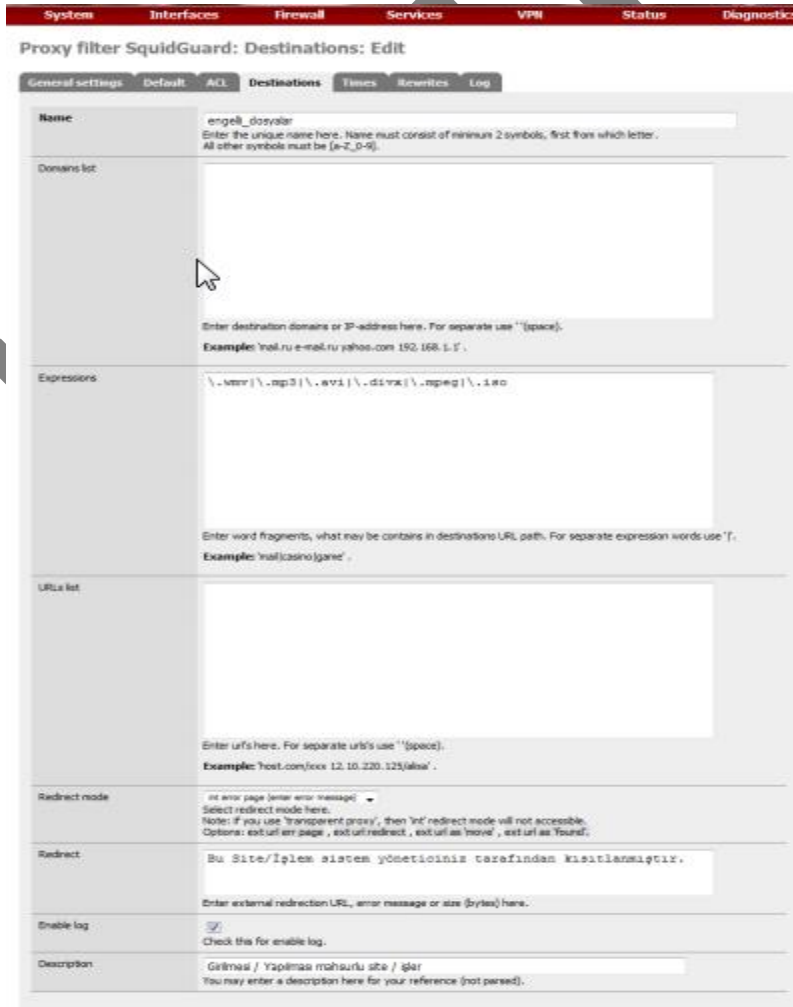
- **int error page (enter error message):** (Redirect info kısmında belirleyeceğimiz) hata mesajının gösterilmesini sağlar.
- **int blank page:** Engellenen bir içerikle karşılaşıldığında boş bir sayfa görüntüler.
- **ext url err page (enter URL):** Harici bir hata sayfasına yönlendirmek için kullanılır.
- **ext url redirect (enter URL):** Başka bir internet sitesine yönlendirmek için kullanılır. Burada kendi işyerinize/kurumunuza ait web siteniz varsa o adrese yönlendirebilirsiniz.
- **ext url move (enter URL):** İsteği alternatif olarak bir başka sayfaya taşımak için kullanılır.
- **ext url found (enter URL):** Normal istek sayfa açılıyormuş gibi bir başka sayfanın açılmasını sağlar.
- **Spec: Use safe search engine:** Çocukların kontrol dışı arama motorları tarafından mahzurlu içeriğe yönlendirilmesini engellemek için bu seçenek aktif hale getirilebilir. Böylelikle güvenli sörf sağlanmış olur. Şimdi Google, Yandex, Yahoo, MSN Live Search tarafından desteklenen bu özellik eğer "Rewrite" ayarı aktifse devre dışı kalır. İşlem tamamlandıktan sonra aktif sayfanın altında yer alan **Save** düğmesine daha sonra General settings sekmesinden **Apply** düğmesine basılırsa sistemimiz son yaptığımız değişiklik ve ayarları sistemde işler hale getirecektir. Bundan sonrası için istediğiniz kadar kullanıcı grubu tanımlayabilir, bu gruplara ait farklı farklı kısıtlamalar yapabilirsiniz.

İçerik Filtrelemede Dosya Uzantılarına Göre Engelleme

Yukarıdaki sayfalarda anlatılanlarla kategorilere ayrılmış siteleri kolaylıkla engelleyebildik. Ancak sadece siteleri engellemek için bir kısmı. İşin diğer kısmında internet üzerinde ulaşılmasını istemediğimiz dosya uzantılarına da kota koymak var. Bu işlem için önce Services menüsünde yer alan Proxy filter komutu, daha sonra açılan pencereden Destinations sekmesi tıklanır. Ekran aşağıdaki gibi bir pencere gelecektir.



Bu pencere üzerinden + simgesine tıklayarak yeni bir kural oluşturabiliriz. Bunun için aşağıdaki pencereyi ve üzerinde yapabileceğimizi gözden geçirelim.



Domain list: Burada bütün içeriğiyle birlikte engellemek ya da engelini kaldırmak istediğimiz internet adreslerini girebiliriz. Örneğin bu alana www.falancasite.com adresini yazdıysak pfSense bu site altında yer alan www.falancasite.com/gunluk kategorisine girişe de izin vermeyecek ya da verir hale gelecektir.

Buradaki "engellemek ya da engelini kaldırmak", "giriş izni vermek ya da vermemek" şartı ACL sekmesinde yapmış olduğumuz grup ayarlamalarında Destinations rules kısmında "allow" ya da "deny" yapmamıza göre değişir. "allow" yaparsak bu adreslere izin verilir, "deny" yaparsak blokaj uygulanır.

Expressions: Siteler üzerinde yer alan farklı farklı uzantılardaki dosyalara erişime engel koymak (bu işlem için yukarıda anlatılan "deny" yapma işlemi uygulanmalı) istediğimizde bu alana yazabiliriz. Dosya uzantıları tanımlanırken ".wmv" formatı uygulanır. Birden fazla dosya uzantısı yazılacaksa araya "|" işareti konmalıdır. Örneğin;

.wmv|.iso|.zip|.rar|.avi|.mpg|.exe

URLs list: Bir internet sitesine komple değil de sadece o site altında yer alan bir kategoriye blokaj uygulamak istediğimizde bu alanı kullanabiliriz. Erişimi iptal edilecek sayfa ya da kategorinin tam adresi bu alana yazılarak işlem tamamlanabilir. Örneğin;
www.falancasite.com/gunluk

Redirect mode: Engellenen bir içerikle karşılaşıldığında ekranda ne gibi bir işlem yapılması gerektiğini burada belirtiriz. Burada seçebileceğimiz altı farklı seçenek vardır.

Bunlar:

- **int error page (enter error message):** (Redirect kısmında belirleyeceğimiz) hata mesajının gösterilmesini sağlar.
- **int blank page:** Engellenen bir içerikle karşılaşıldığında boş bir sayfa görüntüler.
- **ext url err page (enter URL):** Harici bir hata sayfasına yönlendirmek için kullanılır.
- **ext url redirect (enter URL):** Başka bir internet sitesine yönlendirmek için kullanılır. Burada kendi işyerinize/kurumunuza ait web siteniz varsa o adrese yönlendirebilirsiniz.
- **ext url move (enter URL):** İsteği alternatif olarak bir başka sayfaya taşımak için kullanılır.
- **ext url found (enter URL):** Normal istek sayfa açılıyormuş gibi bir başka sayfanın açılmasını sağlar.

Redirect: Redirect mode alanında seçtiğiniz seçeneğe göre buraya bir mesaj ya da internet adresi girebilirsiniz.

Enable log: Bu ayarlarla ve ayarların çalışması esnasında log tutulup-tutulmayacağı bu alanda belirtilir.

Descripton: Bu tanımlamalarla ilgili açıklama cümlesi yazılabilir. Arzu edilirse boş olarak da bırakılabilir

Bütün bu ayarlar yapıldıktan sonra önce **Save** düğmesine daha sonra General settings sekmesinden **Apply** düğmesine basılmalıdır. Ki ayarlarımız çalıştırılsın

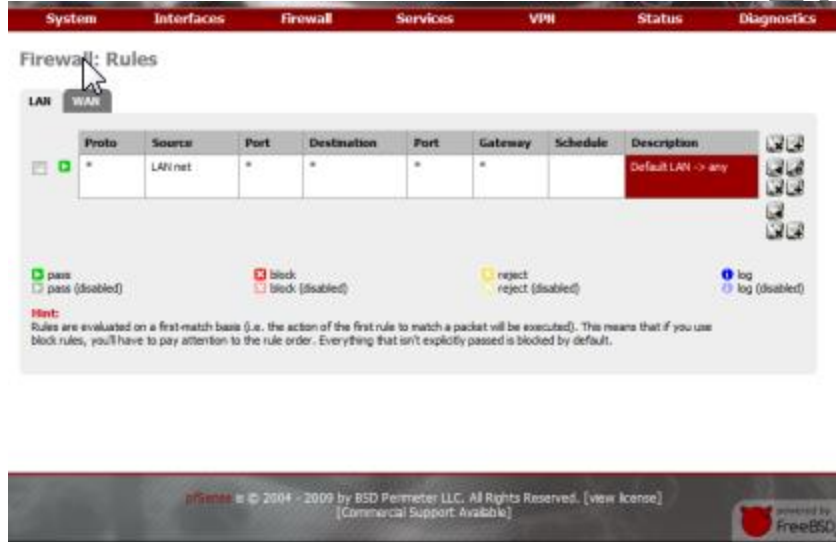
pfSense'de MSN Messenger Engelleme

Günümüzde dünya genelinde çok yaygın bir şekilde kullanılmakta olan MSN Messenger, kullanım esnasında sürekli birilerine laf yetiştirme durumunda olmayı gerektirdiğinden çalışılan ortamlarda konsantrasyon eksikliği, verimsizlik gibi olumsuz etkiler oluşturmaktadır. Hal böyle olunca çoğu firma/kurum bu anlık ileti programının kullanılmasını istememektedir. İşte tam da bu noktada bize düşen MSN Messenger'in yerel ağımızda kullanımını kısıtlamaktır. Hem programın çalışmasını hem de web üzerinden erişimini kısıtlayabilmek için pfSense'de bir dizi işlem yapmamız gerekecek.

Öncelikle bilmemiz gereken ham bilgi:

MSN Messenger sunucularına bağlanıp iletişimini gerçekleştirebilmek için; TCP/UDP-901, TCP/UDP-1863 ve TCP-6891/6900 arasındaki portları kullanır. Bu portlar üzerinden iletişim engelledikten sonra son olarak web üzerinden girişe de engel olmak için Proxy filter üzerinde tanımlama yapmamız gerekecek.

Yukarıda belirtilen portları bloklamak için Firewall menüsü altında yer alan Rules komutu çalıştırılmalıdır. Ekranı gelen pencere üzerinden önce LAN sekmesi, daha sonra + seçilerek blok tanımlamalarına başlayabiliriz



Firewall: Rules: Edit

| | |
|------------------------|---|
| Action | Block <small>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. Reject only works when the protocol is set to either TCP or UDP (but not TCP/UDP) below.</small> |
| Disabled | <input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small> |
| Interface | LAN <small>Choose on which interface packets must come in to match this rule.</small> |
| Protocol | TCP/UDP <small>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</small> |
| Source | <input type="checkbox"/> not <small>Use this option to invert the sense of the match.</small> Type: any Address: [redacted] / 31 <input type="button" value="Advanced"/> - Show source port range |
| Source OS | OS Type: any <small>Note: this only works for TCP rules</small> |
| Destination | <input type="checkbox"/> not <small>Use this option to invert the sense of the match.</small> Type: any Address: [redacted] / 31 |
| Destination port range | from: (other) [redacted] 901 to: (other) [redacted] 901 <small>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</small> |
| Log | <input type="checkbox"/> Log packets that are handled by this rule <small>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).</small> |
| Advanced Options | <input type="button" value="Advanced"/> - Show advanced options |
| State Type | <input type="button" value="Advanced"/> - Show state |
| No XMLRPC Sync | <input type="checkbox"/> <small>HINT: This prevents the rule from automatically syncing to other CARP members.</small> |
| Schedule | none <small>Leave as 'none' to leave the rule enabled all the time. NOTE: schedule logic can be a bit different. Click here for more information.</small> |
| Gateway | default <small>Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.</small> |
| Description | <input type="text"/> <small>You may enter a description here for your reference (not parsed).</small> |

Action: Tanımladığımız kuralda ne yapılacağını belirlediği kısımdır. Bu alandan Block ifadesini seçiyoruz.

Disabled: Yazılan kuralın geçici olarak kullanılmaması halinde kuralı tamamen silmek yerine pasif hale getirmemizi sağlar

Interface: Kuraldan hangi ara yüzün etkileneceği seçilir. Biz yerel ağımızda işletilecek bir kural tanımlayacağımız için LAN seçilmeli.

Protocol: Kural için geçerli olacak protokol seçilir.

Source: Kaynak olarak LAN, WAN, VPN ya da tekil olarak belirli bir ip seçebiliriz.

Destination: Kuralın hedefinin seçileceği kısımdır.

Destination Port Range: Port aralığının girileceği kısımdır.

Log: Tanımlanan kural için log tutulmasını sağlar.

Advanced Options: Bu seçenekte bağlantı sınırlama, maksimum bağlantı gibi seçenekler mevcut.

State Type: Yine ekstra özellikler tanımlayabileceğimiz kısım.

Schedule: Tanımladığımız kuralın hangi zaman dilimlerinde uygulanacağını belirleyebiliriz. Bu zamanlama ayarları kural yazılırken değil, kural yazılmadan önce Firewall menüsü altındaki Schedule kısmından tanımlanır.

Gateway: Kuraldan etkilenecek kullanıcılar için ayrı bir ağ geçidi tanımlayabiliriz.

Description: Kural için tanımlama girebileceğimiz kısım. Örneğin; MSN Messenger Yasak

Port block için bütün kurallarımızı tanımladıktan sonra kural ekranımız aşağıdaki gibi görünecektir.

| Proto | Source | Port | Destination | Port | Gateway | Schedule | Description |
|---------|---------|------|----------------------|-------------|---------|----------|-----------------------------|
| TCP/UDP | * | * | 192.168.0.0/24 (MSN) | * | * | | MSN Messenger Yasaklama - 3 |
| TCP | * | * | * | 6881 - 6900 | * | | MSN Messenger Yasaklama - 2 |
| TCP/UDP | * | * | * | 901 | * | | MSN Messenger Yasaklama - 1 |
| * | LAN net | * | * | * | * | | Default LAN -> any |

© 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

pfSense'de tanımlanan kurallar işletilirken yukarıdan aşağıda doğru bir sıralama takip edilir. Hal böyle olunca yaptığımız kısıtlamalar –üstteki resimde de görüleceği üzere- LAN net için tanımlanan tüm geçiş haklarının üstünde sıralanmalıdır. Eğer LAN net seçeneği bu sıralamada en üstte olursa bizim işletilmesini istediğimiz kurallara sıra gelmeden bu kuralın gereği yapılacak ve bütün portlardan geçiş hakkı verecektir.

MSN Messenger'in kullandığı portlar ve adresler için <http://support.microsoft.com/kb/927847> adresindeki makaleye bakılabilir.

Bu yapılandırmadan sonra MSN Messenger'a girmeye çalıştığınızda aşağıdaki gibi bir hata mesajıyla karşılaşacaksınız.

Oturum açın:
Windows Live Messenger

Windows Live Messenger oturumunuzu açamıyoruz
Hizmet geçici olarak kullanılmadığından Windows Live Messenger oturumu açılmadı. Lütfen daha sonra yeniden deneyin.
Daha fazla bilgi edinin...

Ayrıntıları göster

Yeniden Dene İptal

Oturum aç İptal

Windows Live ID'niz yok mu? Kaydolun

Günlük bildirimleri Kullanım koşulları Sunucu durumu Hakkında

MSN Messenger'in kullanabileceği PORT'ları yasakladık. Artık bundan sonra kullanıcılar MSN bağlantısı yapamayacaklar. Fakat MSN Messenger'a bağlanmak isteyen kullanıcılar bir diğer yöntem olan HTTP PORT'unu (80 portu) kullanarak internet siteleri üzerinden bağlantı yapmayı deneyeceklerdir. Bunu engellemedin yolu ise Services menüsü içinde yer alan Proxy server komutunu çalıştırdıktan sonra açılan pencereden Access Control sekmesini tıklamak ve Blacklist kategorisine MSN Messenger'in kullandığı adresleri girmek olacaktır.

Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives set in this page.

Banned host addresses

Enter each IP address on a new line that is not to be allowed to use the proxy.

Whitelist

Enter each destination domain on a new line that will be accessible to the users that are allowed to use the proxy. You also can use regular expressions.

Blacklist

207.46.110.16
207.46.110.13
207.46.110.3
*/gateway/gateway.dll
*avos.microsoft.com
*rad.msn.com

Enter each destination domain on a new line that will be blocked to the users that are allowed to use the proxy. You also can use regular expressions.

External Cache-Managers

Enter the IPs for the external Cache Managers to be allowed here, separated by semi-colons (;).

Save

İsmail K...
...raça

pfSense'de Facebook Engelleme

SquidGuard içinde yapacağımız tanımlamalarla filtreleme yaptırabiliriz. Bunun için Services menüsünde yer alan Proxy filter komutunu çalıştırdıktan sonra Destinations sekmesine tıklayalım. Burada + düğmesine basarak ,Facebook engelleme' tanımlamalarına başlayabiliriz.

Proxy filter SquidGuard: Destinations: Edit

General settings Default ACL Destinations Times Rewrites Log

Name: facebook_engelle
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].

Domains list

Enter destination domains or IP-address here. For separate use ^ (space).
Example: !nat.ru e-mail.ru yahoo.com 192.168.1.1

Expressions: facebook|tr.facebook

En fazla 16 karakterden oluşacak bir isim belirledikten sonra (Türkçe karakterler, boşluk karakteri kullanılmamalı) Expressions kısmına "facebook|tr.facebook" şeklinde bir ifade giriyoruz. İşlemi kaydettikten sonra Destinations ana penceresine döneriz.

Proxy filter SquidGuard: Destinations

General settings Default ACL Destinations Times Rewrites Log

| Destination name | Redirect | Description |
|------------------|----------|-------------|
| facebook_engelle | | |

Kuralımız tanımlanmış durumda. Bundan sonra ACL sekmesine tıklararak tanımlayacağımız kullanıcı grubuna burada tanımlamış olduğumuz ,facebook_engelle' kuralını ,deny' olarak tanımlayacağız.

Proxy filter SquidGuard: Access Control List (ACL): Edit

General settings Default ACL Destinations Times Rewrite Log

Disabled Check this for disable this ACL rule.

Name Users
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].

Order
Select the new position for ACL item. ACL are evaluated on a first-match source basis.
Note: Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
For example:
ACL with single (or short range) source ip 10.0.0.15, must be placed before ACL with more large ip range 10.0.0.0/24

Source IP addresses and domains
10.0.1.10-10.0.1.100
Enter source IP address or domain or "username" here. For separate use space.
Example:
ip: 192.168.0.1 or subnet 192.168.0/24 or subnet 192.168.1.0/255.255.0 or range 192.168.1.1-192.168.1.10
domain: foo.bar match foo.bar or *.foo.bar
username: 'user J'

Time
none (time not defined)
Enter time name in current which this rule permitted.

Destination
Destination ruleset (click) ACCESS: whitelist - deny: deny - block: 'allow' - pass: if not blocked.
Destination rules in overtime
Destination rules not defined, the ruleset will be ignored.

| Destination rules | access | action |
|--------------------|--------|--------|
| [facebook_engelle] | deny | deny |
| [adk] | allow | allow |
| [aggressive] | allow | allow |
| [adult-video] | allow | allow |
| [drugs] | allow | allow |
| [gambling] | allow | allow |
| [hacking] | allow | allow |
| [mail] | allow | allow |

Name kısmında belirttiğimiz Users kullanıcıları için facebook_engelle kategorisini ,deny' olarak tanımlayarak bundan sonra bu kullanıcıların facebook giriş alternatiflerini daralttık. Tam çözüm mü ? hayır. Devam edelim:

Yukarıdaki işleme ilave olarak Destination kısmında yer alan [blk_BL_socialnet] kategorisinin access değerini de ,deny' yaptığınızda çıkış alternatifleri iyice daralacaktır.

Yukarıdaki gibi bir kullanıcı grubu yerine yerel ağdaki tüm kullanıcılara genel bir facebook filtrelemesi yapmak isterseniz Services menüsünde yer alan Proxy Server komutunu çalıştırın. Daha sonra ekrana gelen pencereden Access Control sekmesini tıklayın. Bu pencere üzerinde yer alan Blacklist kısmına facebook ile ilgili bildiğiniz ne kadar internet adresi varsa yazın ve save yapın.

pfSense çalışma düzeni bir sistem takip eder. Kara düzen bir çalışma sistemi yoktur. Yukarıda yaptığımız ayarlar çerçevesinde ilk önce squid (Proxy server) ayarları, sonra squidGuard (Proxy filter) ayarları, daha sonra da oluşturduğunuz Firewall / Rules'leri varsa onlar işletilir.

Facebook'a https://. üzerinden Erişimi Engelleme

Buraya kadar yapageldiğimiz tüm ayarlar http protokolü (80 nolu PORT) üzerinden yapılan istekleri bloke etmek içindi. Oysa her yerel ağda olması muhtemel uyanık kullanıcılarımız bu şekilde erişemediği facebook'a http://... 'nin hemen yanına s ekleyerek erişebiliyorlar. Dikkat ederseniz https://... şeklinde yapılan istekler sorunsuz çalıştırılmakta.

Çünkü ,Secure Hypertext Transfer Protocol' demek olan https:// sayesinde sunumcu ve istemci arasında kurulan bağlantıda veriler şifrelenir. Bunun için yüksek güvenlik isteyen bankacılık siteleri gibi siteler erişim için bu protokolü kullanır.

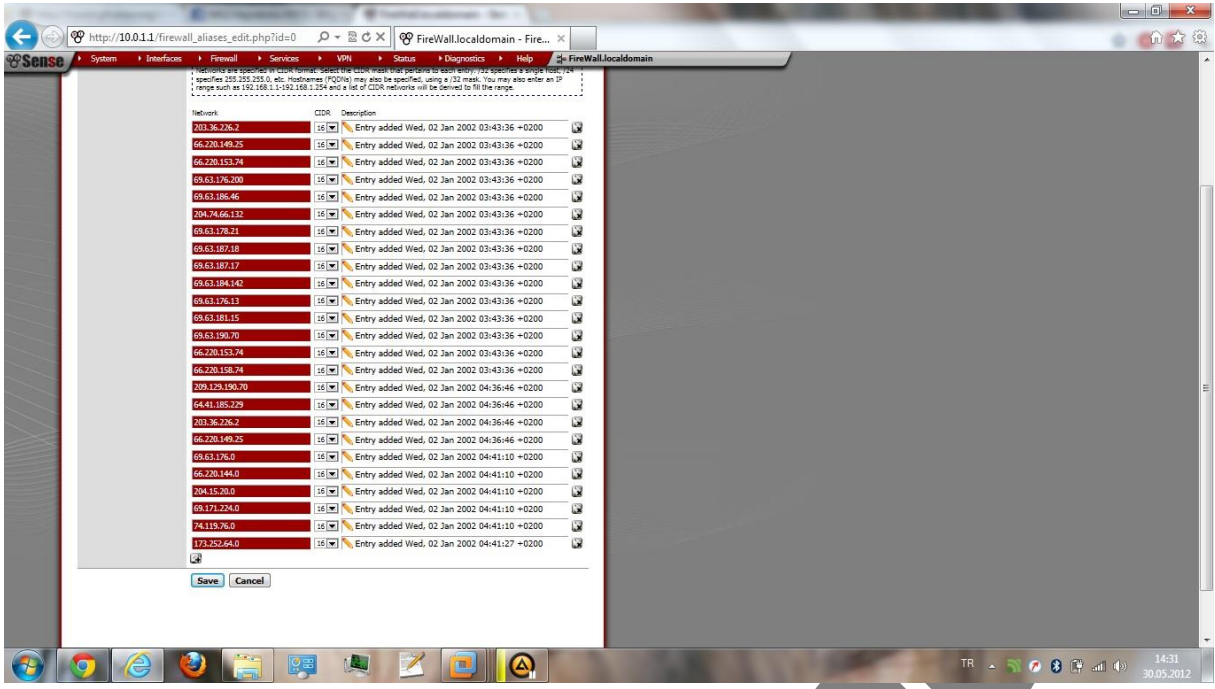
Ancak sadece bankacılık siteleri değil bu güvenlik seçeneğini sunan sitelere de bu şekilde erişmek mümkün. Hal böyle olunca facebook'un https://... erişimini de engelleyebilmek için birkaç ayar daha yapmamız gerekecek. Şöyle ki: Eğer https:// çıkış portu olan 443 portunu tamamen bloke etsek bu kez bankacılık siteleri de devre dışı kalacak, o sitelere de bağlanılamayacak.

O zaman öyle bir ayar yapmalıyız ki hem bankacılık sitesi işlemlerimiz engellenmesin hem de facebook'a blok koysun.

Bu işlem için öncelikle bir Alias tanımlamamız gerekecek. Firewall menüsünde yer alan Alias komutunu çalıştıralım.



Bu pencere üzerinde yer alan + simgesine tıklayarak bir sonraki adıma geçelim. Bu adımda facebook'un kullandığı ve bizim tespit ettiğimiz ne kadar IP adresi varsa bunları aşağıdaki resimde de görüldüğü gibi yazarak save yapalım.



Bir sonraki adımda tanımlanmış olduğumuz bu Alias'ı yine Firewall menüsü altında yer alan Rules komutunu kullanarak tanımlayalım.

Ismail Karadağ

Rules penceresi açıldıktan sonra LAN sekmesine tıklayalım. Burada + simgesine tıklayarak yukarıda tanımladığımız Alias'e https://'yi (443 portunu) kapatalım.

System Interfaces Firewall Services VPN Status Diagnostics

Firewall: Rules: Edit

Action Block
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. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose on which interface packets must come in to match this rule.

Protocol TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source not
Use this option to invert the sense of the match.
Type: any
Address: [redacted] / 31
Advanced - Show source port range

Source OS OS Type: any
Note: this only works for TCP rules

Destination not
Use this option to invert the sense of the match.
Type: Single host or alias
Address: Facebook / 31

Destination port range from: HTTPS to: HTTPS
Specify the port or port range for the destination of the packet for this rule.
Hint: you can leave the 'to' field empty if you only want to filter a single port

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Advanced Options Advanced - Show advanced options

State Type Advanced - Show state

No XMLESPC Sync
HINT: This prevents the rule from automatically syncing to other CARP members.

Schedule none
Leave as 'none' to leave the rule enabled at the time.
NOTE: schedule logic can be a bit different. Click here for more information.

Gateway default
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

Description Facebook https engelleme islemi
You may enter a description here for your reference (not parsed).

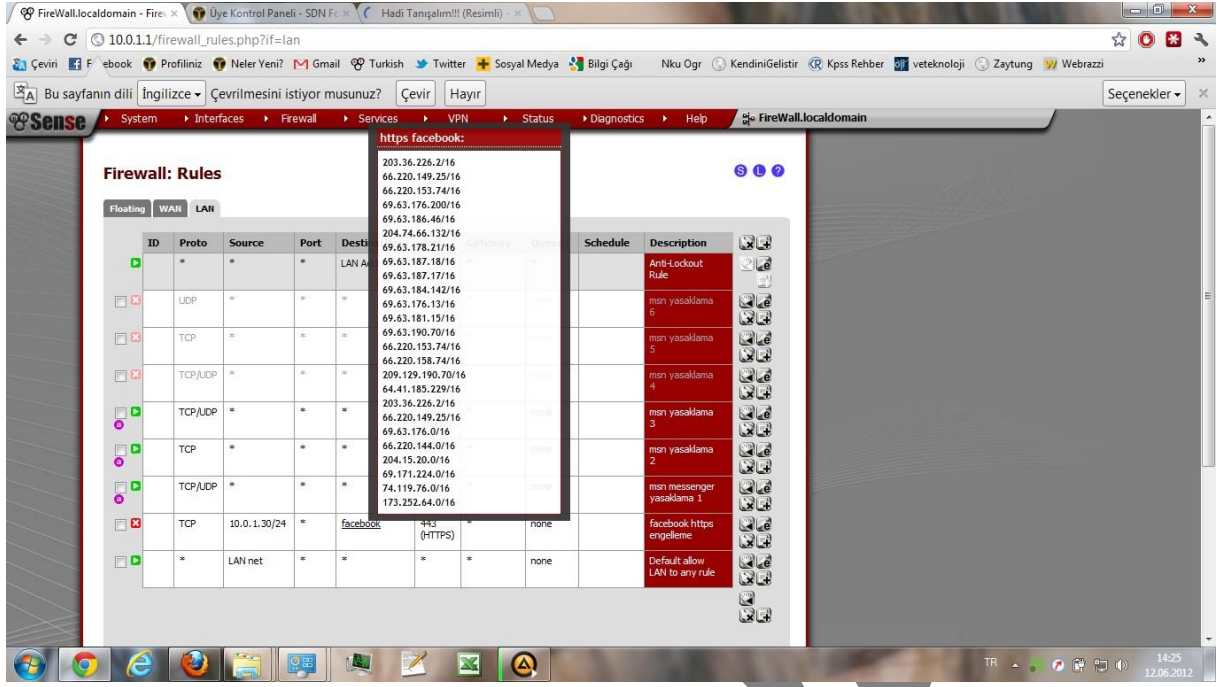
Save Cancel

Action: Block

Destination alanının Type: kısmı 'Single host or alias', Address kısmına Alias kısmında oluşturduğumuz kuralın adını (örneğin Facebook) yazalım.

Destination port range: kısmı ise 'HTTPS' olmalı.

Bu işlemlerden sonra Firewall / Rules altındaki LAN sekmesinin görünümü aşağıdaki gibi olacaktır.

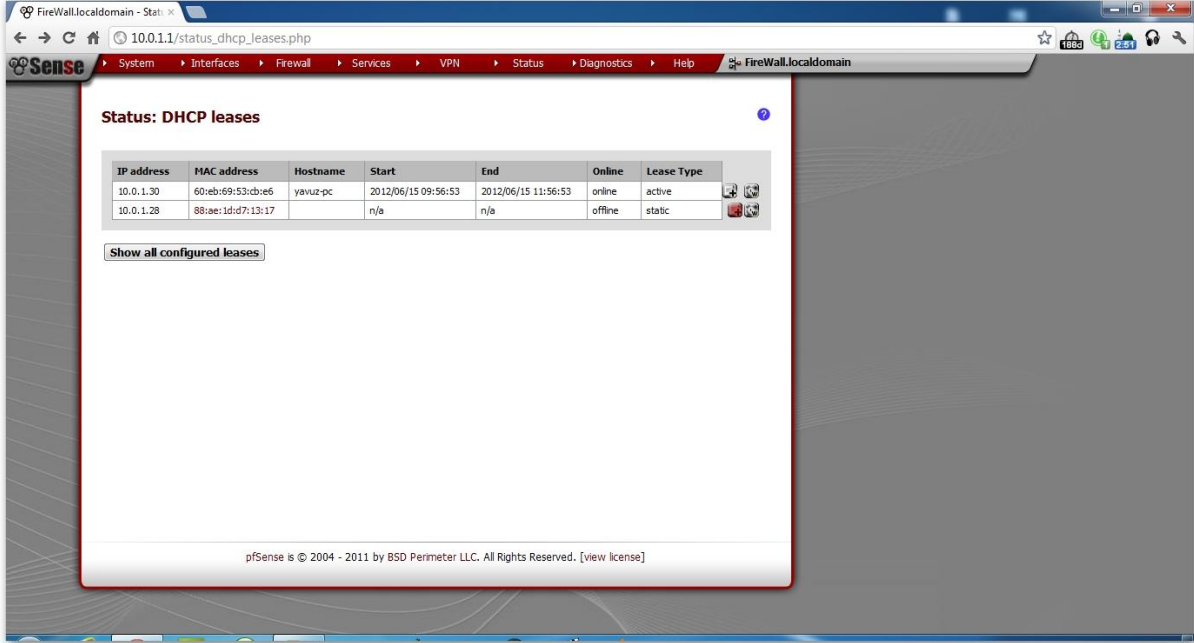


Bundan sonra facebook'a https:// protokolü kullanılarak girilmek istendiğinde girilemeyecek, ekranda aşağıdaki gibi bir sonuç görünecektir.



Mac adreslerine göre İp Atama

“Status” Menüsünden “DHCP leases” seçeneğine gelerek güvenlik duvarımıza bağlı ipleri görebiliyoruz, belirli iplerin güvenlik duvarımıza uğramadan internete bağlanabilmesini sağlayacak bu ayar için aşağıdaki resimde de görüldüğü gibi istediğimiz mac adresine ip atamak için sağ tarafındaki “+” simgesine tıklıyoruz.



| IP address | MAC address | Hostname | Start | End | Online | Lease Type |
|------------|-------------------|----------|---------------------|---------------------|---------|------------|
| 10.0.1.30 | 60:eb:69:53:cb:e6 | yavuz-pc | 2012/06/15 09:56:53 | 2012/06/15 11:56:53 | online | active |
| 10.0.1.28 | 88:ae:1d:d7:13:17 | n/a | n/a | n/a | offline | static |

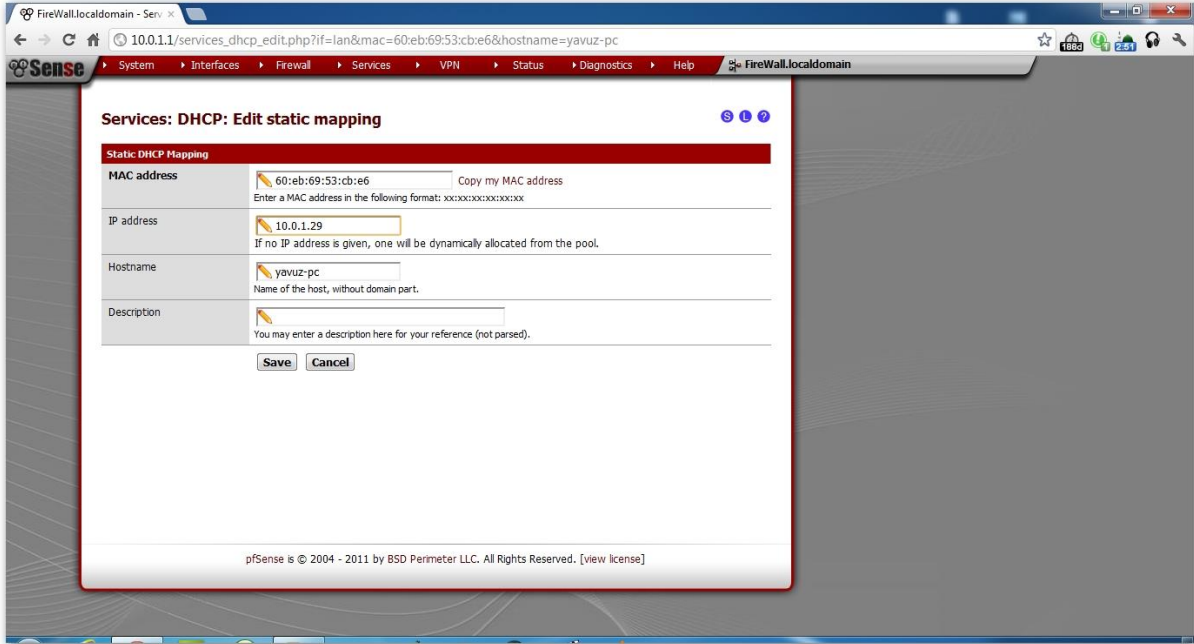
Show all configured leases

pSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [view license]

Gelen menüde **İp Adres:** bölümüne pfsense'in kontrol ettiği ipler dışında bir ip yazıyoruz.

Hostname: Host adresimizi yazıyoruz.

Description kısmına açıklama giriyoruz.



Services: DHCP: Edit static mapping

Static DHCP Mapping

MAC address: 60:eb:69:53:cb:e6 Copy my MAC address
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx

IP address: 10.0.1.29
If no IP address is given, one will be dynamically allocated from the pool.

Hostname: yavuz-pc
Name of the host, without domain part.

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

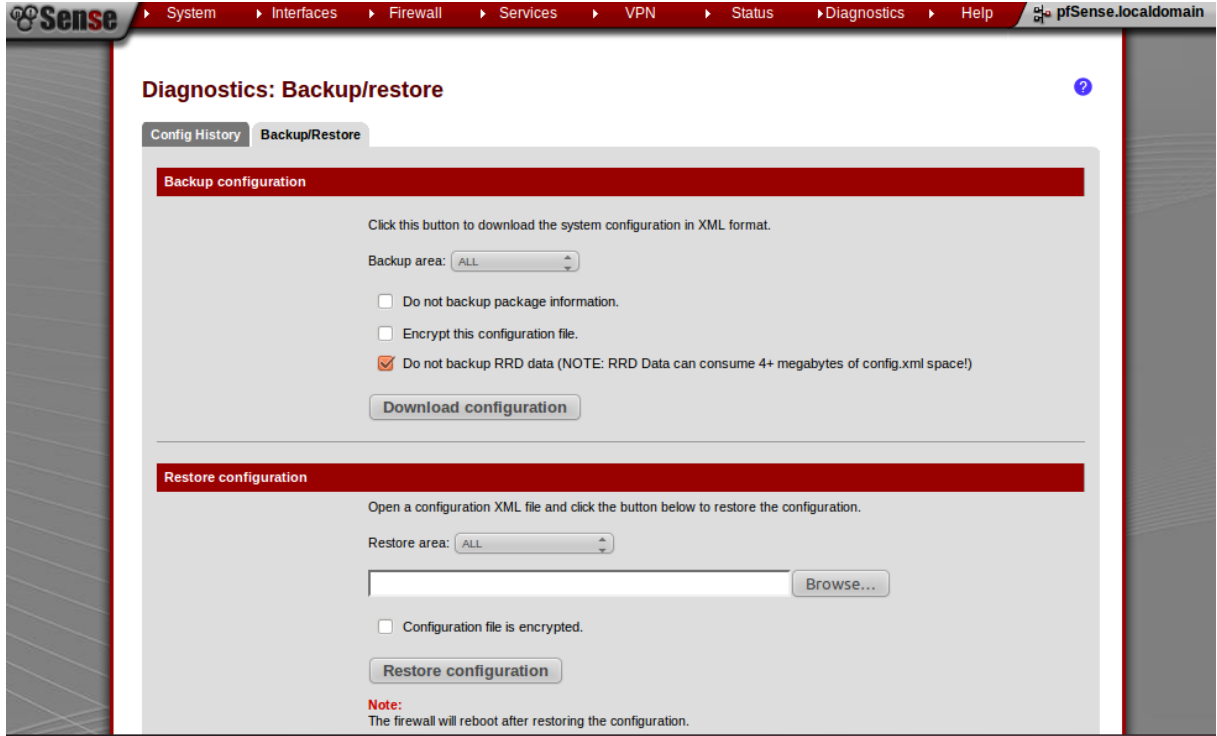
Save Cancel

pSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [view license]

pfSense Backup/Restore Yapma

Diagnostic menüsünden Backup/Restore seçeneğiyle sistemde yapılan belirli ayarlar seçilerek veya bütün ayarlar topluca yedeklenebilir ve daha önce yedeklenmiş olan ayarlar da bu menüdeki Restore configuration menüsünden restore edilebilir.

“config-FireWall.localdomain-20120615122654” örneği gibi .xml dosyası olarak yedek alınır.



The screenshot shows the pfSense web interface for the Backup/Restore configuration. The breadcrumb navigation at the top reads: System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help. The page title is "Diagnostics: Backup/restore".

Under the "Backup/Restore" tab, there are two main sections:

- Backup configuration:** This section includes a "Download configuration" button. Below it, there is a "Backup area" dropdown menu set to "ALL". There are three checkboxes: "Do not backup package information." (unchecked), "Encrypt this configuration file." (unchecked), and "Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)" (checked).
- Restore configuration:** This section includes a "Restore configuration" button. Below it, there is a "Restore area" dropdown menu set to "ALL". There is a text input field for the configuration file path, followed by a "Browse..." button. There is one checkbox: "Configuration file is encrypted." (unchecked).

A note at the bottom of the restore section states: "Note: The firewall will reboot after restoring the configuration."

İsmail