



**Hazırlayan: Ömer Faruk ERDEM**

## İçindekiler

pfSense.....	3
pfSense'in Temel Özellikleri.....	3
pfSense Kurulumu.....	4
Sanal Ağ Ayarları.....	4
Sanal Makine Kurulumu.....	5
NAT ve WAN Kurulumu.....	6
pfSense Web Arayüzü.....	9
Ana Makineden Web Arayüzüne Erişim.....	9
.....	10
NAT.....	11
DNS Resolver.....	11
virt-manager kurulumu (Opsiyonel).....	14
Basit Ağ Topolojisi.....	14
.....	14

## pfSense

pfSense, açık kaynak kodlu bir güvenlik duvarı ve yönlendirici (router) yazılımıdır. Genellikle ağ güvenliği ve yönetimi için kullanılır. BSD tabanlı bir işletim sistemi olan FreeBSD üzerinde çalışır ve gelişmiş güvenlik duvarı ve yönlendirme özellikleri sunar.

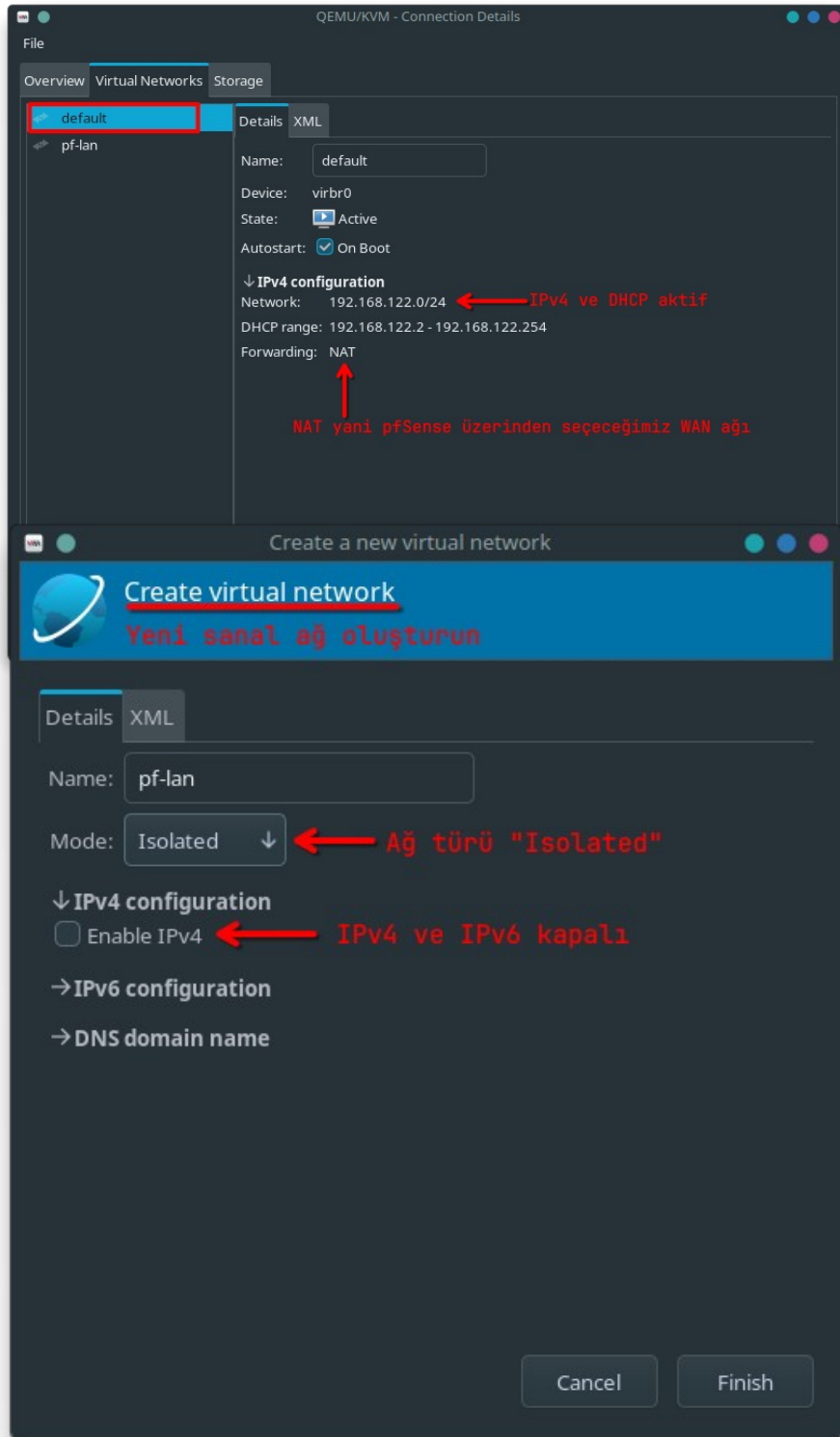
### pfSense'in Temel Özellikleri

- **Güvenlik Duvarı ve NAT (Network Address Translation):** pfSense, çok gelişmiş bir güvenlik duvarı olarak çalışır. Gelen ve giden trafiği kontrol eden kurallar tanımlayarak ağınızı korur. NAT ile dahili IP adreslerini harici IP adreslerine dönüştürerek internet erişimini sağlar.
- **VPN (Virtual Private Network) Desteği:** pfSense, çeşitli VPN protokollerini (OpenVPN, IPSec, PPTP, L2TP, vb.) destekler. Bu sayede uzak ofisler arasında güvenli bağlantılar kurabilir veya kullanıcıların uzaktan güvenli bir şekilde ağa erişimini sağlayabilirsiniz.
- **Yönlendirme (Routing):** pfSense, statik ve dinamik yönlendirme yeteneklerine sahiptir. BGP, OSPF gibi protokoller ile karmaşık ağ yapılarında yönlendirme işlemlerini yönetebilir.
- **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):** pfSense, Snort ve Suricata gibi araçlar ile entegre olarak çalışabilir. Bu sayede ağ trafiğinizi analiz eder ve potansiyel saldırılara karşı önlem alır.
- **Load Balancing (Yük Dengeleme):** pfSense, hem ağ trafiği hem de internet bağlantısı için yük dengeleme yapabilir. Birden fazla internet bağlantınız varsa, pfSense bu bağlantılar arasında trafiği dağıtarak performansı artırır.
- **QoS (Quality of Service):** Bant genişliği yönetimi yaparak ağınızdaki trafiği önceliklendirebilirsiniz. Bu, özellikle VoIP ve video konferans gibi uygulamalar için önemlidir.
- **Paket Yönetimi:** pfSense, özelliklerini genişletmek için çeşitli paketler yüklemenize olanak tanır. Örneğin, pfBlockerNG ile reklam engelleme veya Squid ile web filtreleme yapabilirsiniz.

## pfSense Kurulumu

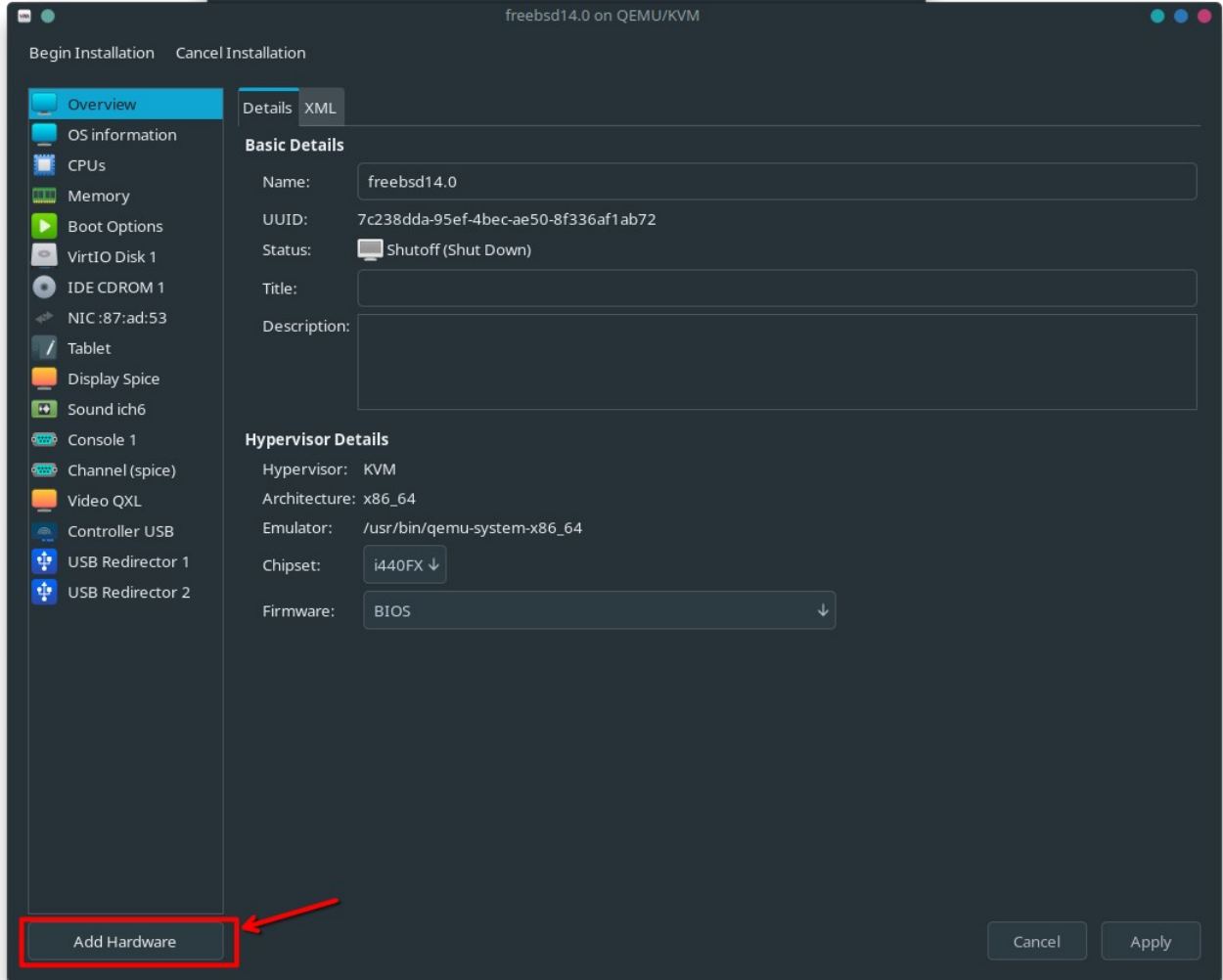
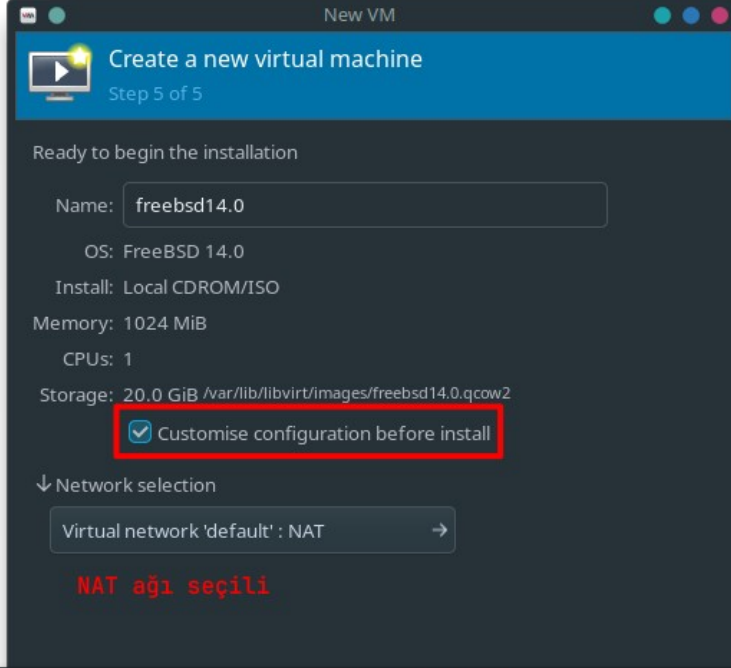
<https://www.pfsense.org/download/> adresinden pfSense'e ait en son yayımlanan ISO dosyasını indirebilirsiniz. Kurulumu geçmeden önce sanal makine yöneticinizden NAT ve LAN ağı ayarlarını gerçekleştirmelisiniz. Aşağıdaki görsellerde KVM/QEMU virt-manager üzerinden yapılan ayarlara ulaşabilirsiniz.

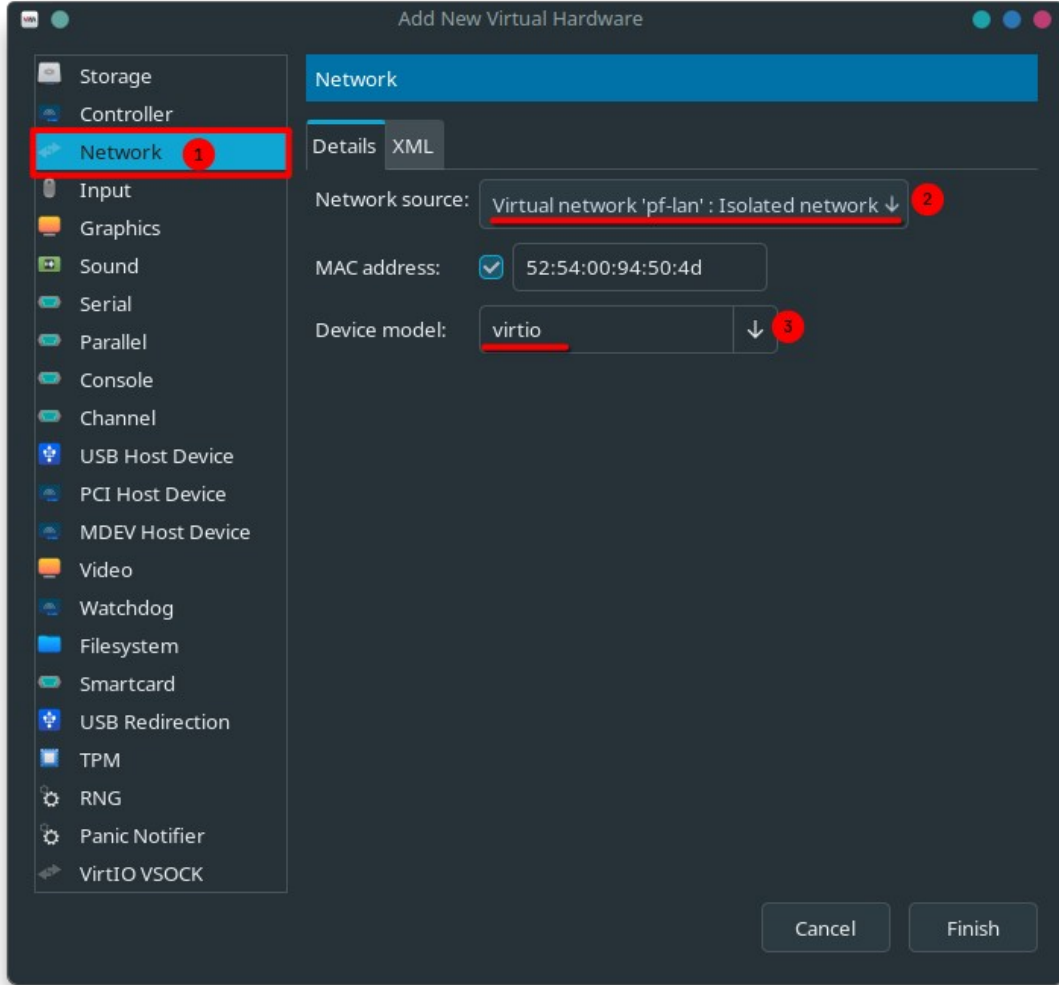
### Sanal Ağ Ayarları



## Sanal Makine Kurulumu

- Yeni sanal makine oluşturma seçeneğini seçin
- pfSense netgate ISO dosyasını bulun ve kurulacak işletim sistemi türü olarak FreeBSD seçeneğini seçin
- Depolama, RAM ve CPU değerlerini sisteminizin karşılayabileceği değerler olarak belirleyin





Ekranın sol üst köşesindeki “Begin Installation” butonuna basarak ilerleyin. Kurulum sırasında karşınıza çıkacak seçeneklere ileri seçeneğini seçerek devam edin, bir seçenek hariç. Kurulum size WAN ve LAN ağını seçmenizi isteyecek bu noktada sanal makinenizin konfigürasyon ayarlarına gelerek pf-lan yani Isolated ağınıza bağlı olduğu NIC sekmesine gelerek MAC adresini öğrenmelisiniz. Bu MAC adresine sahip olan ağ arayüzünü -genellikle vtnet1- LAN olarak ayarlayıp, ikinci ağ arayüzünü yani NAT ağına bağlı olan arayüzü ise WAN olarak belirleyerek kurulumu devam ettirin. Kurulum tamamlanıp pfSense CLI arayüzü geldiğinde aşağıdaki ayarlarla devam etmelisiniz.

## NAT ve WAN Kurulumu

```
php-fpm[400]: /index.php: Successful login for user 'admin' from: 10.0.1.3 (Local Database)

FreeBSD/amd64 (pfSense.pfsense.firewall) (ttyv0)
KVM Guest - Netgate Device ID: c12b3d58dcd0864e15ea
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.122.169/24
LAN (lan)      -> vtnet1      -> v4: 10.0.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

```
Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 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 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
pfsense on QEMU/KVM
File Virtual Machine View Send Key
[Icons] [Full Screen]

>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.1.2
Enter the end address of the IPv4 client address range: 10.0.1.254
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

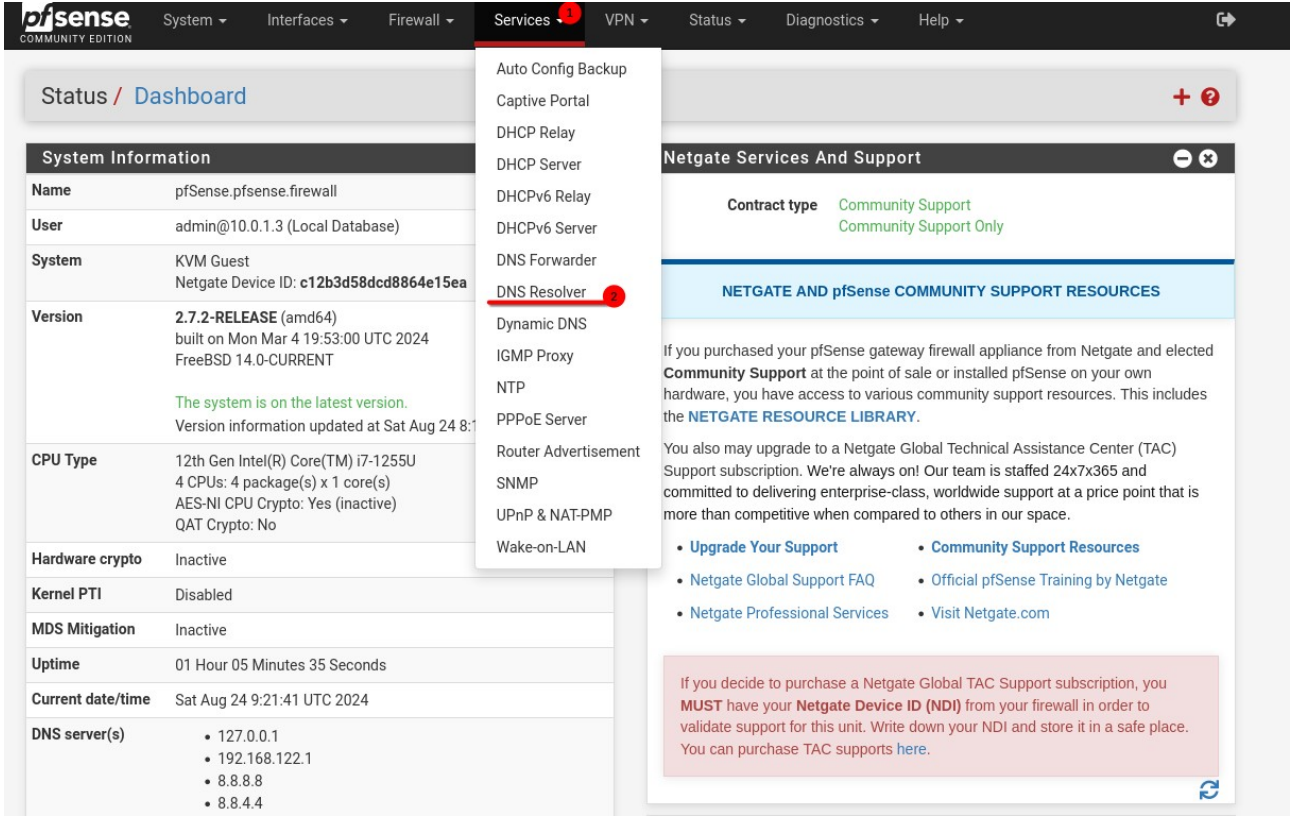
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.0.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.0.1.1/

Press <ENTER> to continue.
```

Sırada sadece pfSense web arayüzünden güvenlik duvarı ve DNS ayarlarını yaparak LAN ağımızda sunucularımızı çalıştırmak kaldı. Herhangi bir sanal makinenizi pf-lan olarak adlandırdığımız Isolated ağında çalıştırarak <https://10.0.1.1> adresine gittiğinizde karşınıza çıkacak olan giriş sayfasında admin:pfsense bilgilerini kullanarak web arayüzünün kurulum adımlarını takip ederek web arayüzüne erişebilirsiniz.



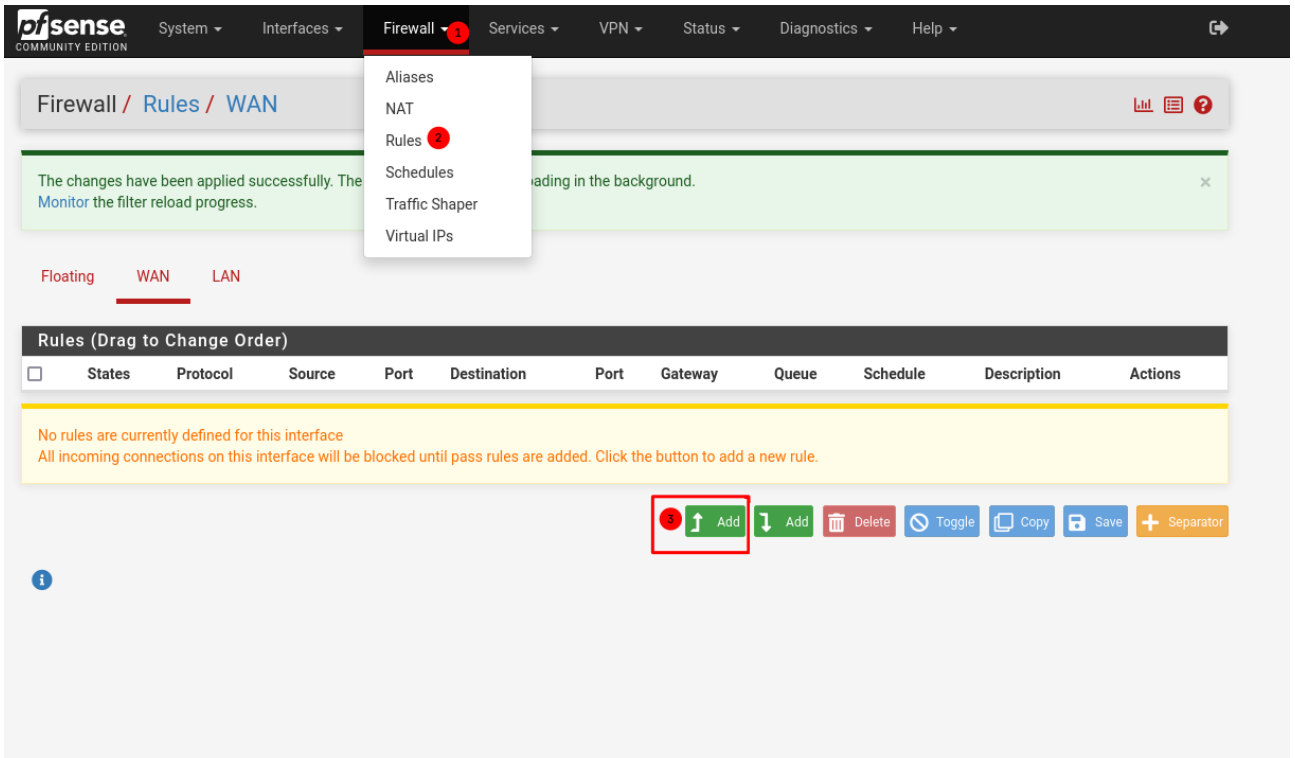


The screenshot shows the pfSense web interface. The 'System' tab is selected, displaying system information. The 'Services' menu is open, showing various services like Auto Config Backup, Captive Portal, DHCP Relay, etc. The 'DNS Resolver' service is highlighted with a red circle. The 'Netgate Services And Support' section is also visible, providing information about community support and resources.

Sayfayı aşağıya kaydırarak “Save” butonuna tıkladığımızda DNS sunucusu aktifleşecek ve internet erişimi sorunsuz bir şekilde sağlanabilecek.

## Ana Makineden Web Arayüzüne Erişim

Dilerseniz WAN arayüzünü kullanarak ana -host- makinenizden pfSense web arayüzüne erişmek için “Rules” bölümünden aşağıdaki adımları izleyerek yeni bir kural yazdığınızda erişim sağlayabilirsiniz.



The screenshot shows the pfSense Firewall Rules configuration page. The 'Rules' menu is open, and the 'Rules' option is selected. The 'WAN' interface is selected. The 'Rules (Drag to Change Order)' table is empty, indicating no rules are currently defined for this interface. The 'Add' button is highlighted with a red box, and the 'Save' button is also visible.

### Edit Firewall Rule

**Action** Pass **1**

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule

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

**Interface** WAN **2**

Choose the interface from which packets must come to match this rule.

**Address Family** IPv4 **3**

Select the Internet Protocol version this rule applies to.

**Protocol** TCP **4**

Choose which IP protocol this rule should match.

### Source

**Source** ☐ Invert match WAN subnets **5**

Source Address /

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

### Destination

**Destination** ☐ Invert match This Firewall (self) **6**

Destination Address /

**Destination Port Range** (other) From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

### Extra Options

**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 doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**  Display Advanced

 Save **7**

## NAT

<b>Interface</b>	WAN		
	Choose which interface this rule applies to. In most cases "WAN" is specified.		
<b>Address Family</b>	IPv4		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	TCP/UDP		
	Choose which protocol this rule should match. In most cases "TCP" is specified.		
<b>Source</b>	<a href="#">Display Advanced</a>		
<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
<b>Destination port range</b>	HTTPS	HTTPS	
	From port	To port	Custom
	Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.		
<b>Redirect target IP</b>	Address or Alias	10.0.1.3	Web Sunucusu LAN Ip Adresi
	Type	Address	
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)		
<b>Redirect target port</b>	HTTPS		
	Port	Custom	
	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.		
<b>Description</b>			
	A description may be entered here for administrative reference (not parsed).		
<b>No XMLRPC Sync</b>	<input type="checkbox"/> Do not automatically sync to other CARP members		
	This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.		
<b>NAT reflection</b>	Use system default		
<b>Filter rule association</b>	Rule NAT		
	<a href="#">View the filter rule</a>		

## DNS Resolver

## Services / DNS Resolver / General Settings



General Settings Advanced Settings Access Lists

### General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate

The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port

The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

#### Network Interfaces

☒ All  
☐ WAN  
☐ LAN  
☐ WAN IPv6 Link-Local  
☐ LAN IPv6 Link-Local

Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

#### Outgoing Network Interfaces

☒ All  
☐ WAN  
☐ LAN  
☐ WAN IPv6 Link-Local  
☐ LAN IPv6 Link-Local

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

## Services / DNS Resolver / General Settings / Edit Host Override



### Host Override Options

Host

Name of the host, without the domain part  
e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain

Parent domain of the host  
e.g. enter "example.com" for "myhost.example.com"

IP Address

IPv4 or IPv6 comma-separated addresses to be returned for the host  
e.g.: 192.168.100.100 or fd00:abcd::  
or list 192.168.1.3,192.168.4.5,fc00:123::3

Description

A description may be entered here for administrative reference (not parsed).

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'has.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.

### Additional Names for this Host

Additional	Host name	Domain	Description	
	<input type="text" value="stirling-pdf"/>	<input type="text" value="skylab.com"/>	<input type="text" value="stirling-pdf"/>	<input type="button" value="Delete"/>

### New Access List

Access List name

pfSenseDNS

Provide an Access List name.

Action

Allow

**Allow**

**Deny:** Stops queries from hosts within the netblock defined below.

**Refuse:** Stops queries from hosts within the netblock defined below, but sends a DNS rcode REFUSED error message back to the client.

**Allow:** Allow queries from hosts within the netblock defined below.

**Allow Snoop:** Allow recursive and nonrecursive access from hosts within the netblock defined below. Used for cache snooping and ideally should only be configured for the administrative host.

**Deny Nonlocal:** Allow only authoritative local-data queries from hosts within the netblock defined below. Messages that are disallowed are dropped.

**Refuse Nonlocal:** Allow only authoritative local-data queries from hosts within the netblock defined below. Sends a DNS rcode REFUSED error message back to the client for messages that are disallowed.

Description

A description may be entered here for administrative reference.

Networks

0.0.0.0

**Allow All**

/

0

Network/mask

Description

Save

+ Add Network



faruk@localhost:~



```
[faruk@localhost ~]$ nmcli d
checkpoint disconnect lldp reapply status
connect down modify set up
delete help monitor show wifi
[faruk@localhost ~]$ nmcli d mod enp1s0 ipv4.dns 192.168.122.99
```

**Set pfSense as DNS server from WAN interface machines**

## virt-manager kurulumu (Opsiyonel)

```
# Fedora tabanlı dağıtımlar için:
dnf install @virtualization
```

```
# Debian tabanlı dağıtımlar için:
apt install qemu-kvm libvirt-clients libvirt-daemon-system bridge-utils
virtinst libvirt-daemon virt-manager
```

```
# Ubuntu tabanlı dağıtımlar için:
apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils
```

[Adresinden](#) daha detaylı bilgilere ulaşılabilir.

## Basit Ağ Topolojisi

Source IP	Source Port	Dest IP	Dest Port	Proto	Forward IP	Forward Port	Description
WAN Subnets	*	WAN Address	443	TCP	10.0.1.2	443	NAT
*	*	WAN Address	80	TCP	10.0.1.2	80	NAT
*	*	WAN Address	53	UDP	N/A	N/A	DNS
LAN Subnets	*	LAN Address	443	TCP	N/A	N/A	LAN anti-lockout
LAN Subnets	*	LAN Address	80	TCP	N/A	N/A	LAN anti-lockout
LAN Subnets	*	0.0.0.0/0	443	TCP	N/A	N/A	Allow HTTP

