

OVERVIEW:

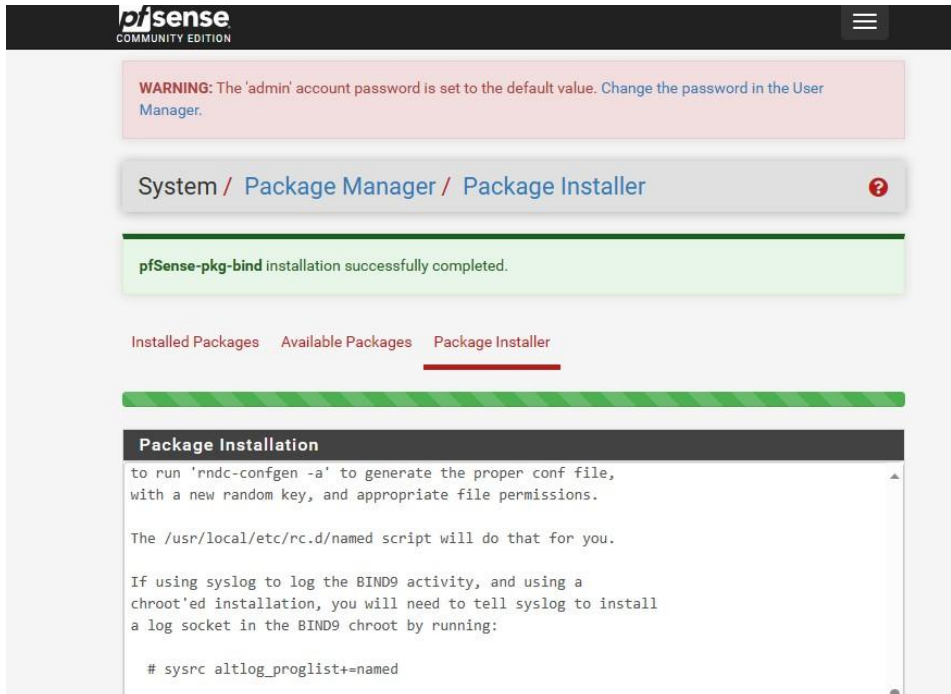
The purpose of this lab was to configure DHCP and DNS on the pfSense firewall. I worked on setting up these protocols to better understand how they function and tested their connectivity. This experience is valuable because it provides hands-on knowledge for managing static IP addresses through DHCP and ensuring proper name resolution with DNS—skills that are essential for real-world network administration.

ANALYSIS:

First, I installed BIND on pfSense to enable DNS services.



After installation, I verified that BIND was successfully installed and operational.



Next, I navigated to the general setup section of pfSense and updated the information to match the network's requirements.

System / General Setup



System

Hostname

Name of the firewall host, without domain part.

Domain

Domain name for the firewall.

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is **widely used** by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

Disable SMTP☒ Disable SMTP Notifications

Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.

E-Mail server

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

SMTP Port of E-Mail server

This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).

Connection timeout to E-Mail server

This is how many seconds it will wait for the SMTP server to connect. Default is 20s.

Secure SMTP Connection☐ Enable SMTP over SSL/TLS**Validate SSL/TLS**☒ Validate the SSL/TLS certificate presented by the server

When disabled, the server certificate will not be validated. Encryption will still be used if available, but the identity of the server will not be confirmed.

From e-mail address

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

Notification E-Mail address

Enter the e-mail address to send email notifications to.

To better reflect the network structure, I renamed the OPT1 interface to DMZ.





General Configuration

Enable☒ Enable interface**Description**

Enter a description (name) for the interface here.

I disabled the DNS resolver on pfSense to avoid conflicts with the new DNS settings.


Enable ☐ Enable DNS resolver

Services / DHCP Server / DMZ / Edit Static Mapping    

Static DHCP Mapping on DMZ

MAC Address

00:0C:29:0A:31:2E

 Copy My MAC

MAC address of the client to match (6 hex octets separated by colons).

Client Identifier

An optional identifier to match based on the value sent by the client (RFC 2132)

IP Address

192.168.3.3

IPv4 address to assign this client.

Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool.
The same IP address may be assigned to multiple mappings.

Hostname

web

Name of the client host without the domain part.

Daemon Settings

Enable BIND

☒ Enable BIND DNS server.
Disable DNS Forwarder and Resolver services on selected interfaces before enabling BIND.

IP Version

IPv4+IPv6

Select IP transport version.
This controls which transports are used when resolving queries.

Listen on

LAN
DMZ
WAN
loopback

Choose the interfaces on which to enable BIND.

Enable Notify

☐ Notify slave server after any update on master.

Hide Version

☐ Hide the version of BIND (ignore queries for version.bind).

Limit Memory Use

256M
Limits RAM use for DNS server (Recommended: 256M)

Logging Options

Enable Logging

☐ Enable BIND logs under Status > System logs, Resolver tab.

Logging Severity

Critical

I proceeded to create a custom view to organize the DNS configuration as needed.

Settings ACLs **Views** Zones Sync

General Options

View Name
Enter the name of the View.

Description
Enter a description of the View.

Recursion
A recursive query occurs when your DNS server is queried for a domain that it currently knows nothing about, in which case it will try to resolve the given host by performing further queries (e.g. by starting at the root servers and working out, or by simply passing the request to yet another DNS server).

match-clients
If either or both of match-clients are missing they default to any (all hosts match).
The match-clients statement defines the address_match_list for the source IP address of the incoming messages.

allow-recursion

A forward lookup zone was then created to allow for proper resolution of domain names to IP addresses.

Settings ACLs Views **Zones** Sync

Domain Zone Configuration

Disable This Zone ☐ Do not include this zone in BIND config files.

Zone Name
Enter the name for this zone (e.g. example.com)
For reverse zones, include zone IP in reverse order. (e.g. 1.168.192)
Note: IN-ADDR.ARPA will be automatically included in config files when reverse zone option is checked.

Description
Enter a description for this zone.

Zone Type
Select zone type.

View
Select (CTRL+click) the views that this zone will belong to.

Reverse Zone ☐ Check if this is a reverse zone.

IPv6 Reverse ☐ Check if this is an IPv6 reverse zone. Reverse Zone must also be enabled.

Zone Domain records					
Enter Domain Records	jsimpson.fail	NS		192.168.2.1	Delete
	pfsense	A		192.168.2.1	Delete
	web	A		192.168.3.3	Delete
	www	CNAME		web.jsimpso	Delete

Following that, I set up a reverse lookup zone to resolve IP addresses back to domain names.

Disable This Zone ☐ Do not include this zone in BIND config files.

Zone Name
 Enter the name for this zone (e.g. example.com)
 For reverse zones, include zone IP in reverse order. (e.g. 1.168.192)
Note: IN-ADDR.ARPA will be automatically included in config files when reverse zone option is checked.

Description
 Enter a description for this zone.

Zone Type
 Select zone type.

View
 Select (CTRL+click) the views that this zone will belong to.

Reverse Zone ☒ Check if this is a reverse zone.

Zone Domain records					
Enter Domain Records	2.1	NS		jsimpson.fail	Delete
	2.1	PTR		pfsense	Delete
	3.3	PTR		web	Delete
	Record	Type	Priority	Alias or IP address	
Add	+ Add				
Register DHCP Static Mappings	<input type="checkbox"/> If this option is set, then DHCP static mappings will be registered in DNS, so that their name can be resolved.				

After completing the DNS configuration, I renewed the address to clear the IPv6 address listing, ensuring everything was functioning correctly. Finally, after the renewal, I confirmed that the setup was working as expected.

