



Yago Fernández Blanco
2º ASIR
Seguridad y alta disponibilidad
01/10/2019

PRÁCTICA 10

1. Añadir servidor DNS 8.8.4.4.

Firewall / Aliases / Edit

Properties

Name

dns_server

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

Description

DNS autorizado

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

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

8.8.4.4

Description

Save

Add Host

2. Administradores podrán hacer consultas dns a cualquier DNS.

Edit Firewall Rule

Action Pass

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

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

Interface LAN

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

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol UDP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. LAN net 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. Single host or alias dns_server /

Destination (other) (other)

pfSense.localdomain - Firewall: × +

←

→

↺

🏠

🔒

🚫

192.168.0

⋮

🛡️

☆

⬇️

📁

📄

🕒

🧑

🐶

🟢

🐾

⏏️

☰

Action

Pass

▼

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

Disabled

☐ Disable this rule

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

Interface

LAN

▼

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

Address Family

IPv4

▼

Select the Internet Protocol version this rule applies to.

Protocol

TCP

▼

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match.

any

▼

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.

Single host or alias

▼

dns_server

/

▼

Destination Port Range

(other)

▼

From

Custom

To

(other)

▼

Custom

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

3. Acceso en horario establecido

pfSense.localdomain - Firewall: X

192.168.0

Firewall / Schedules / Edit

Schedule Information

Schedule Name

Comercial_ftp

The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

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

Month

February_20

Date

February_2020

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

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

Time

8

00

14

00

Start Hrs

Start Mins

Stop Hrs

Stop Mins

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

Time range description

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

+ Add Time

Clear selection

Schedule

Comercial_ftp

Leave as 'none' to leave the rule enabled all the time.

4. SMTP en horario

pfSense.localdomain - Firewall: X

pfSense.localdomain - Firewall: X

+

← → ↺ 🏠 🔒 192.168.0 ... 🛡️ ☆ ⬇️ ||| 📄 🔍 🧑🦾 🐉 🟢 🐾 ➡️ ☰

Edit Firewall Rule

ActionPass▼

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▼

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

Address Family

IPv4▼

Select the Internet Protocol version this rule applies to.

Protocol

TCP▼

Choose which IP protocol this rule should match.

Source

Source☒ Invert match.

Single host or alias▼smtp_correo / ▼

⚙️ 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**.

ScheduleComercial_ftp▼

Leave as 'none' to leave the rule enabled all the time.

5. IMAP en horario

Edit Firewall Rule

Action	Pass		
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	WAN		
	Choose the interface from which packets must come to match this rule.		
Address Family	IPv4		
	Select the Internet Protocol version this rule applies to.		
Protocol	TCP		
	Choose which IP protocol this rule should match.		

Source

Source	<input type="checkbox"/> Invert match.	Single host or alias	imap_correo /
	Hide 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 .		
Source Port Range	(other)		(other)
	From Custom	To Custom	

Schedule

Comercial_ftp

Leave as 'none' to leave the rule enabled all the time.

6. Log Denied Rule

The screenshot shows the 'Edit Firewall Rule' page in the pfSense web interface. The browser tabs show 'pfSense.localdomain - Firewall: X' and the address bar shows '192.168.0'. The breadcrumb navigation is 'Firewall / Rules / Edit'. The page title is 'Edit Firewall Rule'. The 'Action' is set to 'Reject'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'WAN'. The 'Address Family' is set to 'IPv4'. The 'Protocol' is set to 'UDP'. The 'Source' section has 'Source' set to 'Single host or alias', 'Invert match' is unchecked, and the source is 'LogDenyRule'. The 'Destination' section has 'Destination' set to 'any', 'Invert' is unchecked, and the destination is 'Destination Address'. A 'Display Advanced' button is visible in the Source section.

Firewall / Rules / Edit

Edit Firewall Rule

Action Reject

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

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

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol UDP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. Single host or alias LogDenyRule /

[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 any Destination Address /

7. No Logging Rule

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol UDP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match. Single host or alias NoLoggingRule /

[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. any Destination Address /