

Section 1 Part 1: Steps 1-15:

Configuring Custom Firewall Rules with pfsense (3e)

LAB GUIDE: 6%

- Part 1: Plan the LAN Firewall Rules
 - Part 2: Configure the LAN Firewall Rules
 - Part 3: Verify Firewall Rules for the LAN
- Section 2: Applied Learning
- Section 3: Challenge and Analysis

Part 1: Plan the LAN Firewall Rules (1/1 completed)

Note: Finally, you will plan a rule configuration for the ICMP protocol, which permits basic network diagnostic tests that are useful in network validation and troubleshooting.

ICMP is an IP protocol of its own, sharing the same layer as TCP and UDP. ICMP does not have ports, but rather types and codes. For this reason, the port range is not applicable. All ICMP types and codes will be permitted by default, so no further specification is required beyond the protocol designation.

13. Repeat steps 1-10 to create the following outbound (LAN) rule.

- Allow Internet Control Message Protocol (ICMP) messages through the LAN interface, to and from any IPv4 address, so that common network diagnostic utilities can be used, such as Ping and Traceroute.

You may enter whatever description you think is suitable.

14. Make a screen capture showing the completed LAN Firewall Rules tab in the PFSense-FW-PLANNER worksheet.

15. In the PFSense-FW-PLANNER spreadsheet, click File > Save

Interface	Address Family	Protocol	Source IP Address			Destination IP Address			Port
			Invert	Type	Address	Subnet Mask	Invert	Type	
3	LAN	IPV4	TCP	ANY		ANY			HTTP (80)
4	LAN	IPV4	TCP	ANY		ANY			DNS (53)
5	LAN	IPV4	TCP	ANY		ANY			SSH (22)
6	LAN	IPV4	UDP	ANY		ANY			ICMP

Part 2: Steps 1-24

Configuring Custom Firewall Rules with pfsense (3e)

LAB GUIDE: 13%

- Part 1: Plan the LAN Firewall Rules
- Part 2: Configure the LAN Firewall Rules
- Part 3: Verify Firewall Rules for the LAN

- Section 2: Applied Learning
- Section 3: Challenge and Analysis

Part 2: Configure the LAN Firewall Rules (1/1 completed)

21. Repeat steps 9-18 to create the ICMP rule detailed in the PFSense-FW-PLANNER, using the appropriate Protocol and Description values.

Once you select the ICMP protocol, the Source and Destination Port Range options will be removed, and an ICMP Subtype list will be added below the Protocol dropdown. Leave the default value of any and continue to the Description field to complete your ICMP rule configuration.

22. On the Firewall / Rules / LAN page, click the Apply Changes button to apply the rule changes that you have made to the firewall.

23. Make a screen capture showing your completed LAN Rules table.

24. Minimize the Firefox browser.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/803 KIB	*	*	*	LAN Address	80	*	*		AntiLockout Rule	⚙️
✓ 0/0 B	IPV4 TCP	*	*	*	80 (HTTP)	*	none		Web Browsing	🔗 📄 🗑️
✓ 0/0 B	IPV4 TCP	*	*	*	53 (DNS)	*	none		DNS Services	🔗 📄 🗑️
✓ 0/0 B	IPV4 TCP	*	*	*	22 (SSH)	*	none		Remote Connections	🔗 📄 🗑️
✓ 0/0 B	IPV4 ICMP	*	*	*		*	none		Pings	🔗 📄 🗑️

Part 3: Steps 1-4

Configuring Custom Firewall Rules with pfSense (3e)

LAB GUIDE: 13%

- Part 1: Plan the LAN Firewall Rules
- Part 2: Configure the LAN Firewall Rules
- Part 3: Verify Firewall Rules for the LAN

Section 2: Applied Learning

Section 3: Challenge and Analysis

Part 3: Verify Firewall Rules for the LAN (0/3 completed)

Assuming DNS resolution is properly configured on pfSense, and records exist for the website, a successful query on the website's fully qualified domain name (FQDN) should return pfSense.localdomain in the Server (the DNS server being queried) field, followed by the IP address, and corporationtechs.com in the Name field (the host being looked-up) followed by its IP address. These values indicate your DNS LAN rule is configured correctly to allow TCP/UDP traffic on port 53.

3. At the command prompt, type `ping corporationtechs.com` to send an ICMP Ping request to the host serving corporationtechs.com.

```
C:\Users\Administrator>ping corporationtechs.com

Pinging corporationtechs.com [172.40.0.20] with 32 bytes of data:
Reply from 172.40.0.20: bytes=32 time=1ms TTL=63

Ping statistics for 172.40.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Firewall / Rules / LAN

The changes have been applied successfully. Monitor the filter reload progress.

Floating WAN LAN DIV

Rules (Drag to Change Order)	States	Protocol
<input type="checkbox"/> 0/927 KB	<input checked="" type="checkbox"/>	*
<input checked="" type="checkbox"/> 0/0 B	<input checked="" type="checkbox"/>	IPV4 TCP
<input type="checkbox"/> 0/0 B	<input checked="" type="checkbox"/>	IPV4 UDP
<input checked="" type="checkbox"/> 0/0 B	<input checked="" type="checkbox"/>	IPV4 TCP
<input checked="" type="checkbox"/> 0/480 B	<input checked="" type="checkbox"/>	IPV4 ICMP

53 (DNS) none DNS Services

22 (SSH) * none Remote Connections

none Pings

pfSense is developed and maintained by Netgate. © ESP 2004 - 2024. View license.

Part 3: Steps 5-8

Configuring Custom Firewall Rules with pfSense (3e)

LAB GUIDE: 20%

- Part 1: Plan the LAN Firewall Rules
- Part 2: Configure the LAN Firewall Rules
- Part 3: Verify Firewall Rules for the LAN

Section 2: Applied Learning

Section 3: Challenge and Analysis

Part 3: Verify Firewall Rules for the LAN (1/3 completed)

5. Close the Command Prompt window.

Note: In the following steps, you will test your HTTP rule by attempting to access the website at corporationtechs.com. A successful retrieval of the webpage from the web server indicates HTTP traffic is permitted through the LAN interface.

6. From the vWorkstation taskbar, restore the Mozilla Firefox browser window.

7. In the browser navigation bar, type `corporationtechs.com` to send an HTTP request for the website's homepage content.

If Firefox displays the contents of the homepage, you can confirm you have correctly configured your HTTP rule.

corporationtechs.com

CORPORATION TECHS

0° Technology

Complete Administration Automation for the IT professional. Centralized Command Center for all locations. We bring you closer to peace of mind!

Part 3: Steps 9-15

The screenshot shows a Windows desktop environment. In the background, a web browser displays a lab guide titled "Configuring Custom Firewall Rules with pfSense (3e)". The lab guide is at 93% completion and includes the following sections:

- Part 1: Plan the LAN Firewall Rules
- Part 2: Configure the LAN Firewall Rules
- Part 3: Verify Firewall Rules for the LAN

Section 3: Challenge and Analysis is currently active, with sub-sections for Applied Learning and Challenge and Analysis. A "Log in" button is highlighted with a red box. Below the login button, a note states: "A successful connection should reveal three folders in the TargetLinux01 directory: *ftpuser*, *stfuser*, and *user*. If these folders are listed in the right-hand pane of WinSCP (the target directory), you have configured the SSH rule correctly."

Task instructions include: "14. Make a screen capture showing the successful SSH connection in WinSCP." and "15. Close the WinSCP window." A final note says: "This concludes Section 1 of the lab."

In the foreground, a WinSCP window is open, showing a successful connection to a remote host. The left pane shows the local directory structure, and the right pane shows the remote directory structure. The remote directory listing is as follows:

Name	Size	Changed	Rights	Owner
.		10/15/2020 10:43:33 AM	rwxr-xr-x	root
ftpuser		10/15/2020 10:36:22 AM	rwxr-xr-x	1001
stfuser		10/15/2020 12:36:00 PM	rwxr-xr-x	1002
user		6/1/2020 6:29:50 AM	rwxr-xr-x	1000

The desktop taskbar shows various applications, including Chrome, Firefox, and WinSCP. The system tray indicates the time is 4:07 PM on 3/24/2024, with a temperature of 48°F and sunny weather.