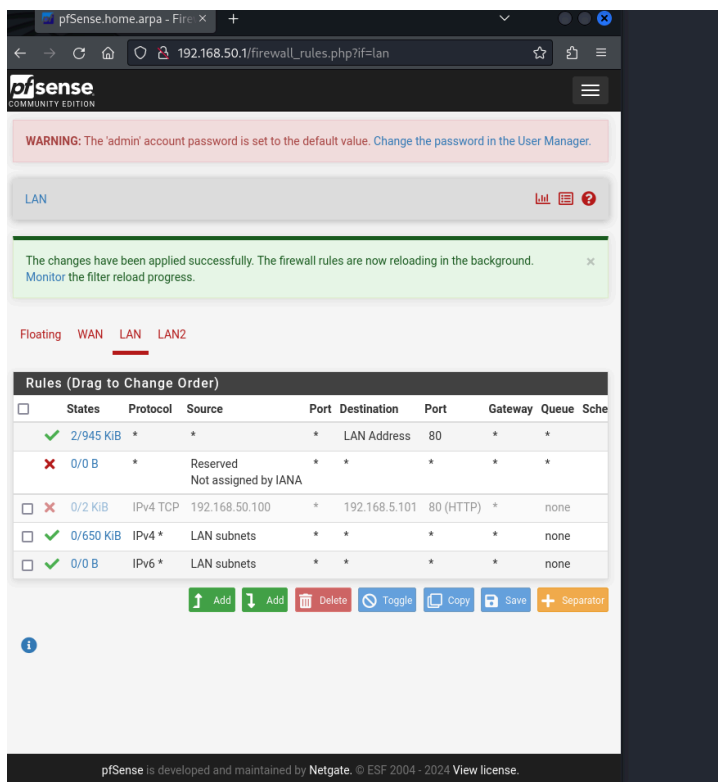


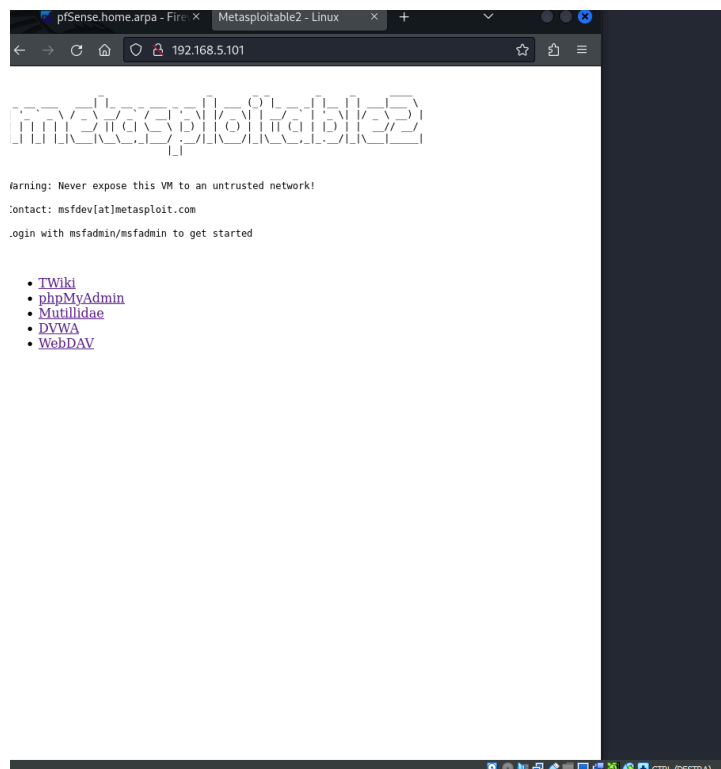
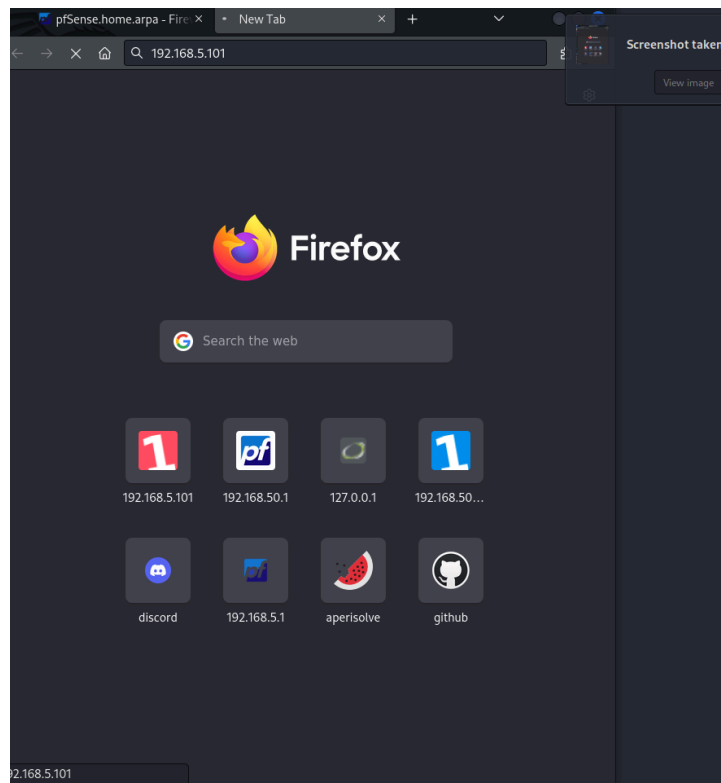
Creazione policy Pfsense



The screenshot shows the pfSense web interface in a browser window. The URL is `192.168.50.1/firewall_rules.php?if=lan`. The page title is "pfSense COMMUNITY EDITION". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, a green success message indicates: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." The interface shows the "LAN" tab selected under the "Filter Rules" section. A table titled "Rules (Drag to Change Order)" displays the current firewall rules. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, and Schedule. The rules listed are:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
✓ 2/945 KIB	*	*	*	LAN Address	80	*	*	
✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	
✗ 0/2 KIB	IPv4 TCP	192.168.50.100	*	192.168.5.101	80 (HTTP)	*	none	
✓ 0/650 KIB	IPv4 *	LAN subnets	*	*	*	*	none	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	

Below the table, there are buttons for "Add", "Add", "Delete", "Toggle", "Copy", "Save", and "Separator". At the bottom, a footer note states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license."



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.

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

Address or Alias

192.168.50.100 /

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

Address or Alias

192.168.5.101 /

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

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

Rule Information

Tracking ID

1710252747