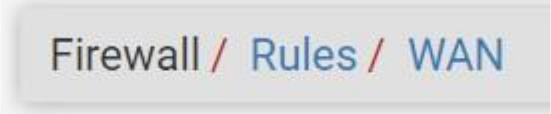
OVERVIEW:

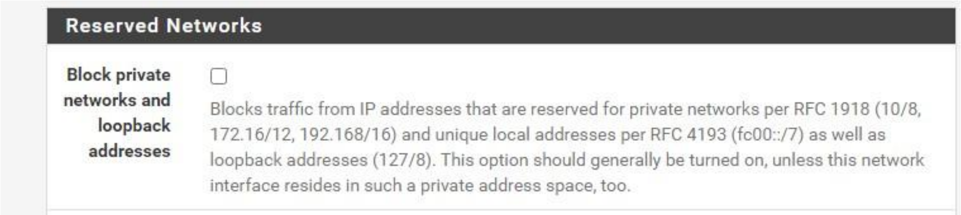
In this lab, I focused on configuring the pfSense firewall to control traffic between the WAN, LAN, and DMZ network segments I had set up. The main goal was to gain hands-on experience with firewalls, setting up rules, and testing connectivity. This lab proved valuable as it simulated a segmented network, giving me the ability to manage communication between devices by configuring firewall rules to either allow or deny traffic. The skills I gained will be helpful outside the classroom for managing network security and configuring firewalls in real-world environments.

ANALYSIS:

I began by creating new firewall rules to manage traffic effectively.



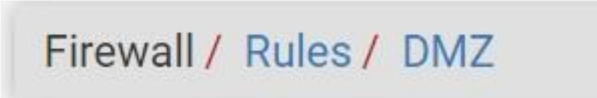
Firewall / Rules / WAN



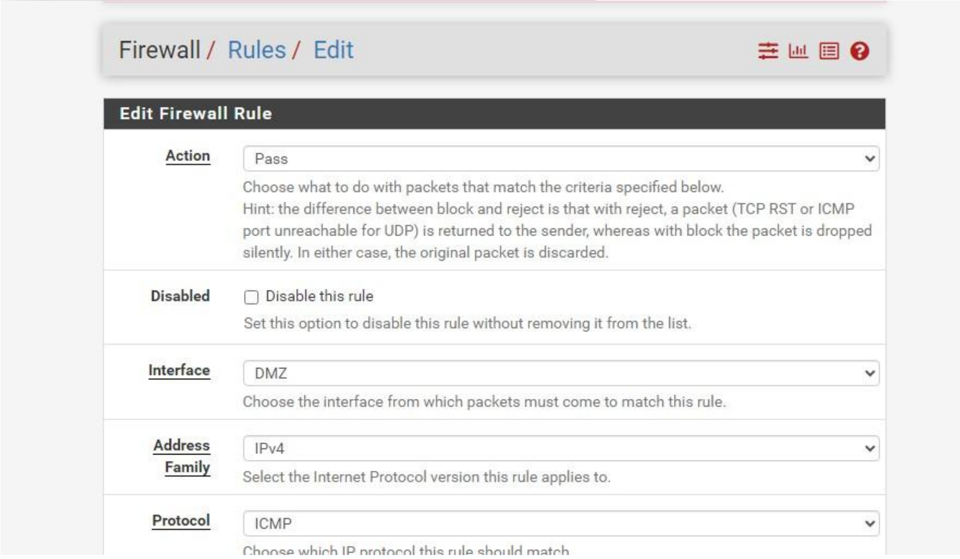
Reserved Networks

Block private networks and loopback addresses □

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.



Firewall / Rules / DMZ



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: DMZ

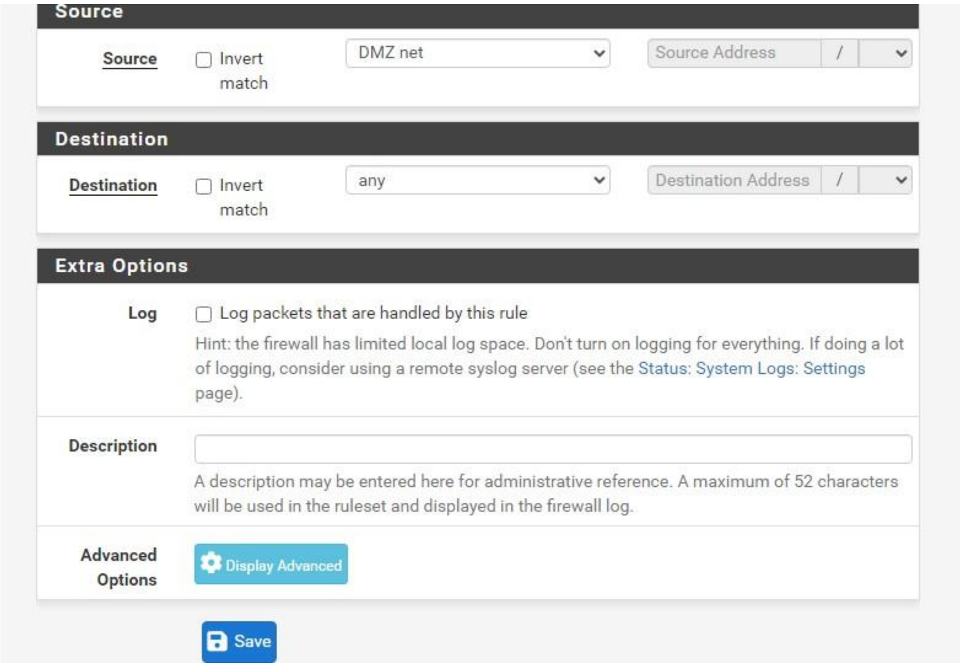
Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: ICMP

Choose which IP protocol this rule should match



Source

Source: □ Invert match | DMZ net | Source Address /

Destination

Destination: □ Invert match | any | Destination Address /

Extra Options

Log: □ Log packets that are handled by this rule

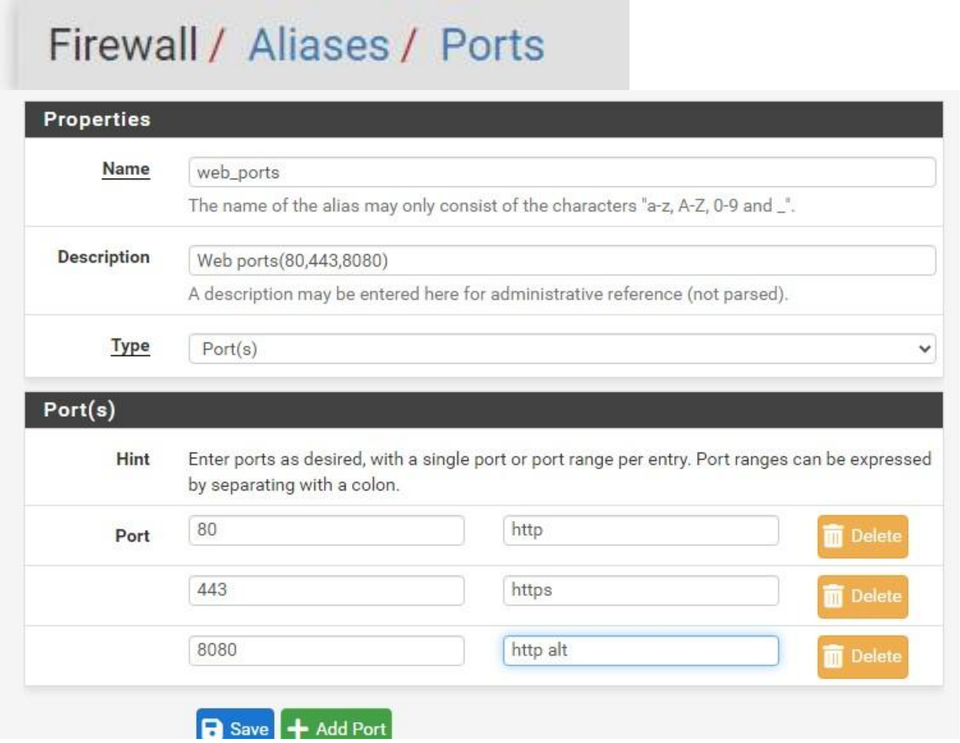
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

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

To simplify future configurations, I created an alias for common services such as HTTP, HTTPS, and HTTP alternate ports. This alias would help streamline rule creation and improve network management.



Firewall / Aliases / Ports

Properties

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

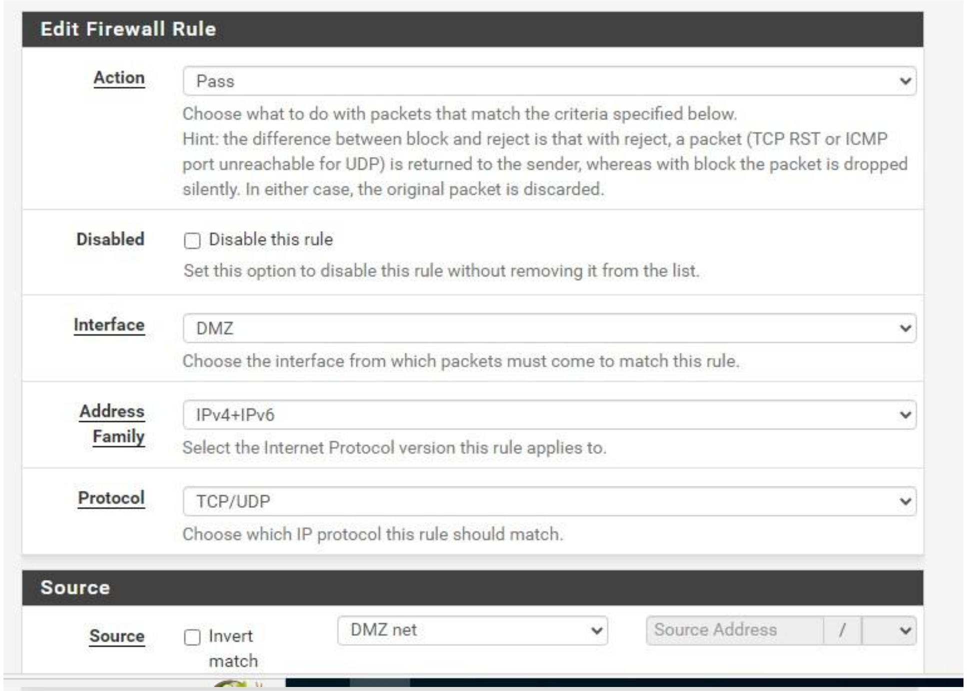
Description: Web ports(80,443,8080)
A description may be entered here for administrative reference (not parsed).

Type: Port(s)

Port(s)

Hint: Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	80	http
	443	https
	8080	http alt

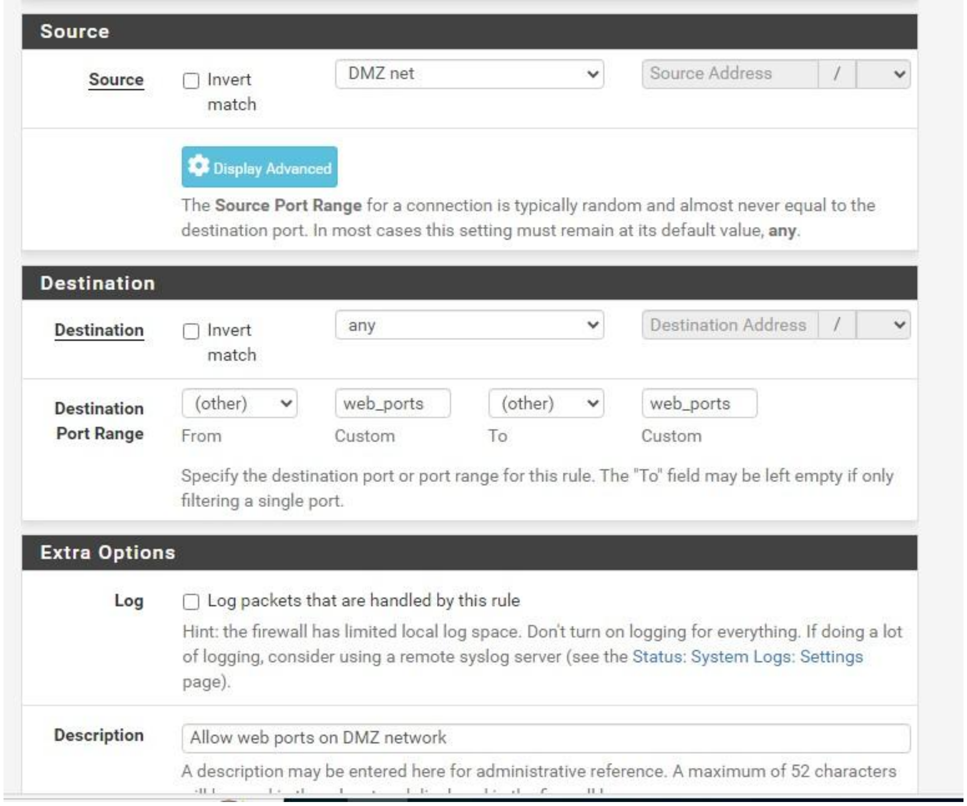


Edit Firewall Rule

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	DMZ Choose the interface from which packets must come to match this rule.
Address Family	IPv4+IPv6 Select the Internet Protocol version this rule applies to.
Protocol	TCP/UDP Choose which IP protocol this rule should match.

Source

Source	□ Invert match	DMZ net	Source Address /



Source

Source	□ Invert match	DMZ net	Source Address /

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**.

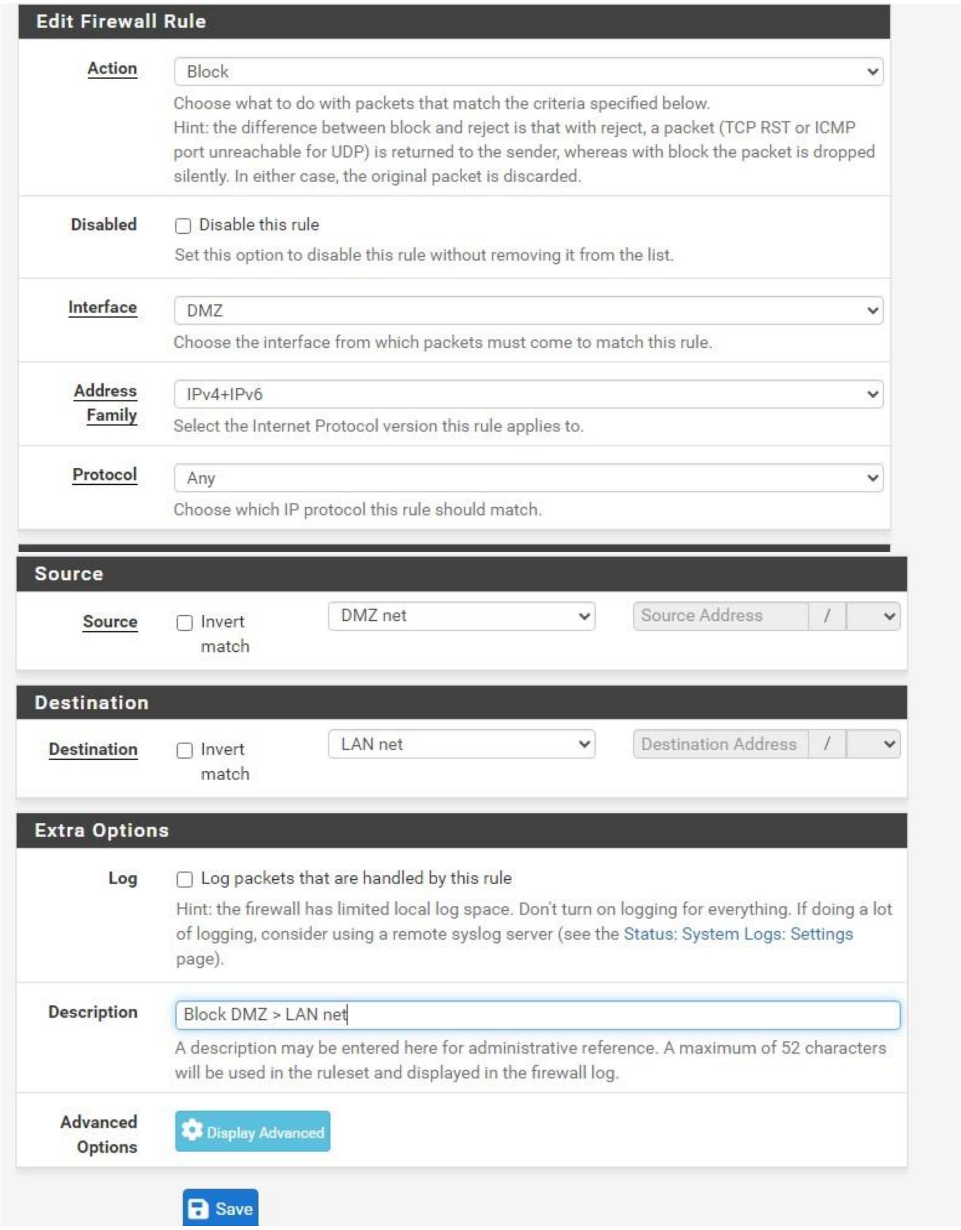
Destination

Destination	□ Invert match	any	Destination Address /	
Destination Port Range	(other) From	web_ports Custom	(other) To	web_ports 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	Allow web ports on DMZ network A description may be entered here for administrative reference. A maximum of 52 characters



Edit Firewall Rule

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: DMZ

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

Address Family: IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | DMZ net | Source Address /

Destination

Destination: □ Invert match | LAN net | Destination Address /

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).

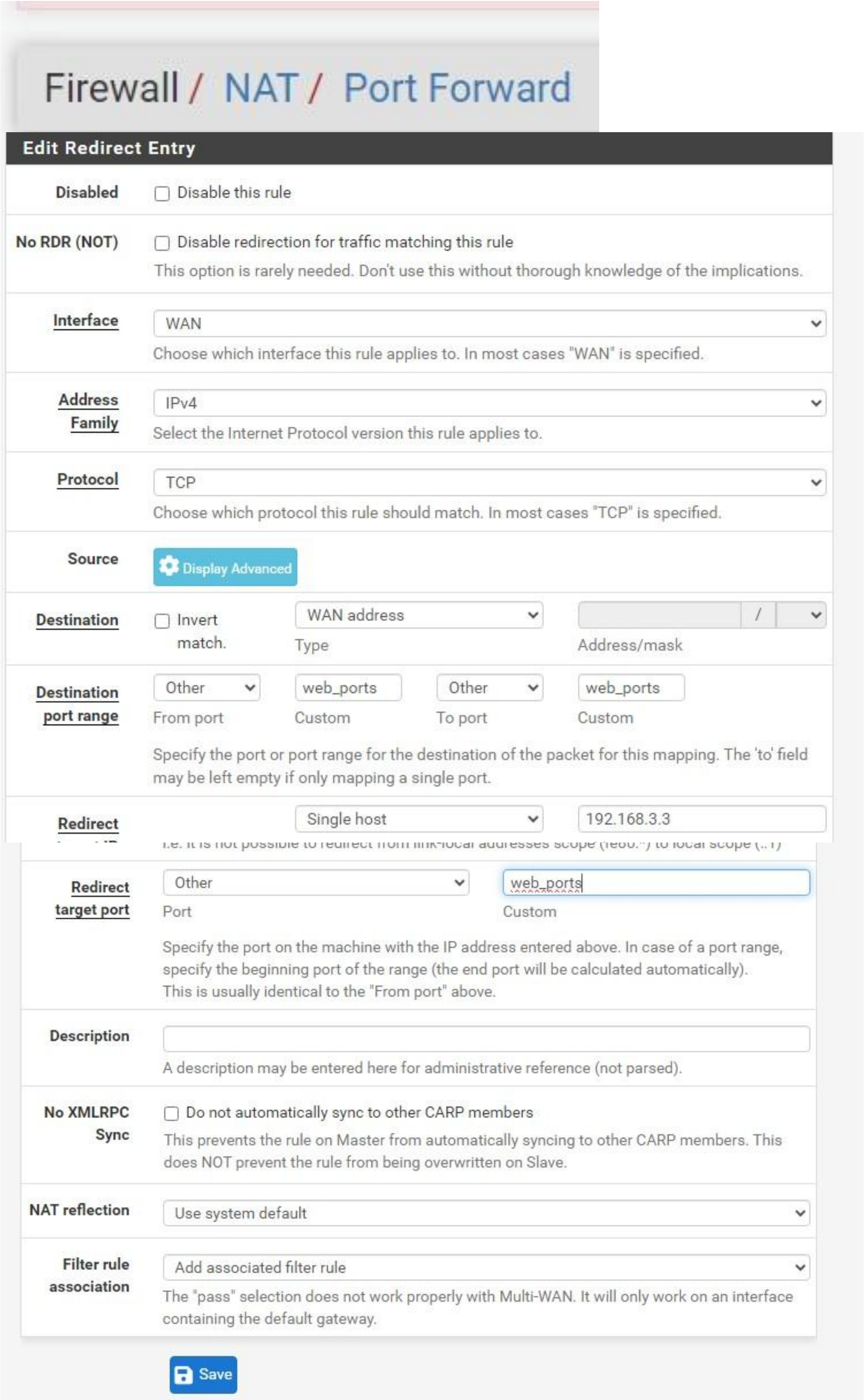
Description: Block DMZ > LAN net

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

Next, I configured a NAT firewall rule to ensure proper traffic routing between the internal network and the external interface.



Firewall / NAT / Port Forward

Edit Redirect Entry

Disabled □ Disable this rule

No RDR (NOT) □ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination □ Invert match. | Type: WAN address | Address/mask: /

Destination port range From port: Other | Custom: web_ports | To port: Other | Custom: web_ports

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.

Redirect Single host | 192.168.3.3

i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port Port: Other | Custom: web_ports

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.

Description

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

No XMLRPC Sync □ Do not automatically sync to other CARP members

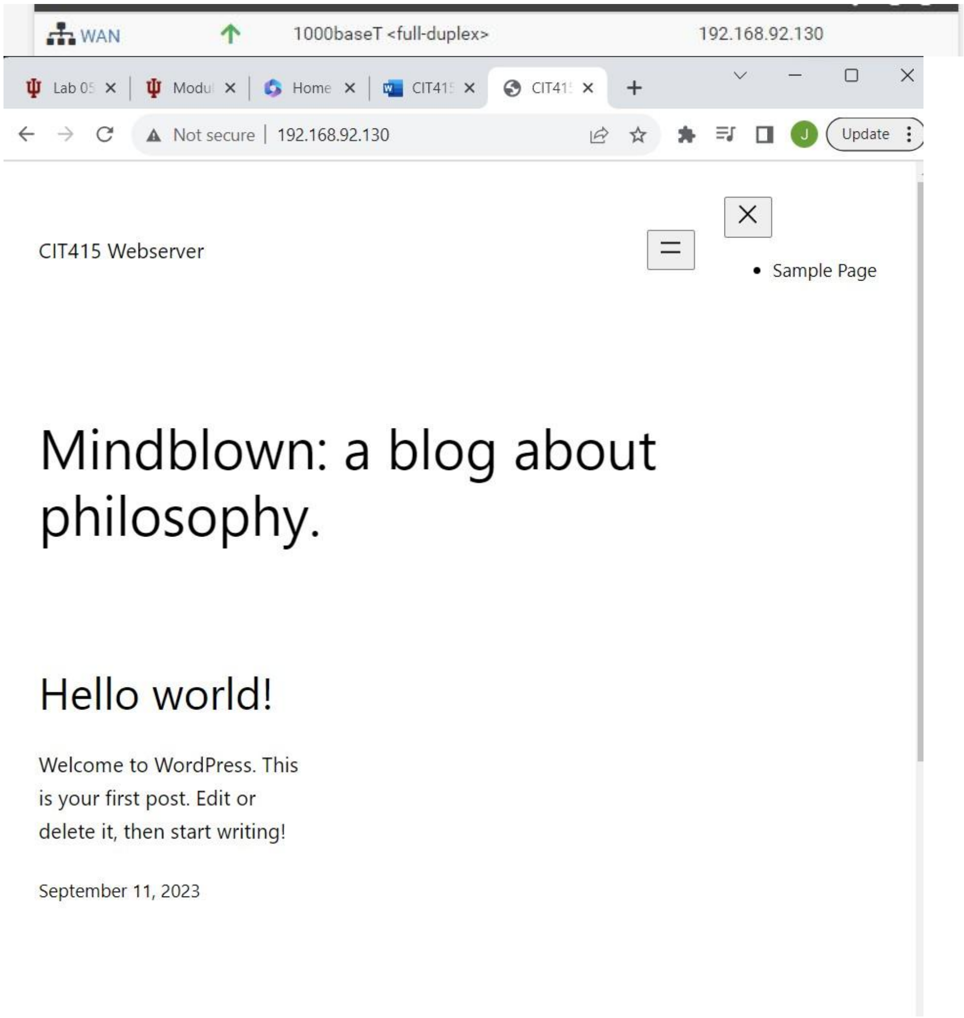
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Add associated filter rule

The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Once the rule was in place, I tested the setup by entering the WAN IP address on the host PC, and successfully accessed the webpage, confirming that the configuration was working as expected.



WAN 1000baseT <full-duplex> 192.168.92.130

Not secure | 192.168.92.130

CIT415 Webserver

- Sample Page

Mindblown: a blog about philosophy.

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

September 11, 2023