Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024

Lab 5.4.5: Network Security - Perimeter Firewall Configuration on a pfSense Security Appliance

From TestOut CompTIA Security+ Course

In this lab I will be setting up Perimeter Firewall on a hypothetical enterprise network using a pfSense Security Appliance.

The scenario for this lab is as follows:

“You work as the IT security administrator for a small corporate network. You recently placed a Web server in the demilitarized zone (DMZ). You need to configure the perimeter firewall on the network security appliance (pfSense) to allow access from the WAN to the Web server in the DMZ using both HTTP and HTTPs. You also want to allow all traffic from the LAN network to the DMZ network.

In this lab, your task is to:

- Access the pfSense management console:
  - Username: admin
  - Password: P@ssw0rd (zero)
- Create and configure a firewall rule to pass HTTP traffic from the WAN to the Web server in the DMZ.
- Create and configure a firewall rule to pass HTTPS traffic from the WAN to the Web server in the DMZ.

○ Use the following table when creating the HTTP and HTTPS firewall rules:

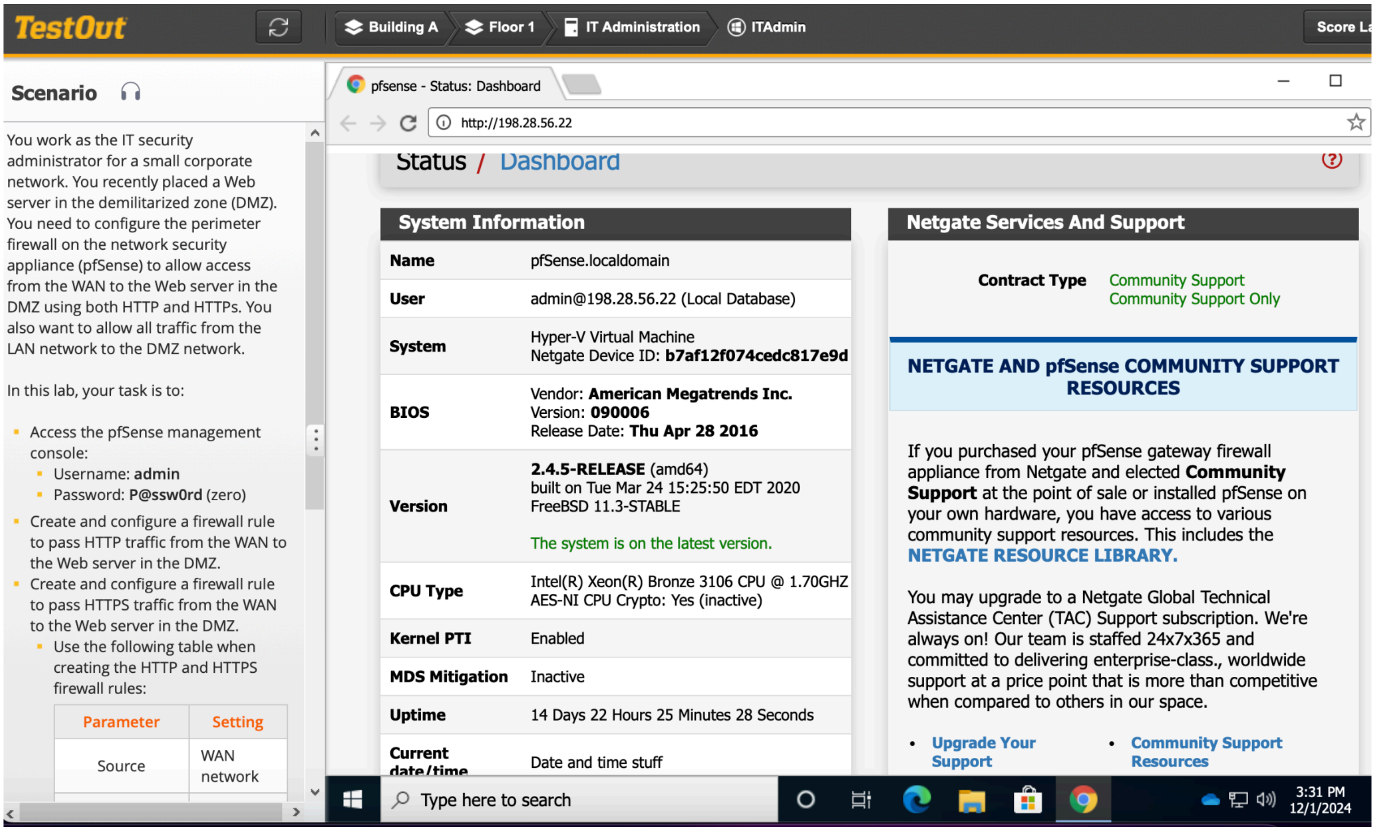
Parameter	Setting
Source	WAN network
Destination port/service	HTTP (80), HTTPS (443)

Destination	A single host
IP address for host	172.16.1.5
Descriptions	For HTTP: HTTP from WAN to DMZ For HTTPS: HTTPS from WAN to DMZ

- Create and configure a firewall rule to pass all traffic from the LAN network to the DMZ network. Use the description *LAN to DMZ Any*.”

First, I will go ahead and login to the pfSense Security portal by navigating to the specified IP address in my browser and entering the credentials provided. Let’s log in now.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Scenario

You work as the IT security administrator for a small corporate network. You recently placed a Web server in the demilitarized zone (DMZ). You need to configure the perimeter firewall on the network security appliance (pfSense) to allow access from the WAN to the Web server in the DMZ using both HTTP and HTTPs. You also want to allow all traffic from the LAN network to the DMZ network.

In this lab, your task is to:

- Access the pfSense management console:
  - Username: **admin**
  - Password: **P@ssw0rd** (zero)
- Create and configure a firewall rule to pass HTTP traffic from the WAN to the Web server in the DMZ.
- Create and configure a firewall rule to pass HTTPS traffic from the WAN to the Web server in the DMZ.
  - Use the following table when creating the HTTP and HTTPS firewall rules:

Parameter	Setting
Source	WAN network

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@198.28.56.22 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: **b7af12f074cedc817e9d**
BIOS	Vendor: **American Megatrends Inc.** Version: **090006** Release Date: **Thu Apr 28 2016**
Version	**2.4.5-RELEASE** (amd64) built on Tue Mar 24 15:25:50 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHZ AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	14 Days 22 Hours 25 Minutes 28 Seconds
Current date/time	Date and time stuff

Netgate Services And Support

Contract Type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY.**

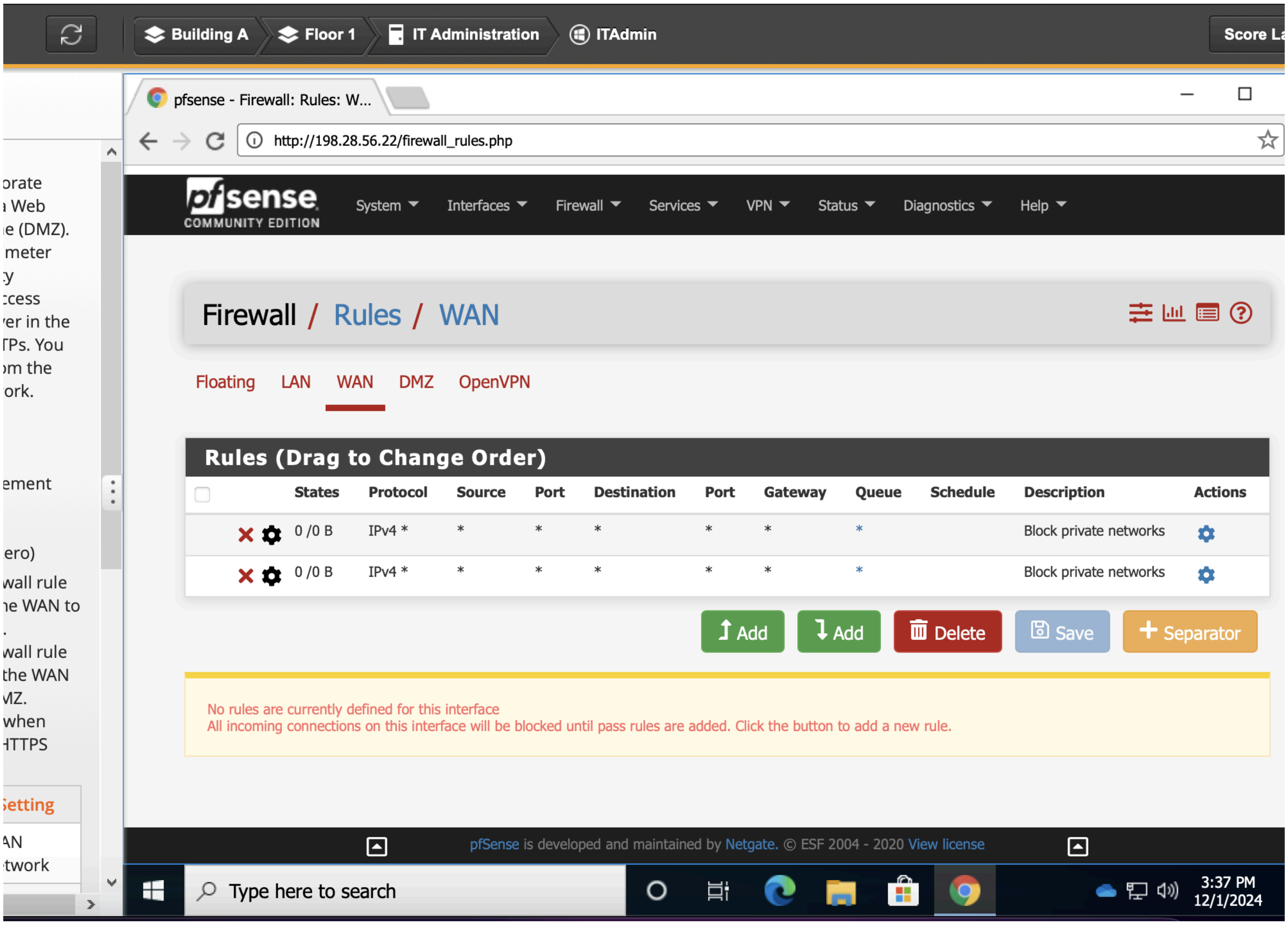
You may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class., worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources

Now that I am in my pfSense security appliance, my first task is to Create a Firewall Rule to pass all HTTP (non-secure) traffic from our WAN to the Web Server that’s located in the DMZ Network Security Zone.

I’ll head to **Firewall > Rules** to create this rule. I’ll click the “**Add”** button and then click the “**Pass”** button on the config screen that comes out.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



orate
ı Web
ıe (DMZ).
meter
:y
:cess
ver in the
TPs. You
ɔm the
ork.

ement

ero)
wall rule
he WAN to
.
wall rule
the WAN
MZ.
when
HTTPS

Setting
AN
twork

Firewall / Rules / WAN

Floating LAN WAN DMZ OpenVPN

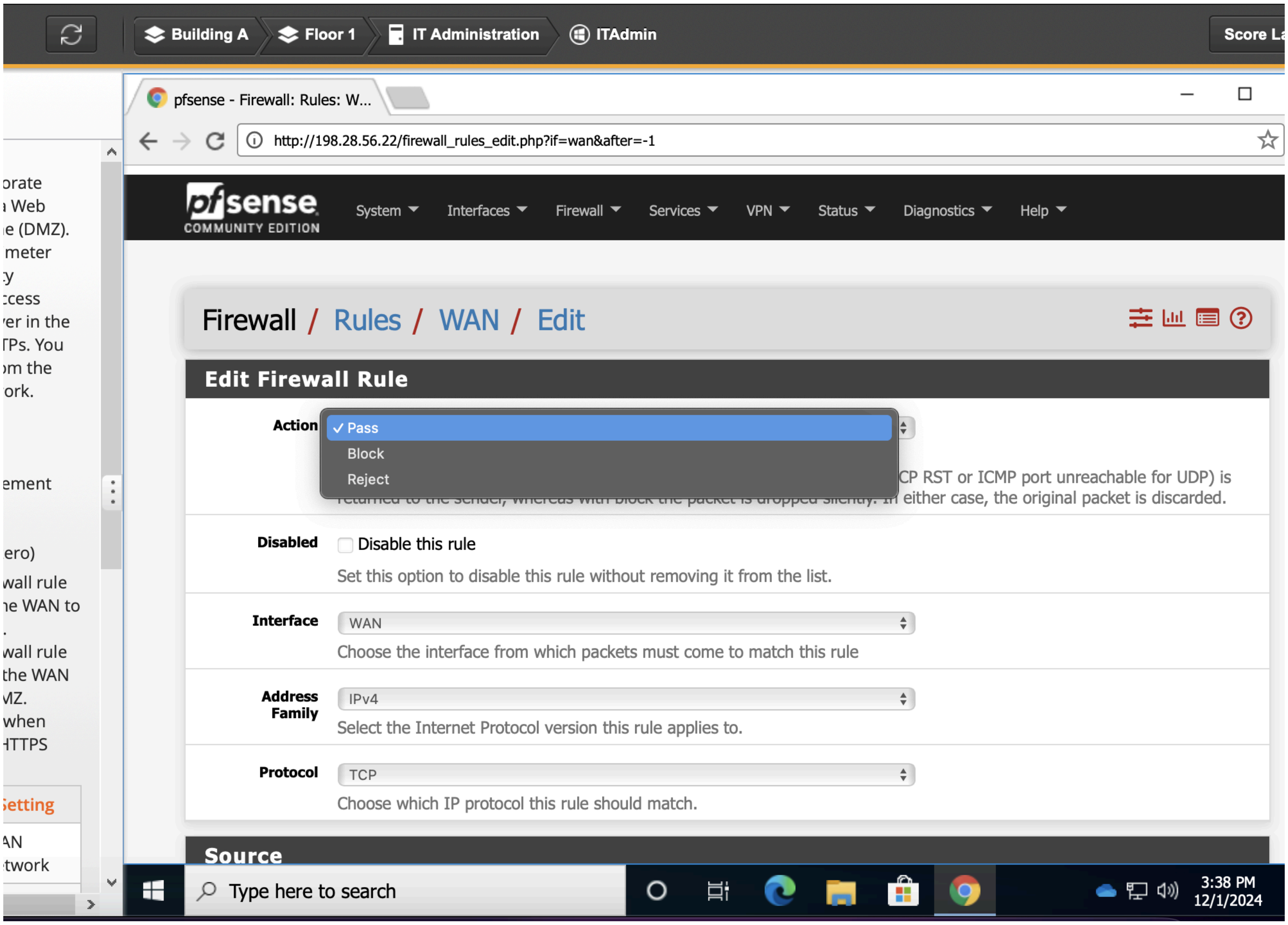
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✕ ⚙	0 /0 B	IPv4 *	*	*	*	*	*	*		Block private networks	⚙
	✕ ⚙	0 /0 B	IPv4 *	*	*	*	*	*	*		Block private networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Firewall / Rules / WAN / Edit

Edit Firewall Rule

Action: ✓ Pass | Block | Reject

...CP 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

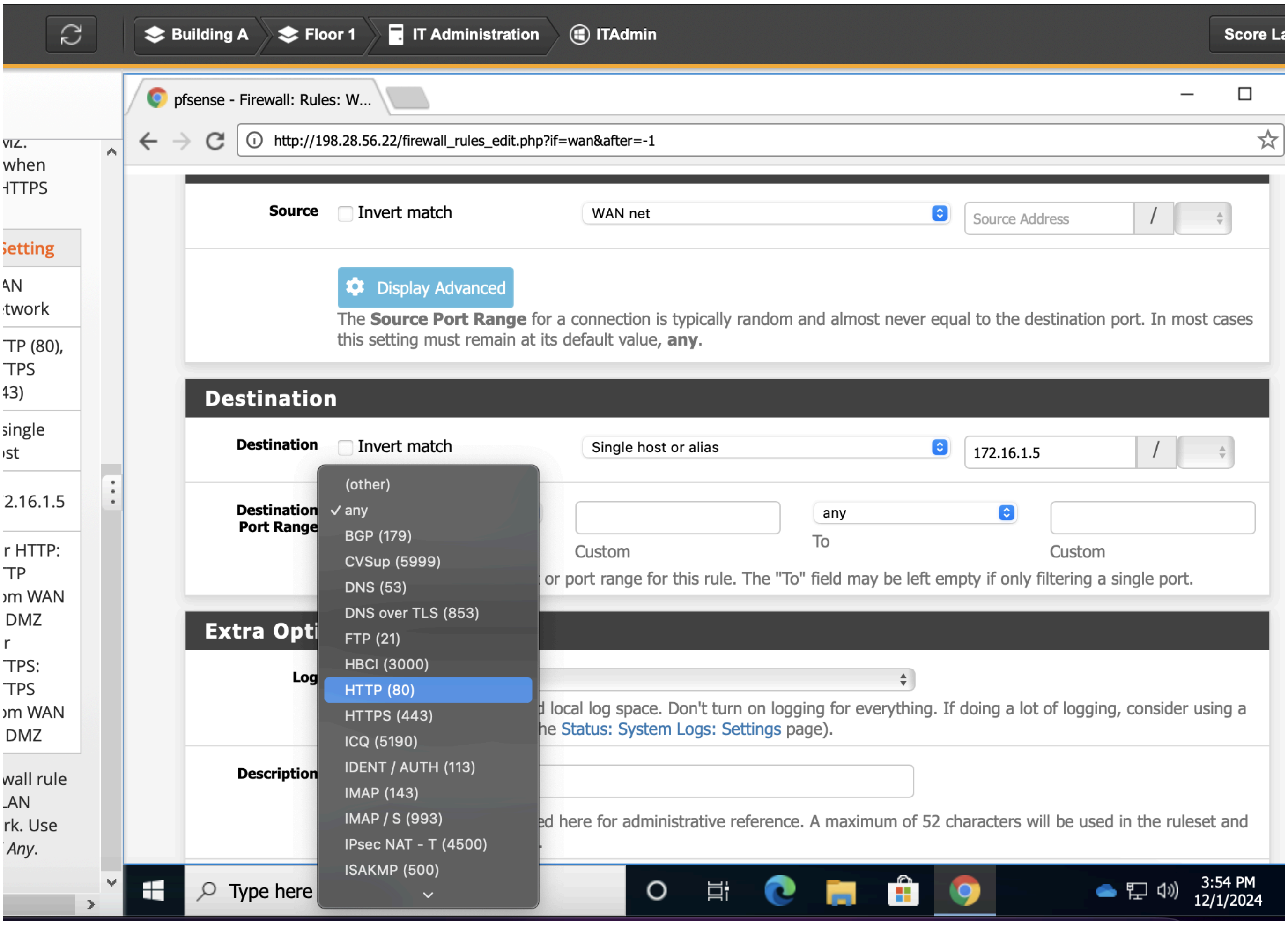
Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Under **Source** I'll put **WAN net ,** since we are passing the WAN traffic to the DMZ , and under the **Destination** I'll add the Webserver. In the Lab scenario it tells us the that Webserver Host is 172.16.1.5. I'll enter that here in the Destination field.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Source □ Invert match WAN 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 Single host or alias 172.16.1.5 /

Destination Port Range any

or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Opti

Log

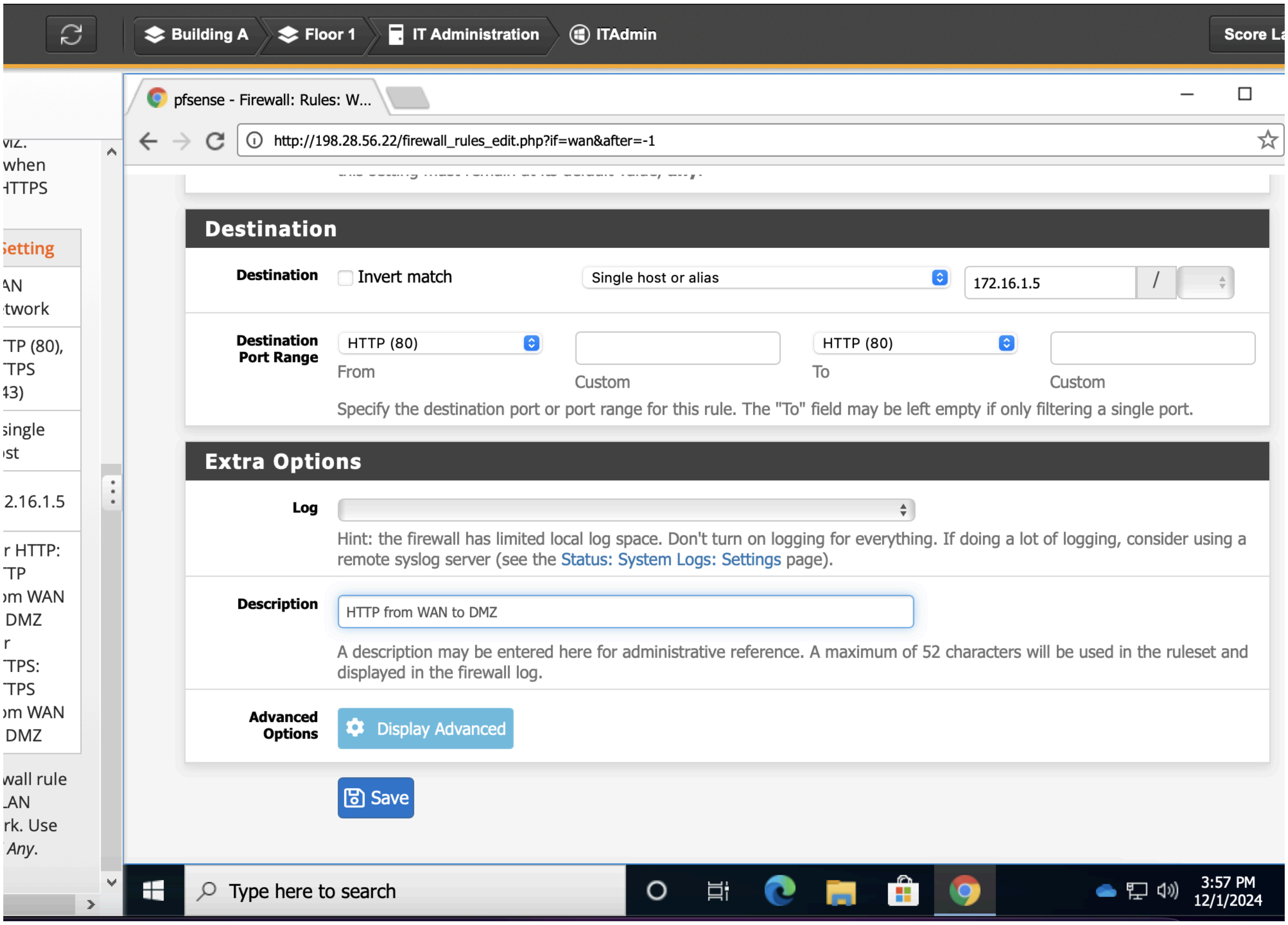
d local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a he Status: System Logs: Settings page).

Description

ed here for administrative reference. A maximum of 52 characters will be used in the ruleset and

Notice that I’m adding only 1 port here. That’s because Port 80 is for HTTP traffic and 445 is for HTTPS. The lab **ONLY WANTS US** to pass **HTTP Traffic** to the webserver **NOT HTTPs.** After entering the destination IP and destination port we can go under Extra options and add a descriptor for this rule. The Lab would like us to use **“HTTP from WAN to DMZ”** as the descriptor.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



pfsense - Firewall: Rules: W...

http://198.28.56.22/firewall_rules_edit.php?if=wan&after=-1

Destination

Destination: □ Invert match | Single host or alias | 172.16.1.5 /

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

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: HTTP from WAN to DMZ

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

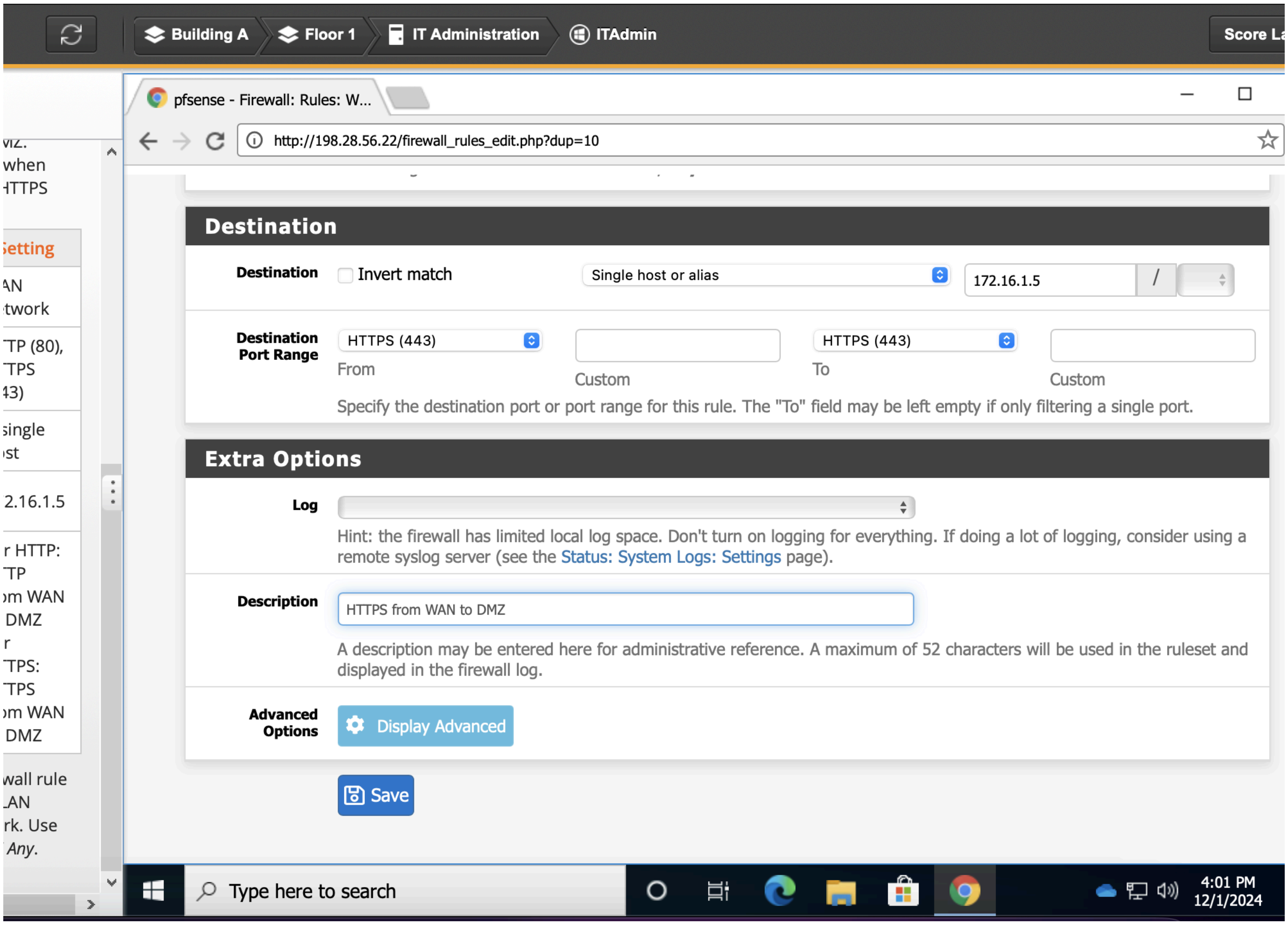
Save

After everything is set, I’ll click the Blue Save button to save these changes.

Now we need to pass HTTPS traffic to this Webserver too! Each port you would like to assign a rule to should be done as a separate rule. Since we pretty much just configured everything we need except of course changing the Port number and Descriptor, we can simply hit the copy button next to the rule in the **Firewall > Rules** and set the ports accordingly.

Hitting the Copy button brings up an identical form we just saved for the HTTP rule we just need to change the protocol.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



http://198.28.56.22/firewall_rules_edit.php?dup=10

Destination

Destination: □ Invert match | Single host or alias | 172.16.1.5 /

Destination Port Range: From HTTPS (443), Custom; To HTTPS (443), 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: □

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: HTTPS from WAN to DMZ

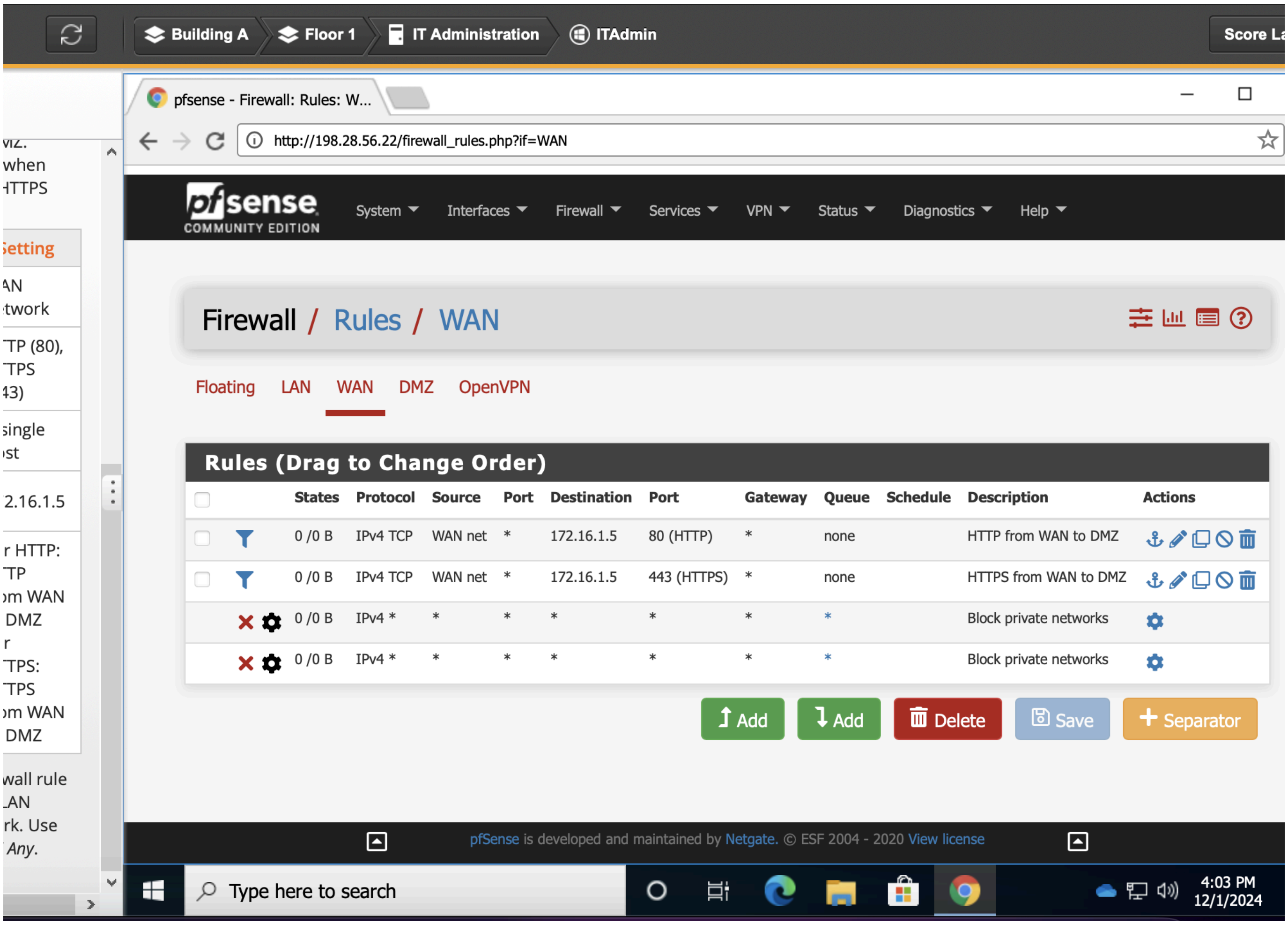
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

Save

After changing the port number from **80 to 443** and also changing the descriptor from "**HTTP from WAN to DMZ**" to "**HTTPS from WAN to DMZ**" we can simply hit the save button!

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Firewall / Rules / WAN

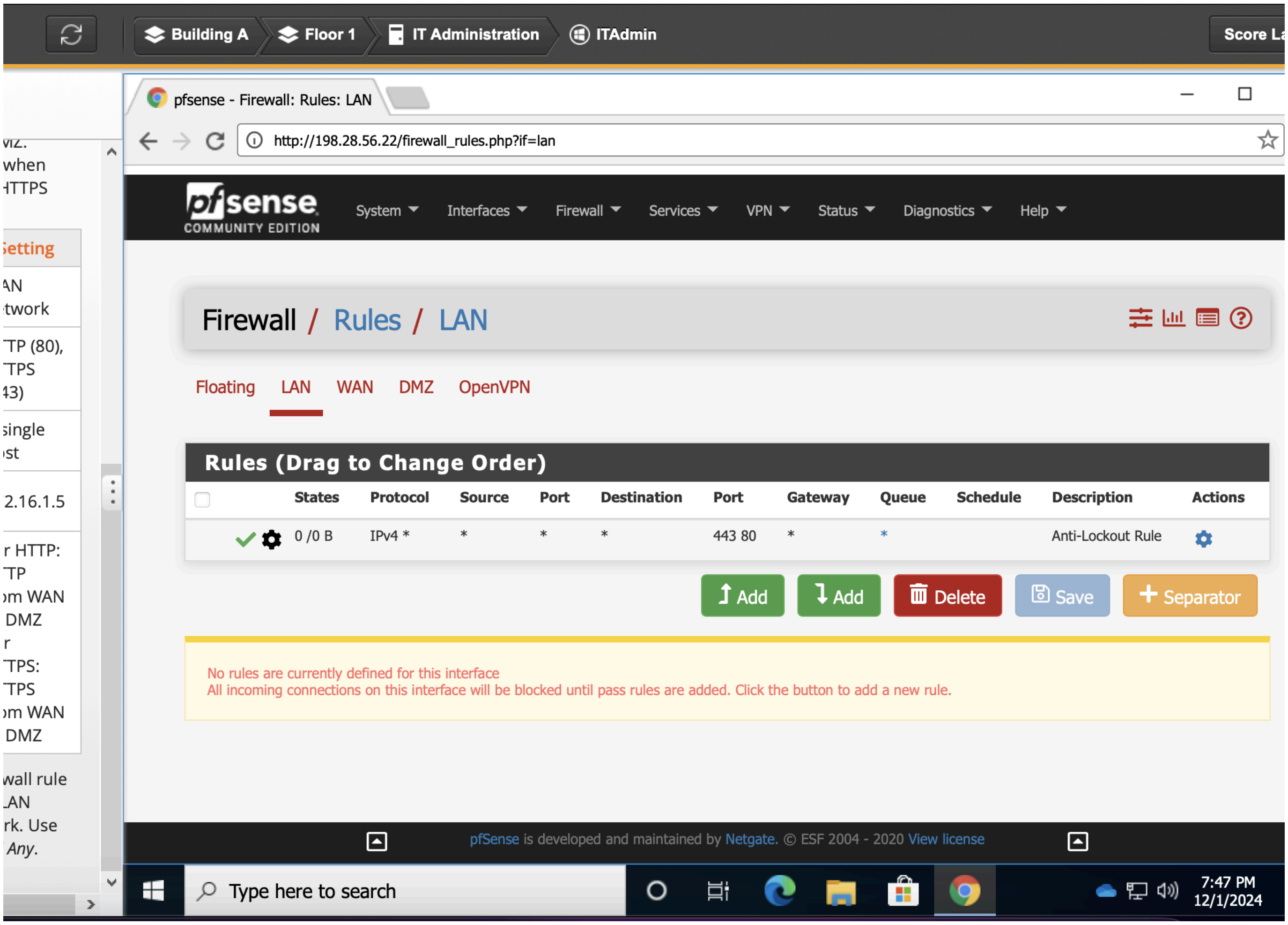
Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□		0 /0 B	IPv4 TCP	WAN net	*	172.16.1.5	80 (HTTP)	*	none		HTTP from WAN to DMZ	
□		0 /0 B	IPv4 TCP	WAN net	*	172.16.1.5	443 (HTTPS)	*	none		HTTPS from WAN to DMZ	
	✕	0 /0 B	IPv4 *	*	*	*	*	*	*		Block private networks	
	✕	0 /0 B	IPv4 *	*	*	*	*	*	*		Block private networks	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

Now that we've passed HTTP and HTTPS traffic to the webserver in the DMZ we also would like to allow LAN traffic to it as well. This could be for internal management purposes so let's set it up now. We'll need to change breadcrumb views on this same page (above pictured) from **WAN** to **LAN** in order to add that rule.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓ ⚙	0 /0 B	IPv4 *	*	*	*	443 80	*	*		Anti-Lockout Rule	⚙

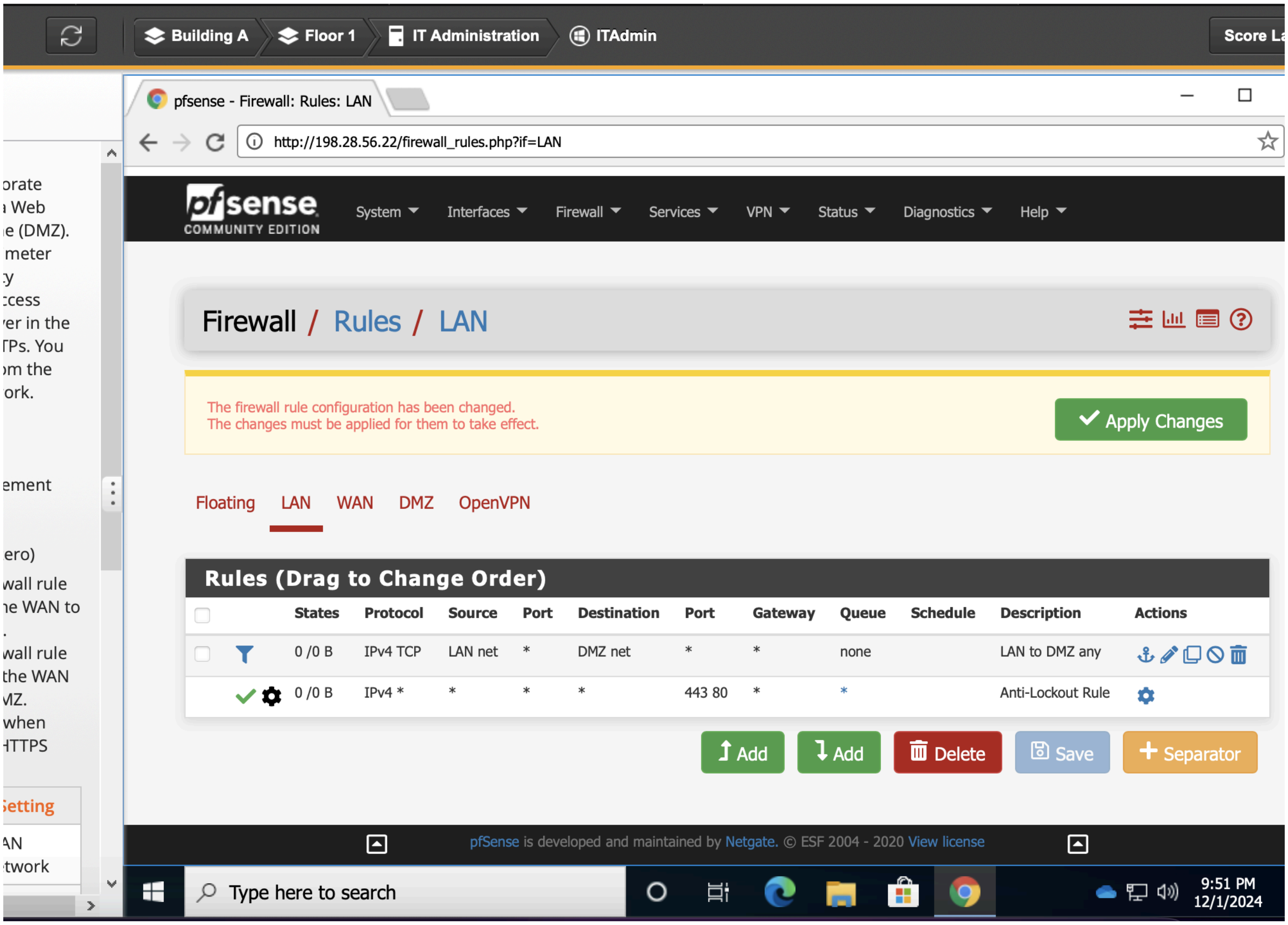
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

I’ll click the **Add** button to add this new rule.

Once the configuration page shows up, I’ll begin to set the given values. We will want to pass LAN traffic to the DMZ net. For the **Action** I will assign **Pass,** and scrolling down to **Source** I’ll assign **LAN net.** This will pass any traffic from ANY host to any other host within the DMZ network.

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024



http://198.28.56.22/firewall_rules.php?if=LAN

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

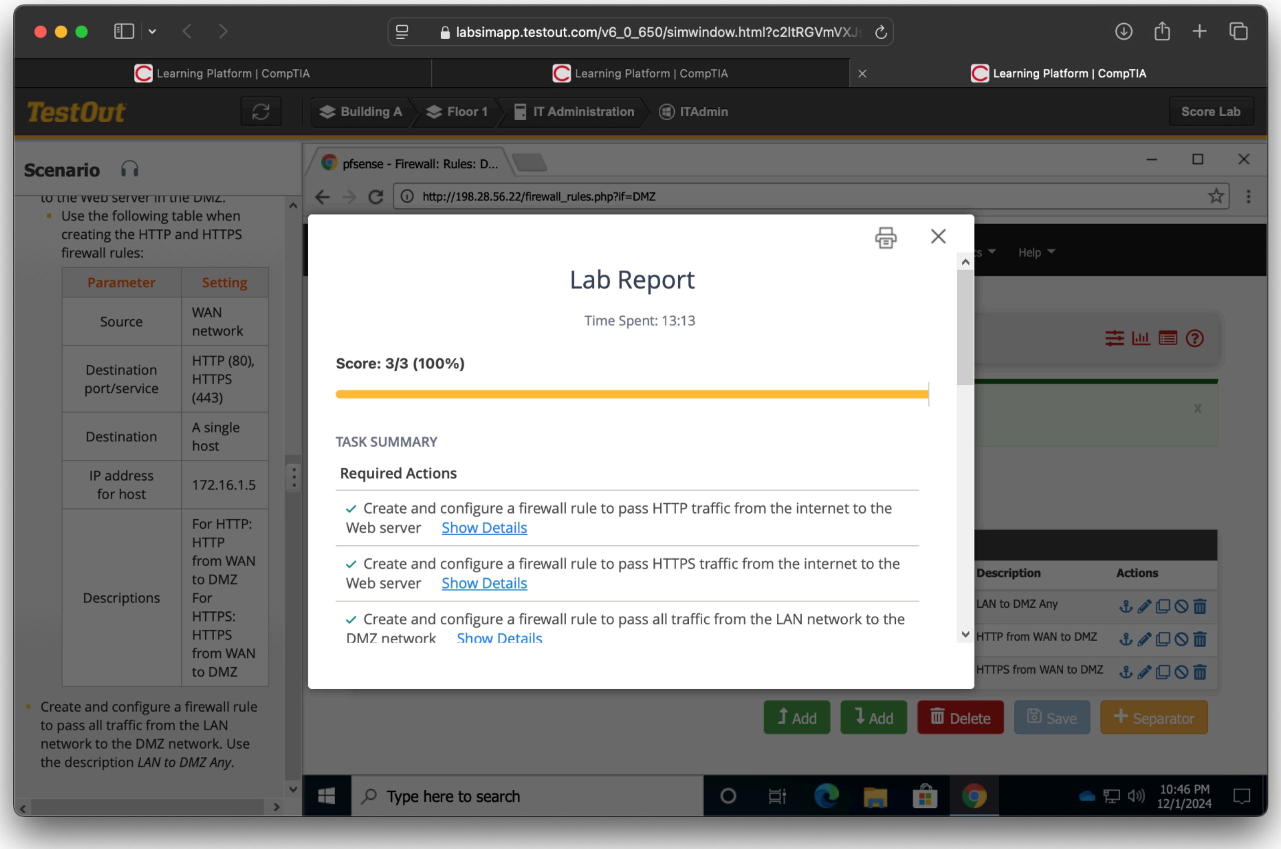
Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□		0 /0 B	IPv4 TCP	LAN net	*	DMZ net	*	*	none		LAN to DMZ any	
	✓	0 /0 B	IPv4 *	*	*	*	443 80	*	*		Anti-Lockout Rule	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020 View license

Ensure that after all rules are applied the DMZ breadcrumb menu looks like this:

Robert Carpenter
github.com/robertmcarpenter
Sun November 24th 2024


labsimapp.testout.com/v6_0_650/simwindow.html?c2ltRGVmVXJ
Learning Platform | CompTIA
Learning Platform | CompTIA
Learning Platform | CompTIA
TestOut
Building A
Floor 1
IT Administration
ITAdmin
Score Lab
Scenario
pfsense - Firewall: Rules: D...
http://198.28.56.22/firewall_rules.php?if=DMZ
Help
Description
Actions
LAN to DMZ Any
HTTP from WAN to DMZ
HTTPS from WAN to DMZ
Add
Add
Delete
Save
Separator
Type here to search
10:46 PM
12/1/2024

to the Web server in the DMZ.

- Use the following table when creating the HTTP and HTTPS firewall rules:

Parameter	Setting
Source	WAN network
Destination port/service	HTTP (80), HTTPS (443)
Destination	A single host
IP address for host	172.16.1.5
Descriptions	For HTTP: HTTP from WAN to DMZ For HTTPS: HTTPS from WAN to DMZ

- Create and configure a firewall rule to pass all traffic from the LAN network to the DMZ network. Use the description *LAN to DMZ Any*.

Lab Report

Time Spent: 13:13

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

✓ Create and configure a firewall rule to pass HTTP traffic from the internet to the Web server Show Details

✓ Create and configure a firewall rule to pass HTTPS traffic from the internet to the Web server Show Details

✓ Create and configure a firewall rule to pass all traffic from the LAN network to the DMZ network Show Details

This now concludes this lab! In this lab, I created 3 rules:

1. Pass HTTP (80) traffic from WAN to DMZ net
2. Pass HTTPs (443) traffic from the WAN to the DMZ
3. Pass all traffic regardless of port number from LAN to DMZ