HW03 - Firewalls

UBNetDef Systems Security(SysSec)

September 23, 2021

UBNetDef

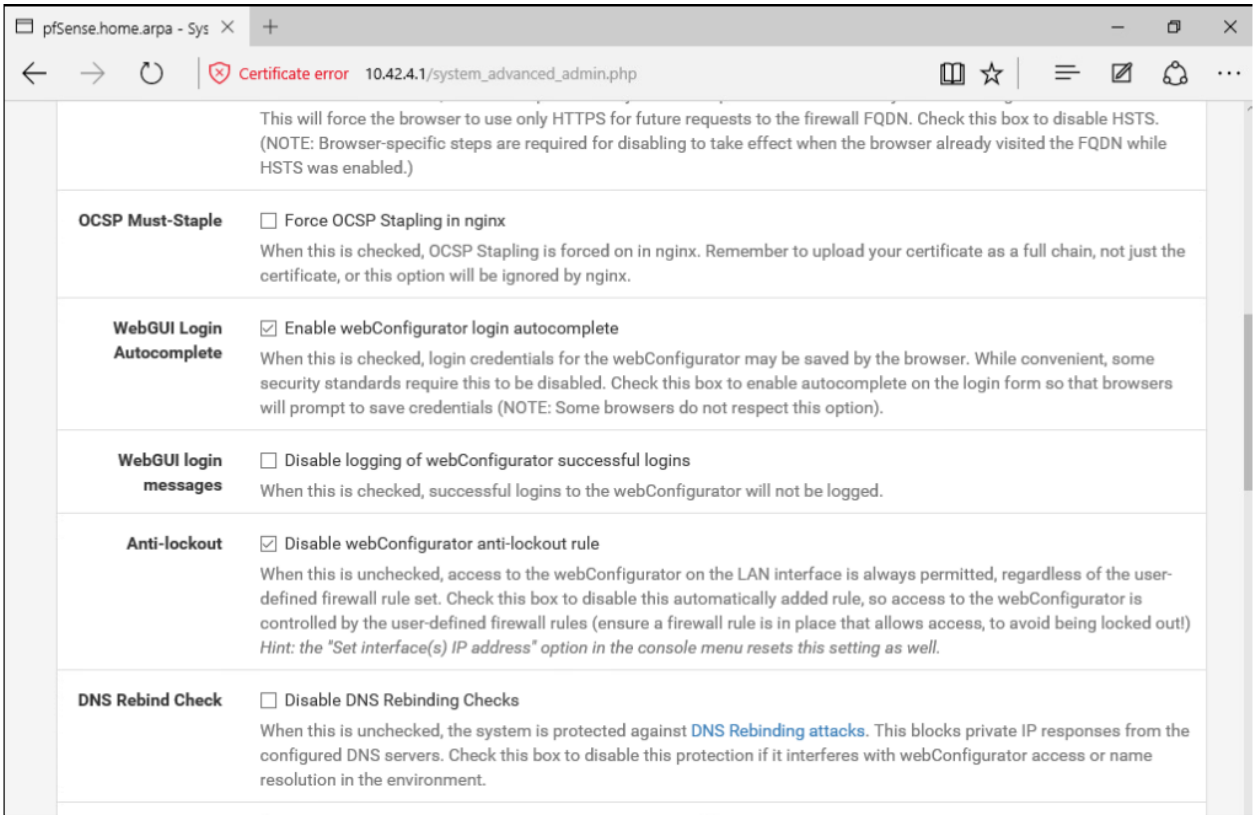
SUBMITTED BY

AKHILESH ANAND UNDRALLA

TABLE OF CONTENTS

Designate One Machine to Manage your Firewall:

By default, Anti-lockout Rule is enabled to prevent locking an administrator out of the web interface. To Disable this, select System > Advanced page from main menu and check the box under Anti-lockout section and click Save.



This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)

OCSP Must-Staple
☐ Force OCSP Stapling in nginx
When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.

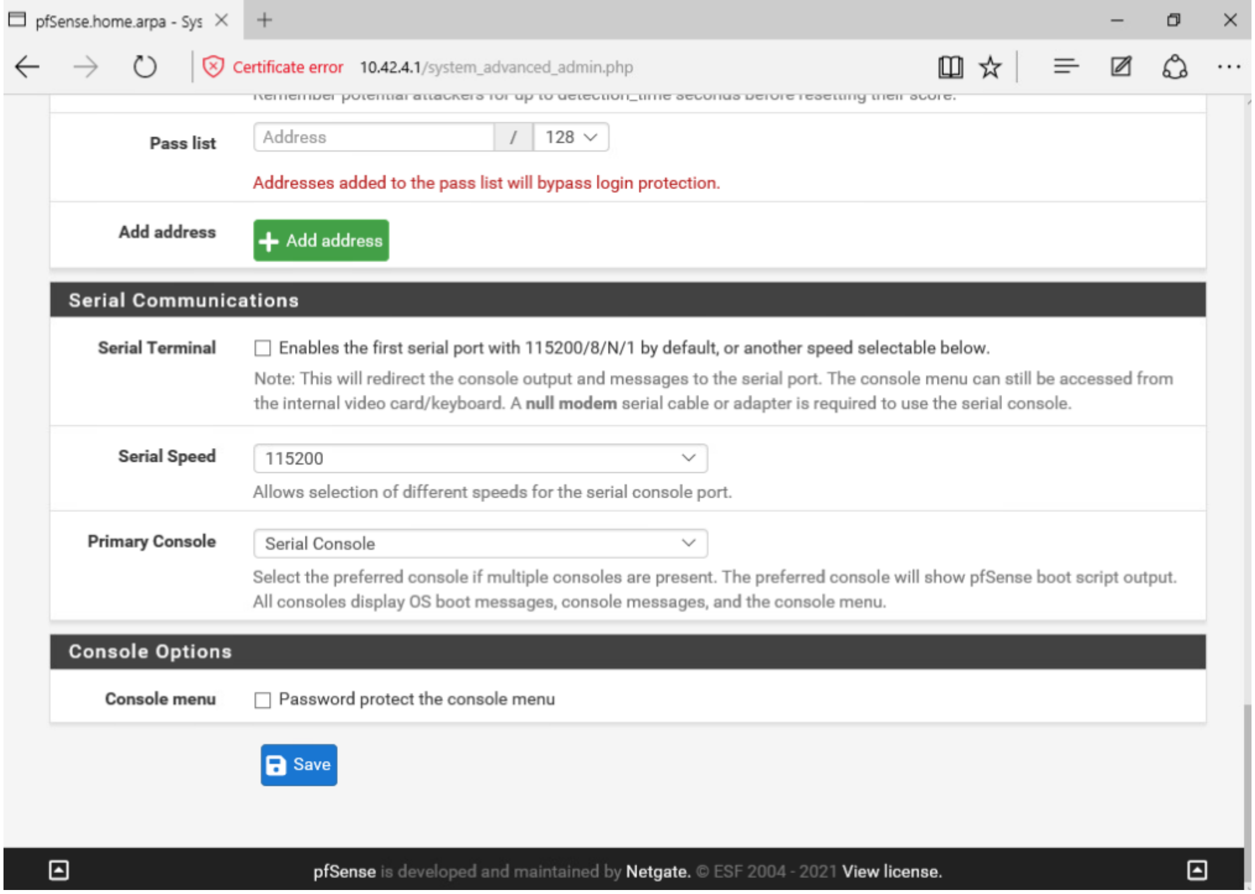
WebGUI Login Autocomplete
☑ Enable webConfigurator login autocomplete
When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

WebGUI login messages
☐ Disable logging of webConfigurator successful logins
When this is checked, successful logins to the webConfigurator will not be logged.

Anti-lockout
☑ Disable webConfigurator anti-lockout rule
When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

DNS Rebind Check
☐ Disable DNS Rebinding Checks
When this is unchecked, the system is protected against DNS Rebinding attacks. This blocks private IP responses from the configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in the environment.

Figure: Disabling the Anti-lockout rule



Remember potential attackers for up to detection_time seconds before resetting their score.

Pass list: Address / 128

Addresses added to the pass list will bypass login protection.

Add address: Add address

Serial Communications

Serial Terminal: □ Enables the first serial port with 115200/8/N/1 by default, or another speed selectable below.

Note: This will redirect the console output and messages to the serial port. The console menu can still be accessed from the internal video card/keyboard. A **null modem** serial cable or adapter is required to use the serial console.

Serial Speed: 115200

Allows selection of different speeds for the serial console port.

Primary Console: Serial Console

Select the preferred console if multiple consoles are present. The preferred console will show pfSense boot script output. All consoles display OS boot messages, console messages, and the console menu.

Console Options

Console menu: □ Password protect the console menu

Save

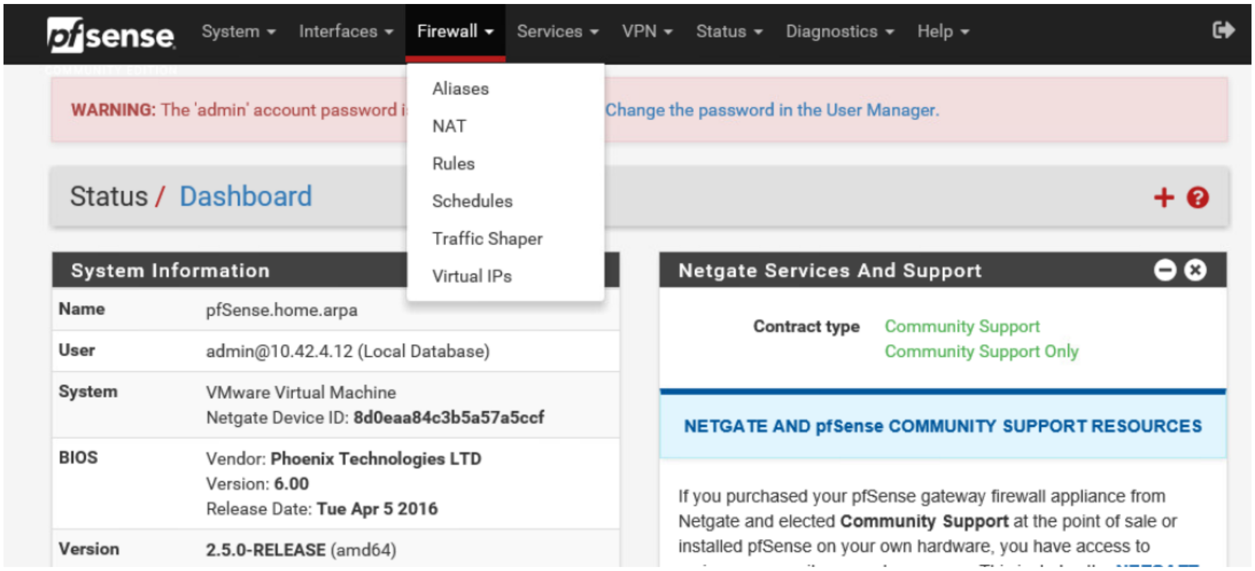
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

Figure: Saving the setting to disable the Anti-lockout rule

Steps required to create firewall rules:

Login in to pfSense from web browser with http://10.42.4.1

Select Firewall from Main Menu and then Rules



WARNING: The 'admin' account password i Change the password in the User Manager.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@10.42.4.12 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **8d0eaa84c3b5a57a5ccf**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Tue Apr 5 2016**
Version	**2.5.0-RELEASE** (amd64)

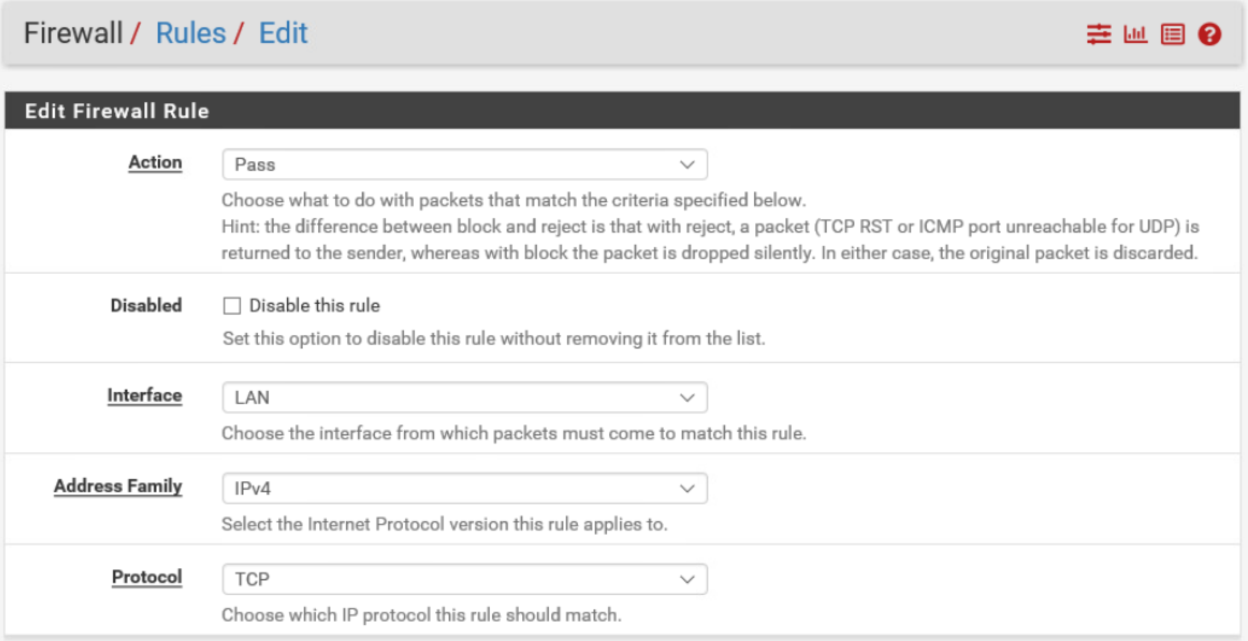
Netgate Services And Support

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

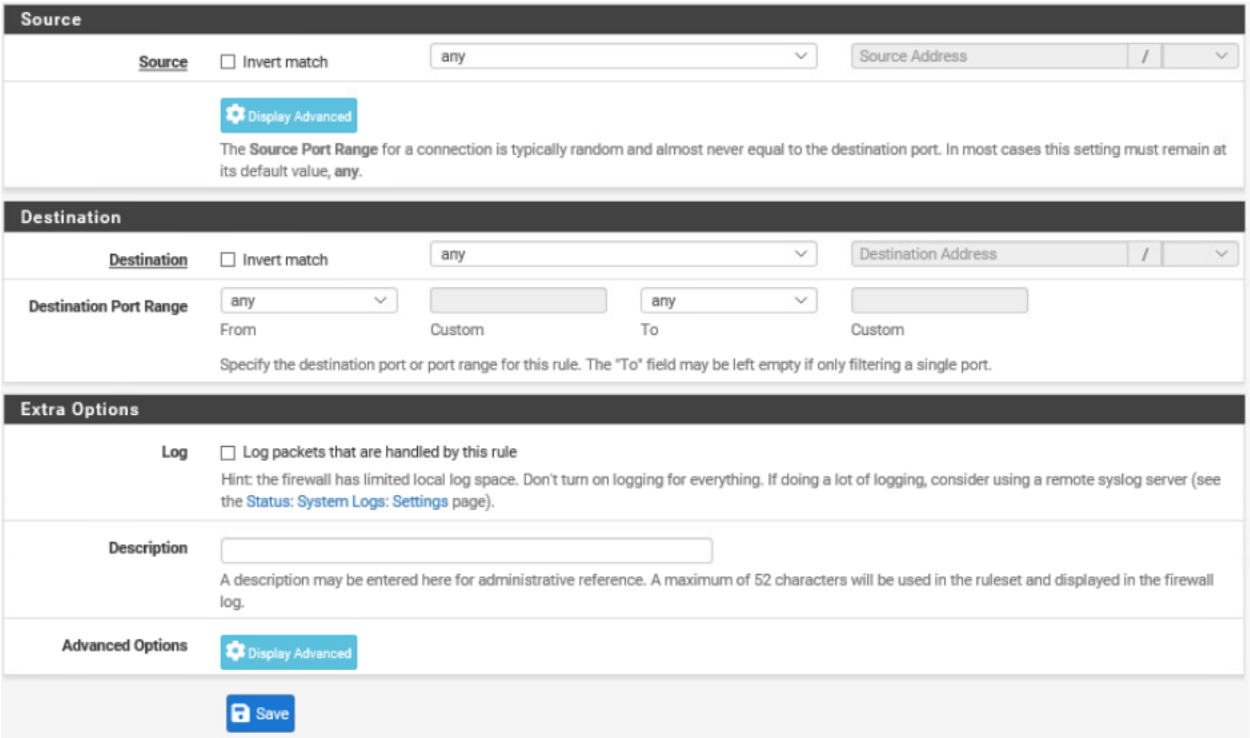
In the LAN tab, Select Add (Add rule to the top of the list)



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	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 /

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	any		any	
	From	Custom	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).

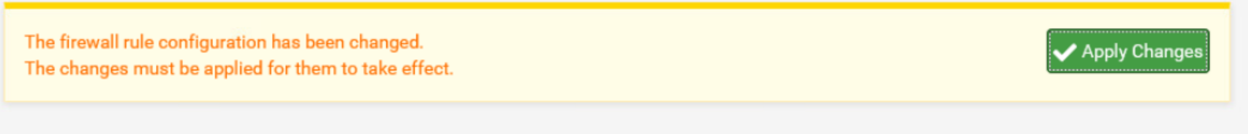
Description

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.

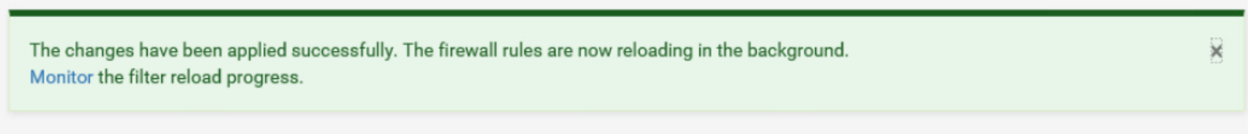
Advanced Options

Action option specifies whether the rule will pass, block, or reject traffic to the outside
Disabled option is to disable a rule while it still shows in the firewall rules screen, but the rule will appear grayed out to indicate its disabled state.
Interface LAN, the interface receiving traffic to be controlled.
Address Family IPv4(Selected) includes rules to select among IPv4, IPv6, or both IPv4+IPv6 traffic.
Protocol TCP(Selected) rule ICMP will show an additional drop down box to select the ICMP Subtype.
Source LAN net should be selected
Destination any
Destination Port Range Select the destination port that needs to be filtered. (Example HTTPS 443)
Log this rule will be logged to the firewall log
Description Give a description here for reference(optional) to describe the purpose of the rule. The maximum length is 52 characters.

Click on Save at the bottom of screen and “Apply Changes” later to apply given settings for the new rule.

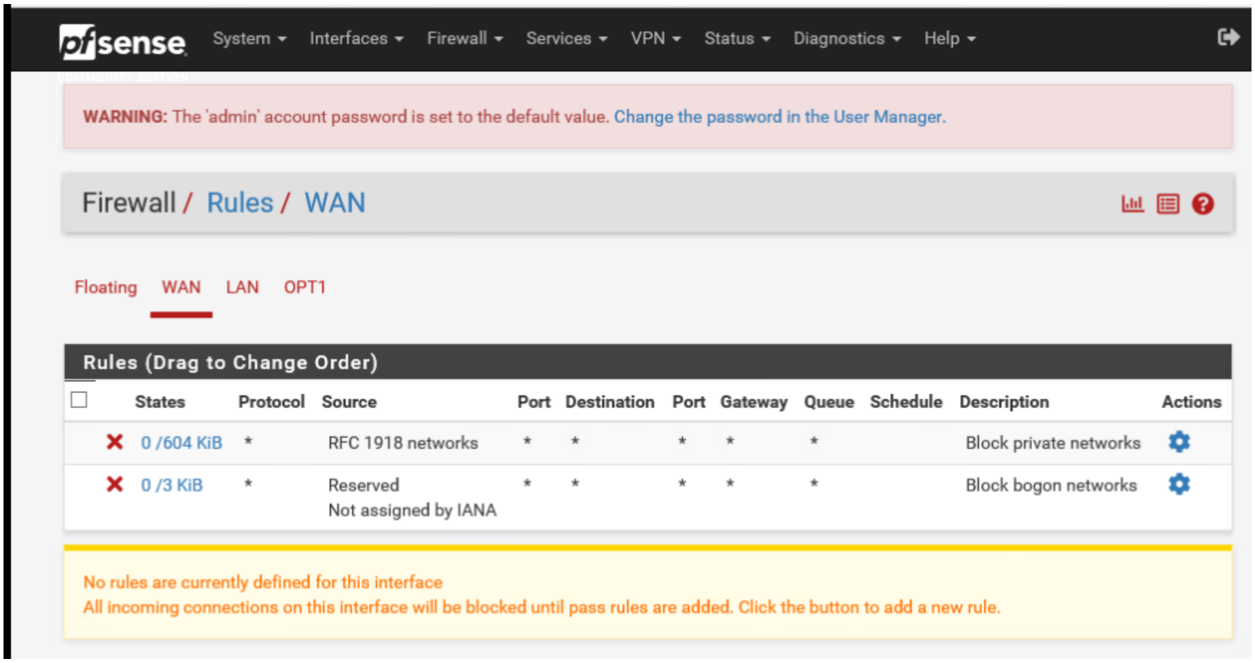


The firewall rule configuration has been changed.
The changes must be applied for them to take effect.



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

All of the firewall rules in the list view of the firewall rules in PFSense:



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

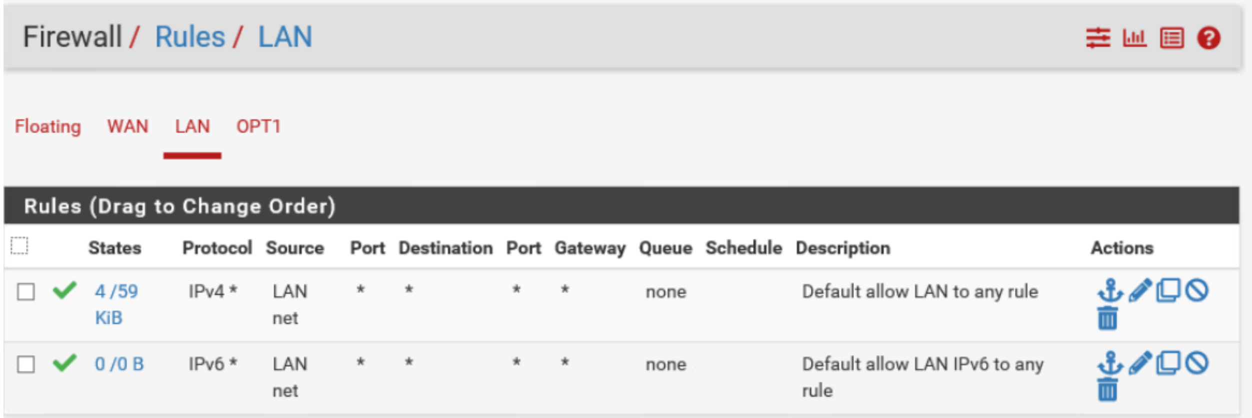
Firewall / Rules / WAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✕ 0 /604 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✕ 0 /3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon 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.

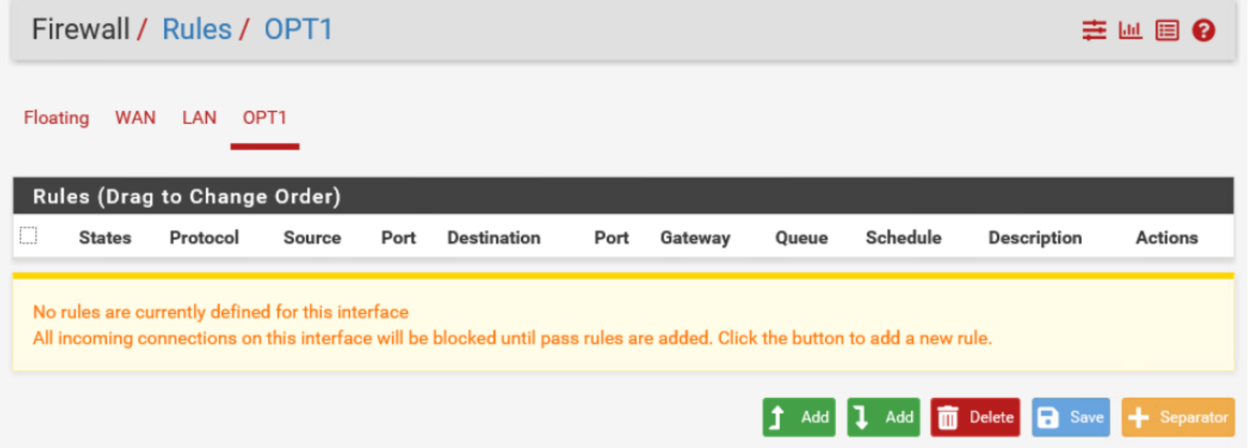


Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓ 4 /59 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ❐ ⊘ 🗑
□	✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ❐ ⊘ 🗑



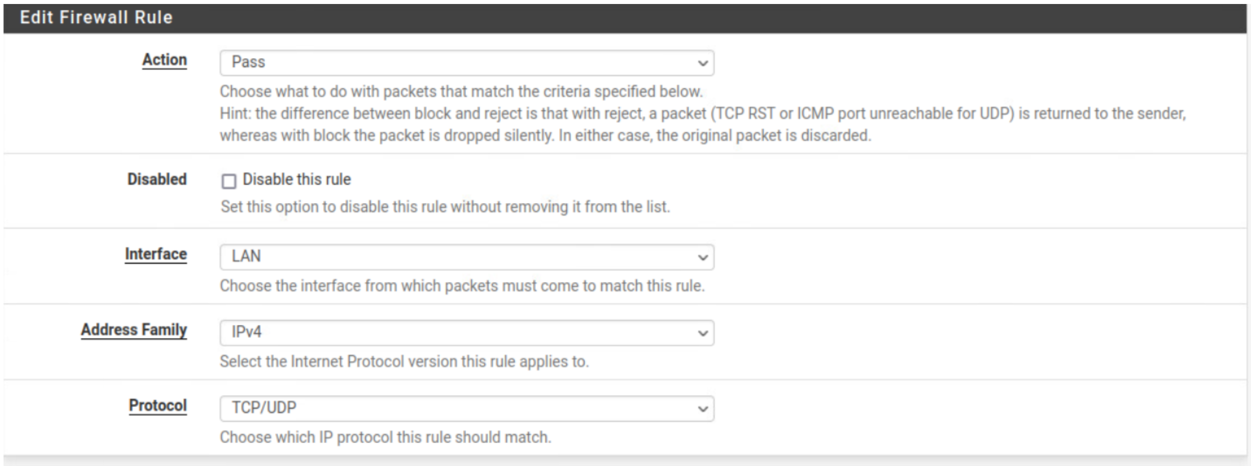
Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

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.

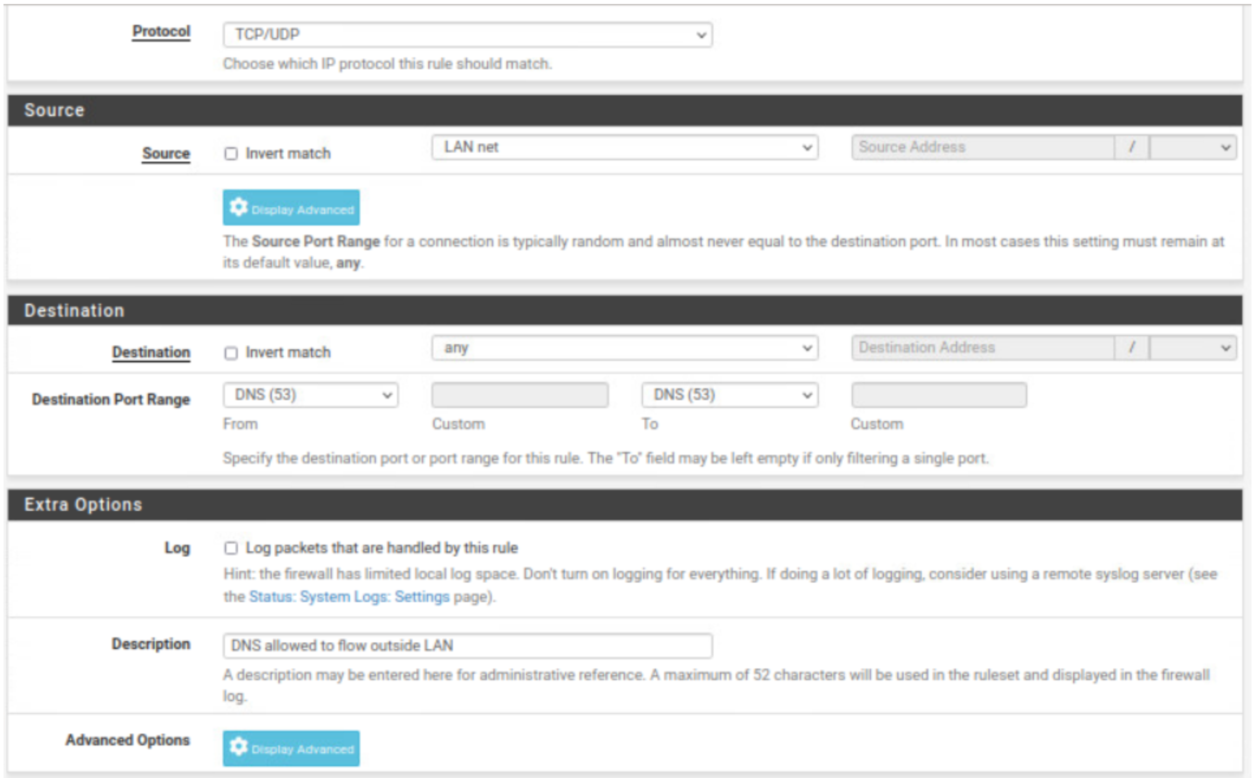
Allow approved protocols to flow to the outside of your LAN:

steps required to create one of the firewall rules:



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	TCP/UDP Choose which IP protocol this rule should match.



Protocol TCP/UDP

Choose which IP protocol this rule should match.

Source

Source □ Invert match LAN 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 DNS (53) From, Custom, DNS (53) 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

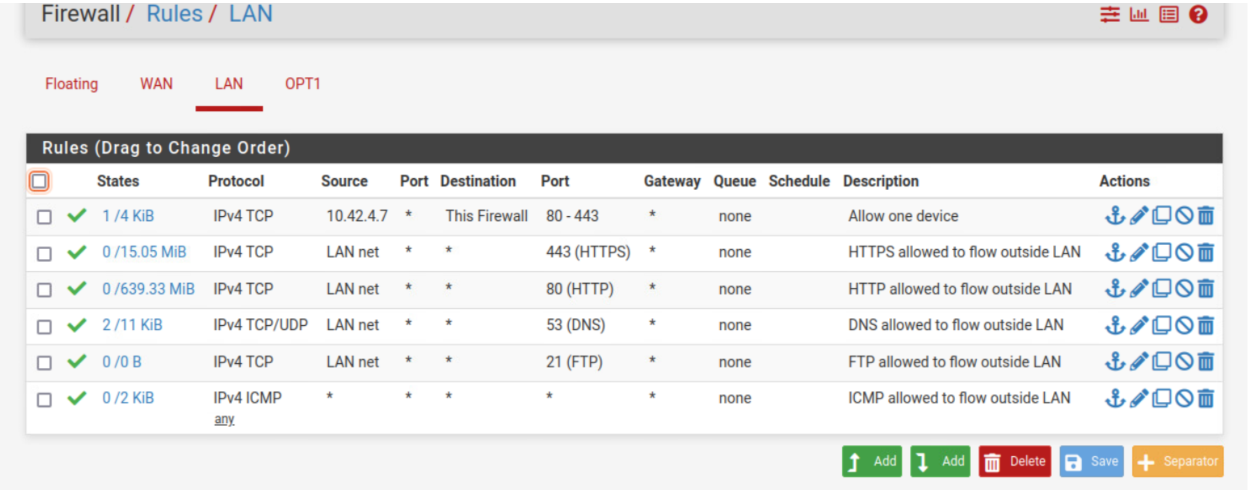
Log □ Log packets that are handled by this rule

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 DNS allowed to flow outside LAN

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



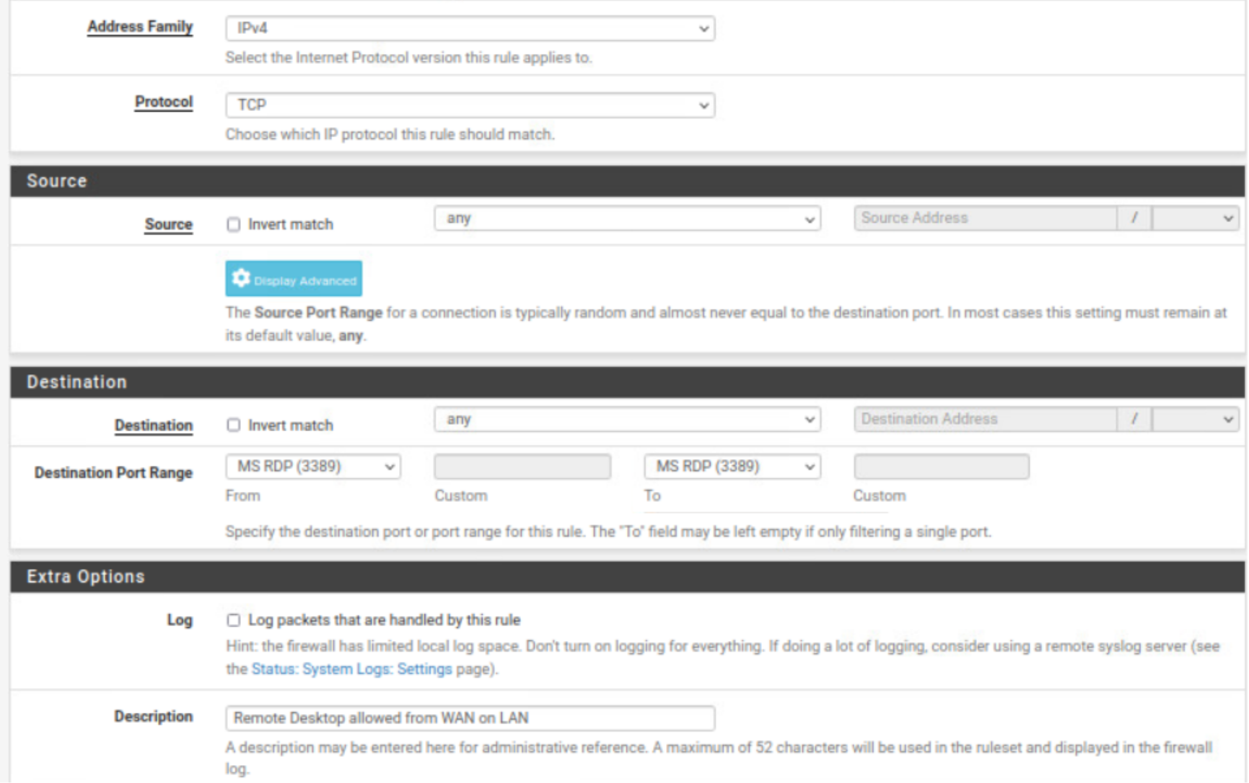
Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	1 /4 KiB	IPv4 TCP	10.42.4.7	*	This Firewall	80 - 443	*	none		Allow one device	
□	✓	0 /15.05 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		HTTPS allowed to flow outside LAN	
□	✓	0 /639.33 MiB	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none		HTTP allowed to flow outside LAN	
□	✓	2 /11 KiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		DNS allowed to flow outside LAN	
□	✓	0 /0 B	IPv4 TCP	LAN net	*	*	21 (FTP)	*	none		FTP allowed to flow outside LAN	
□	✓	0 /2 KiB	IPv4 ICMP any	*	*	*	*	*	none		ICMP allowed to flow outside LAN	

Allow approved protocols to flow to the inside of your LAN:

Steps required to create one of the firewall rules:



Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.

Source

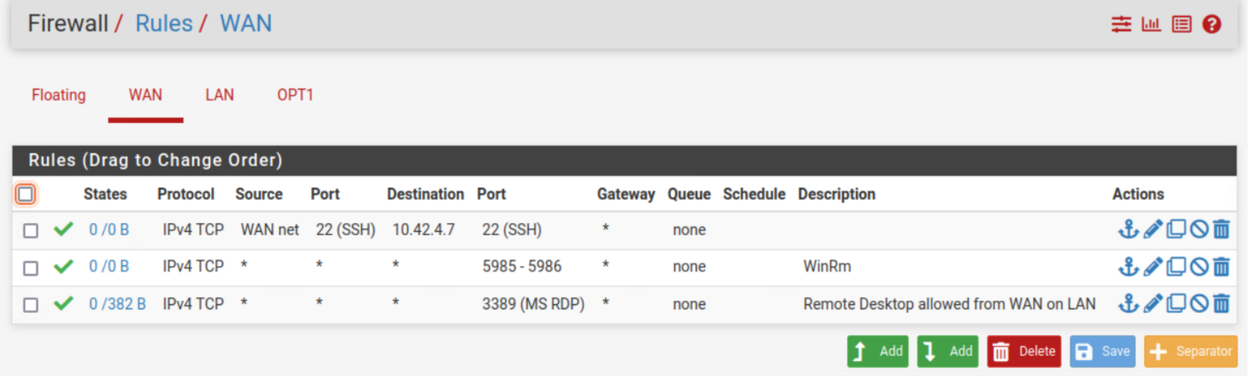
Source	□ Invert match · any · Source Address /
	Display Advanced The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination	□ Invert match · any · Destination Address /
Destination Port Range	MS RDP (3389) (From) · Custom · MS RDP (3389) (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	Remote Desktop allowed from WAN on LAN 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.



Firewall / Rules / WAN

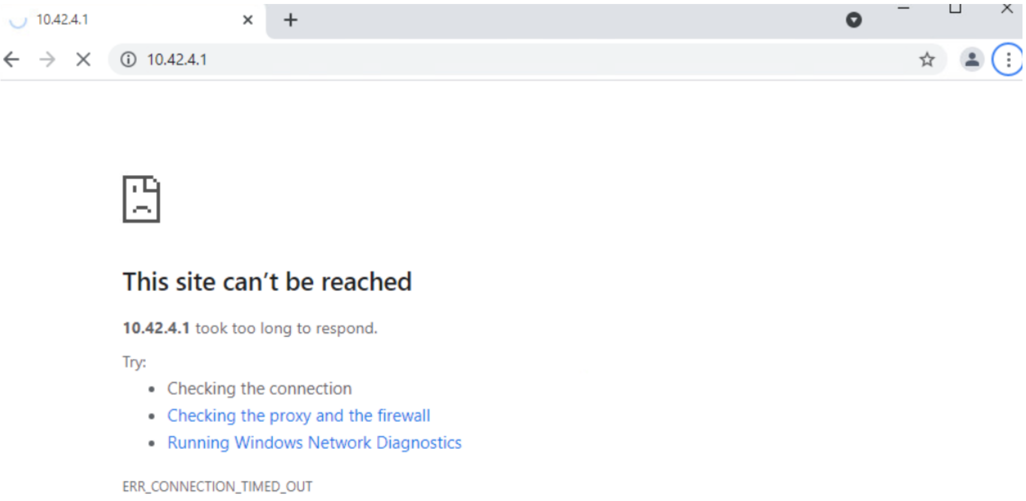
Floating | WAN | LAN | OPT1

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 TCP	WAN net	22 (SSH)	10.42.4.7	22 (SSH)	*	none			
□	✓	0 /0 B	IPv4 TCP	*	*	*	5985 - 5986	*	none		WinRm	
□	✓	0 /382 B	IPv4 TCP	*	*	*	3389 (MS RDP)	*	none		Remote Desktop allowed from WAN on LAN	

Testing:

Attempt to access the PFSense router from a device other than your device:



This site can’t be reached

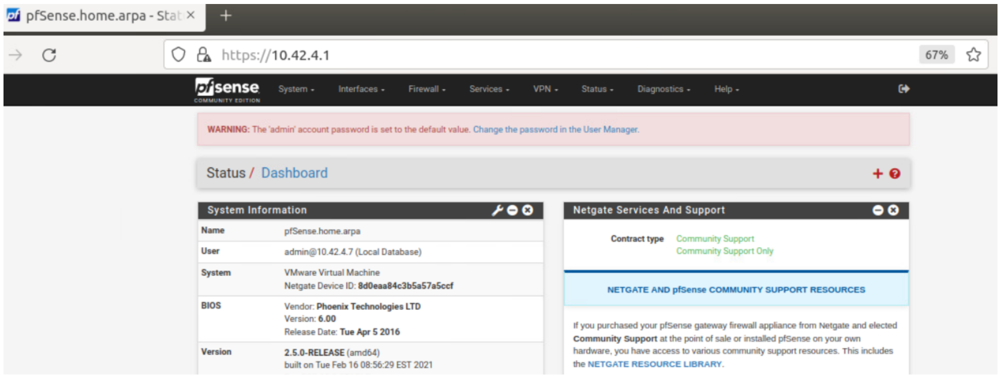
10.42.4.1 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Attempt to access the PFSense router from your designated device:



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@10.42.4.7 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **8d0eaa84c3b5a57a5ccf**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Tue Apr 5 2016**
Version	**2.5.0-RELEASE** (amd64) built on Tue Feb 16 08:56:29 EST 2021

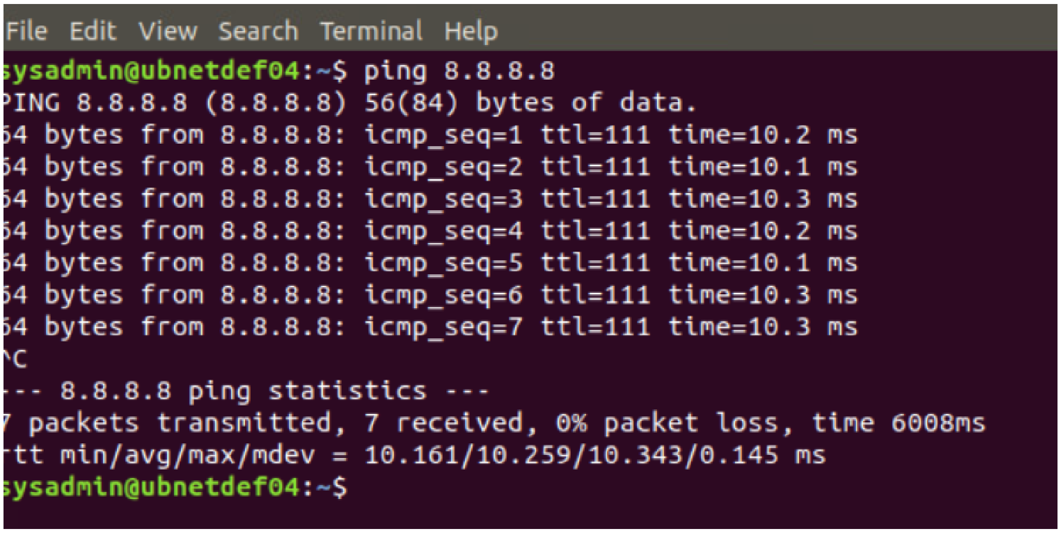
Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

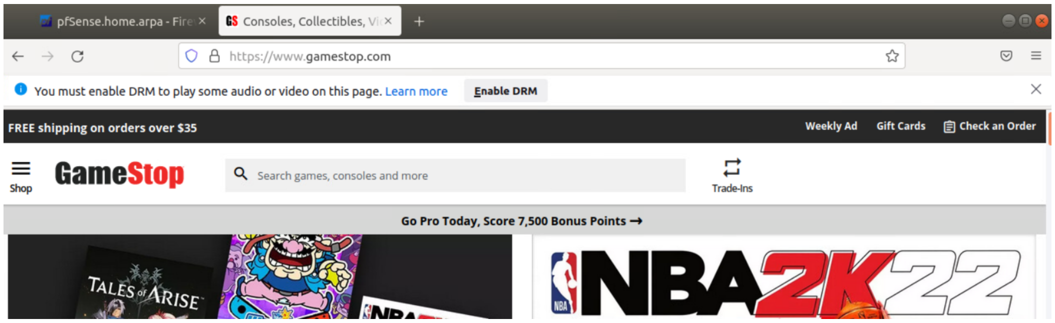
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

ICMP Testing: Ping 8.8.8.8:

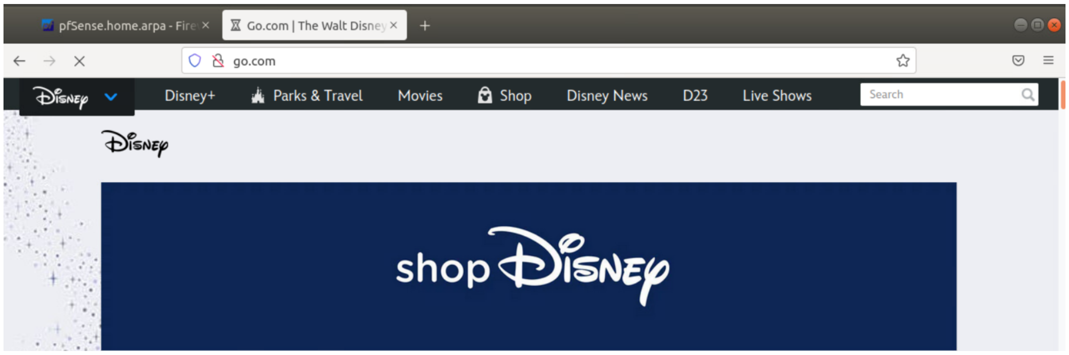


```
sysadmin@ubnetdef04:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=10.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=10.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=10.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=10.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=111 time=10.3 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 10.161/10.259/10.343/0.145 ms
sysadmin@ubnetdef04:~$
```

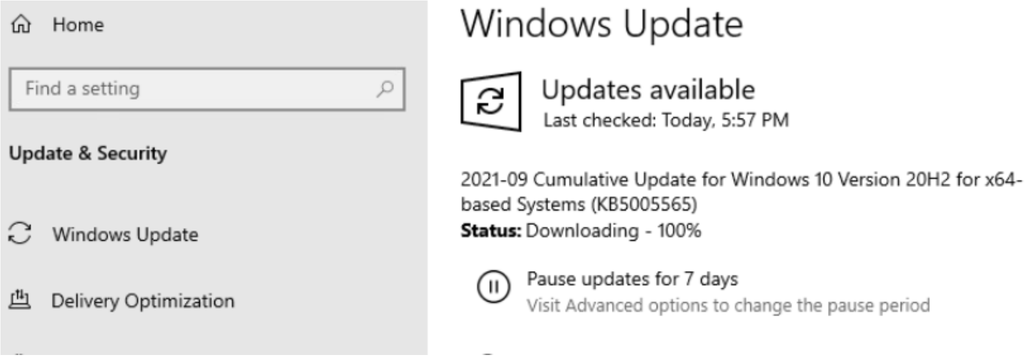
HTTPS Testing: Navigate to www.gamestop.com:


pfSense.home.arpa - Fire
Consoles, Collectibles, Vi
https://www.gamestop.com
You must enable DRM to play some audio or video on this page. Learn more
Enable DRM
FREE shipping on orders over $35
Weekly Ad
Gift Cards
Check an Order
Shop
GameStop
Search games, consoles and more
Trade-Ins
Go Pro Today, Score 7,500 Bonus Points →
TALES of ARISE
NBA 2K22

HTTP Testing: Navigate to www.go.com:



Windows Update:



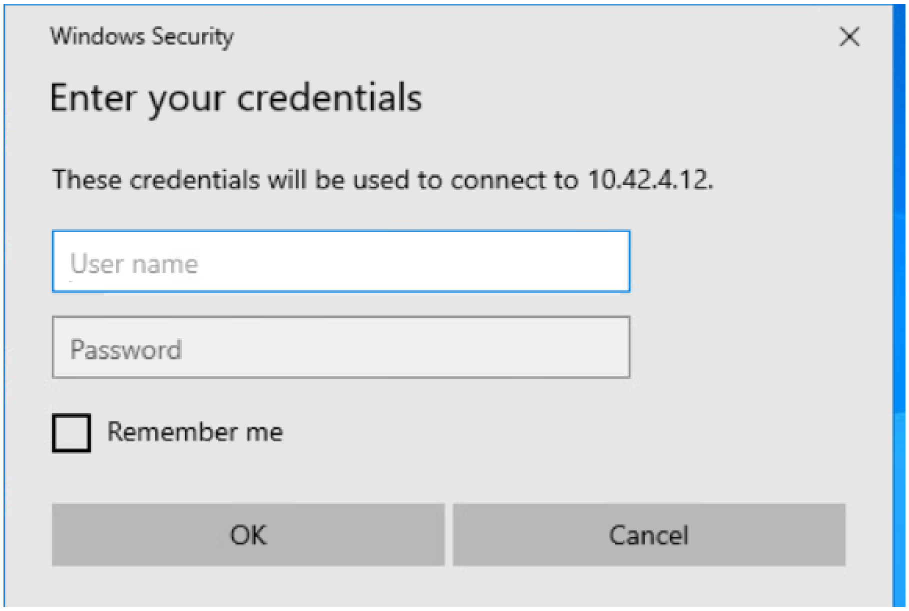
Windows Update

Updates available
Last checked: Today, 5:57 PM

2021-09 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5005565)
Status: Downloading - 100%

Pause updates for 7 days
Visit Advanced options to change the pause period

Open the Remote Desktop Connection tool in Windows:

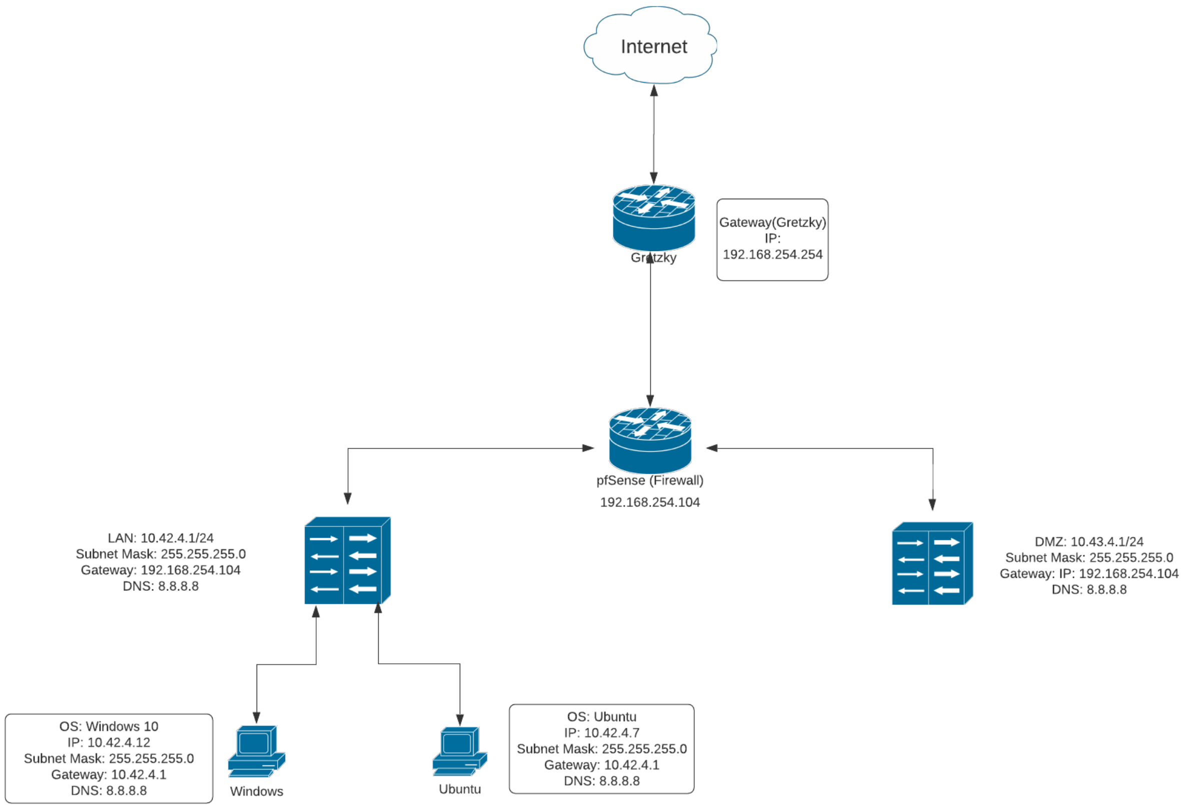


Windows Security

Enter your credentials

These credentials will be used to connect to 10.42.4.12.

Updated Topology:


Internet
Gateway(Gretzky)
IP:
192.168.254.254
Gretzky
pfSense (Firewall)
192.168.254.104
LAN: 10.42.4.1/24
Subnet Mask: 255.255.255.0
Gateway: 192.168.254.104
DNS: 8.8.8.8
DMZ: 10.43.4.1/24
Subnet Mask: 255.255.255.0
Gateway: IP: 192.168.254.104
DNS: 8.8.8.8
OS: Windows 10
IP: 10.42.4.12
Subnet Mask: 255.255.255.0
Gateway: 10.42.4.1
DNS: 8.8.8.8
Windows
Ubuntu
OS: Ubuntu
IP: 10.42.4.7
Subnet Mask: 255.255.255.0
Gateway: 10.42.4.1
DNS: 8.8.8.8