pfSense Firewall Firewall - Adding A Rule

In this lesson, we'll learn how to add a firewall rule.

First, we'll do a quick test to demonstrate that the traffic we want to block works with no rules in place.

Then, we'll create a rule to block. We'll see that the traffic is blocked and the offenders actions logged.

You don't have to follow along in the initial demonstration unless you just like doing that stuff and want to for fun.

In the VirtualBox lab, I have pfSense, the Ubuntu 18.04 Desktop behind pfSense, and an Ubuntu 18.04 server outside the firewall all running.

	Oracle VM VirtualBox Manager
New Settings Discard Show	
Ubuntu-Server Weight Off	Image: Properties Image: Properties Image: Properties
Ubuntu-Remote	Name
MSEdge - Win10 (Snapshot 2)	- Ourrent State
Ubuntu-18-04	
Ubuntu-18-04-Desktop → Running	
fSense → Running	

On the Ubuntu 18.04 server outside the firewall, I'll have netcat listen on port 1337.

```
nc -l 1337
```

On the Ubuntu Desktop behind the firewall, I'll telnet to the listening server.

```
telnet 192.168.254.143 1337
```

The connection goes live, and communication is possible.

The firewall took no action because the activity was permitted.

Now, we'll add a rule, and try again.

Log into the firewall, and go to Firewall, Rules in the menu.

Remembering that we want to place the rule as close to the threat as possible, we'll put our new rule on the LAN interface. The bad actor is supposedly on our LAN trying to get out.

Click on LAN.

We don't expect this rule to be hit very often, so well add it to the bottom of the list by choosing the Add with the down arrow.

For traffic inside the network, we'll choose Reject for the Action.

Edit Firewal	l Rule
Action	Reject
	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.
<u>Address</u> <u>Family</u>	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.

Specify port 1337 in the From field in the Destination Port Range, and leave the To field blank.

Destination					
Destination	 Invert match. 	any		•	Destination Address /
Destination Port Range	(other) ▼ From Specify the destin filtering a single p	1337 Custom nation port or port ra	(other) To ange for this rule	• The	Custom "To" field may be left empty if only

Check the box to Log packets that are handled by this rule.

Provide a descriptive name like Reject 1337 - shadyshell.

Extra Option	s
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	Reject 1337 - shadyshell 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	Cisplay Advanced
	🖺 Save

Save your rule.

□ 🕙 0/0 B	IPv4 TCP	*	*	*	1337	*	none	Reject 1337 - shadyshell	±∕ ⊡0 ∎
					bhA t	ļ	Add 🔟 Delete	🖺 Save 🕇 Sep	arator

You can see your new rule defined at the bottom of the list.

On the Firewall/Rules/LAN page, click Apply Changes.

Firewall / Rules / LAN	≢ Ш ≡ 0
The firewall rule configuration has been changed. The changes must be applied for them to take effect.	 Apply Changes
Floating WAN LAN	

Now, we'll test again by starting netcat and listening on port 1337 on our external server and telnetting to it from the internal Ubuntu Desktop.

It still works! What happened?

The problem is rule order.

We have a permit ANY IP, ANY PORT outbound enabled above our rule. First match wins!

les	(Drag to	o Chang	e Orde	r)							
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
~	1 /8.98 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti- Lockout Rule	0
~	6 /246.89 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	±.∕ ⊡0 ∎
~	0 /0 B	IPv6*	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	±ø ⊡⊘ ∎
0	0 /60 B	IPv4 TCP	*	*	*	1337	*	none		Reject 1337 - shadyshell	±≠ □0 ₪
	es ✓ ✓	es (Drag to States ✓ 1 /8.98 MiB ✓ 6 /246.89 MiB ✓ 0 /0 B 🗠 0 /60 B	Image: States Protocol States Protocol 1/8.98 * MiB * 6 IPv4 * /246.89 IPv4 * MiB IPv6 * 0/0 B IPv6 * 0/60 B IPv4 TCP IPv4	Image: States Protocol Source States Protocol Source 1/8.98 * * 1/8.98 * * MiB * * 6 IPv4 * LAN net MiB IPv6 * LAN net MiB IPv6 * LAN net ● 0/0 B IPv6 * LAN net	States Protocol Source Port States Protocol Source Port 1/8.98 * * * * 1/8.98 * * * * 6 IPv4 * LAN net * 0/0 B IPv6 * LAN net * © 0/60 B IPv4 * LAN net *	States Protocol Source Port Destination States Protocol Source Port Destination 1/8.98 * * * LAN Address 1/246.89 IPv4* LAN net * * 0/0 B IPv6* LAN net * * 0/0 B IPv6* LAN net * *	States Protocol Source Port Destination Port States Protocol Source Port Destination Port 1/8.98 * * * LAN Address 443 80 22 6 IPv4* LAN net * * * 0/0 B IPv6* LAN net * * * * 0/0 B IPv4 LAN net * * * * * 0/0 B IPv6 * LAN net * * * * * *	States Protocol Source Port Destination Port Gateway * 1/8.98 MiB * * * LAN Address 443 80 22 * * 6 /246.89 MiB IPv4* LAN net * * * * • 0/0 B IPv6* LAN net * * * * * • 0/60 B IPv4 LAN net * * * 1337 *	IProtocol Source Port Destination Port Gateway Queue States Protocol Source Port LAN Address 443 80 22 * * 1/8.98 MiB * * * LAN Address 443 80 22 * * 6 /246.89 MiB IPv4* LAN net * * * none • 0 /0 B IPv6* LAN net * * * none • 0 /60 B IPv4 LAN net * * none none	Image: States Protocol Source Port Destination Port Gateway Queue Schedule States Protocol Source Port Destination Port Gateway Queue Schedule * 1/8.98 * * * LAN 443 * * * MiB * * * LAN 443 * * * • 6/246.89 IPv4* LAN * * * none Image: Im	states Protocol Source Port Gateway Queue Schedule Description States Protocol Source Port LAN 443 * * Anti-Lockout Rule MiB * * * * LAN Address 80 22 * none Default allow LAN Rule * 6 //246.89 IPv4 * LAN net * * * * none Default allow LAN to any rule * 0 //0 B IPv6 * LAN net * * * * * none Default allow LAN to any rule * 0 //0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule * 0 //60 B IPv4 * * * 1337 * none Reject 1337- shadyshel

We have to move our rule up so it is hit before the permit ANY ANY rules.

Click to the box next to the green check mark on the two ANY ANY rules (IPv4 and IPv6) then press shift and click the up arrow next to the edit icon on the right.

	~	6 /246.89 MiB	IPv4*	LAN net	*	*	*	*	none	Default allow LAN to any rule	±∕ □0 ⊡
	~	0 /0 B	IPv6*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	±∕ ⊡0 ₪
	0	0 /60 B	IPv4 TCP	*	*	*	1337	*	none	Reject 1337 - shadyshell	±≠ ⊡0 ∎
							1 Add	l Add	🛍 Delete 🖺 S	ave 🕇 Sepa	arator

0	0	0 /60 B	IPv4 TCP	*	*	*	1337	*	none	Reject 1337 - shadyshell	±.∕ ⊡⊘ ∎
	~	6 /246.89 MiB	IPv4*	LAN net	*	*	*	*	none	Default allow LAN to any rule	±.∥ ⊡0 ⊡
	~	0 /0 B	IPv6*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	±.∥ ⊡0 ₪
							1 Add	Ĵ Add	🛅 Delete 💾 S	ave 🕂 Sepa	arator

Click Save at the bottom right of the list, then Apply Changes in green at the top.

Now, we see the traffic is blocked and logged.

If we saw a hit on this rule, we could go and investigate to see what happened to the infected host and clean it up.

Even if you don't want to try the full exercise, I encourage you to add the rule and move it up in the list. You could then try to telnet to any IP address off your network on port 1337 to see the rule enforced.

Nice work!

References pfSense book <u>https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-book.pdf</u>