

Use and Usefulness of Firewall Rules

Firewalls have more than just the purpose of keeping the bad guys out, they also keep legitimate users from deviating from their responsibilities. With the human layer being the weakest one, certain rules should be implemented to keep users from visiting risky sites/sites that have nothing to do with work or the use of that specific network. For instance, if you want clients outside your network to have access to your web server but deny access to other things such as file sharing and pinging; add rules to pfsense (your firewall) through the Graphic User Interface.

From the internal network (in our case from the Windows Web Server 2016), access your pfsense and log into the admin account via Chrome or some other browser. The goal is to use firewall rules in pfsense to limit access from the outside first, so we address the WAN (Wide Area Network) interface of the firewall rules. In the screenshot on the next page, I disabled a rule that allowed filesharing in the common file sharing ports in Windows (139 to 445) on the WAN interface of pfsense (the firewall). You can make a similar rule but make it a blocking rule and that will achieve the same result. Make sure it is at the top of the list of rules so that it is prioritized. The idea is to minimize privileges to the least amount needed to do the necessary tasks. This further secures the network. Go to Firewalls>Rules>Add rule. The protocol is TCP and applies to “any” client outside the private network, so that is the selection you make. Make sure to click “apply changes” after making each rule.



https://192.168.101.1/firewall_rules.php?f=wan

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

Firewall / Rules / WAN ☰ ☰ ☰ ?

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

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✔ 0 / 15 KIB	IPv4 TCP	*	*	192.168.101.2	139 - 445	*	none			
<input type="checkbox"/>	✔ 0 / 0 B	IPv4 TCP	*	*	192.168.101.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✔ 0 / 0 B	IPv4 TCP	*	*	192.168.101.1	443 (HTTPS)	*	none			

↑ Add ↓ Add 🗑 Delete 💾 Save ⊕ Separator



Windows Server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

https://192.168.101.1/firewall_rules_edit.php?id=2

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

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 Single host or alias 192.168.101.1 /

Destination Port Range HTTPS (443) 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 [Display Advanced](#)

Information

Tracking ID 1636492030

Server Manager

Activate Windows
Go to Settings to activate Windows.

Right Ctrl

Above we address what clients can have access to. We allow them to access the webserver through port 443 (a common HTTPS port) and we do the same with port 80 (for HTTP). The source will be “any” (as in any client) etc. Another good rule-of-thumb is to disable anything allowing ping through the firewall. This helps stop unwanted traffic bogging down your network. The protocol to make a rule for blocking this is ICMP. I had a passing rule, so I simply disabled it, and ping was unsuccessful afterwards. This is shown on the next page in two screenshots.

Windows Server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ipsec/192.168.101.1/firewall_rules.php?if=wan

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Firewall / Rules / WAN

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

Floating **WAN** LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 2 / 840 B	IPv4 ICMP	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.101.2	139 - 445	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.101.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.101.1	443 (HTTPS)	*	none			

↑ Add ↓ Add Delete Save Separator

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

Activate Windows
Go to Settings to activate Windows.

```
Command Prompt - ping 192.168.101.1

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\jlane003>girlsgeekout.org nslookup
'girlsgeekout.org' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\jlane003>nslookup girlsgeekout.org
Server: UnKnown
Address: 10.1.1.1

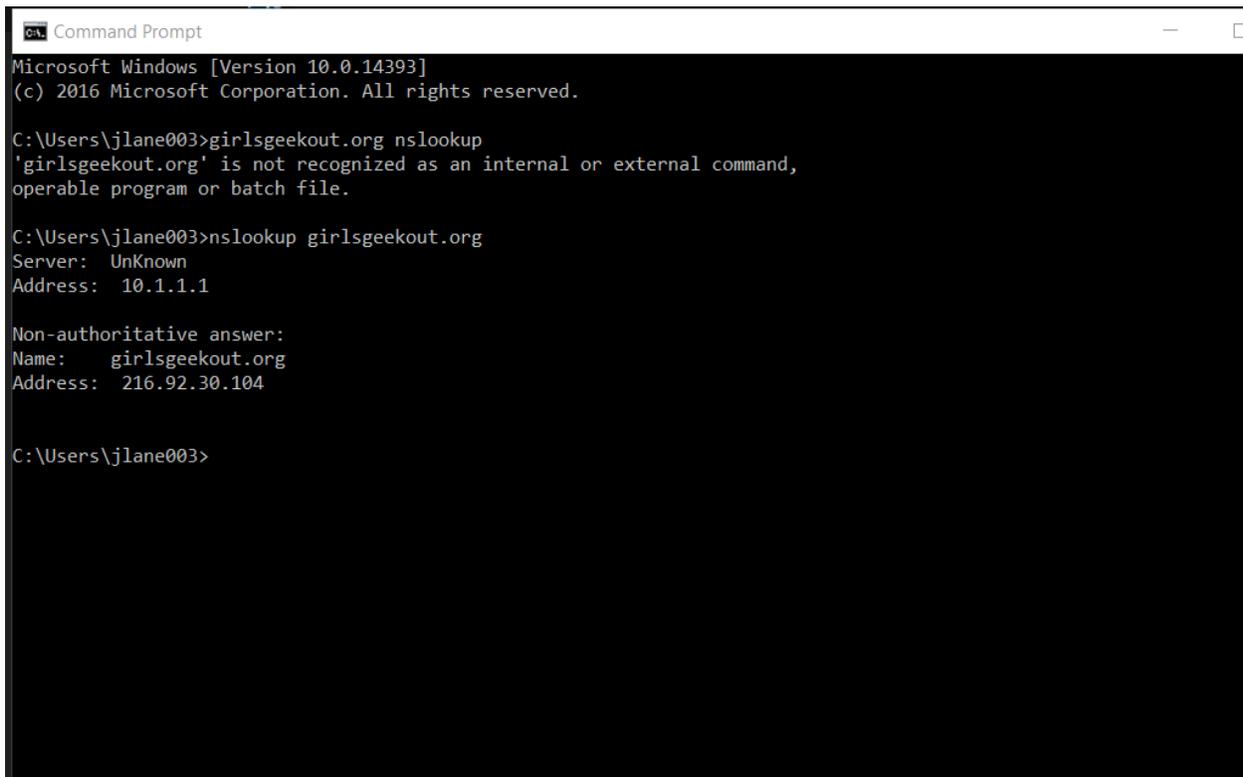
Non-authoritative answer:
Name:    girlsgeekout.org
Address: 216.92.30.104

C:\Users\jlane003>192.168.101.1
'192.168.101.1' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\jlane003>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Next, you want to take care of your clients in your private network. You can blacklist (prohibit access to) certain sites, but professionals recommend whitelisting (allowing access to) to save time and effort. There will always be new sites for clients to abuse, access, etc. For this reason, it takes fewer rules to allow access to the necessary websites. For the following example, however, I will simply show how to prohibit access to certain sites/create a loopback feature that keeps clients from misusing the network. Say, for instance, I wanted to block access to `girlsgeekout.org`. First, I want to find the IP address of the website, I do this by using “`nslookup girlsgeekout.org`” in a command prompt window as shown below.



```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

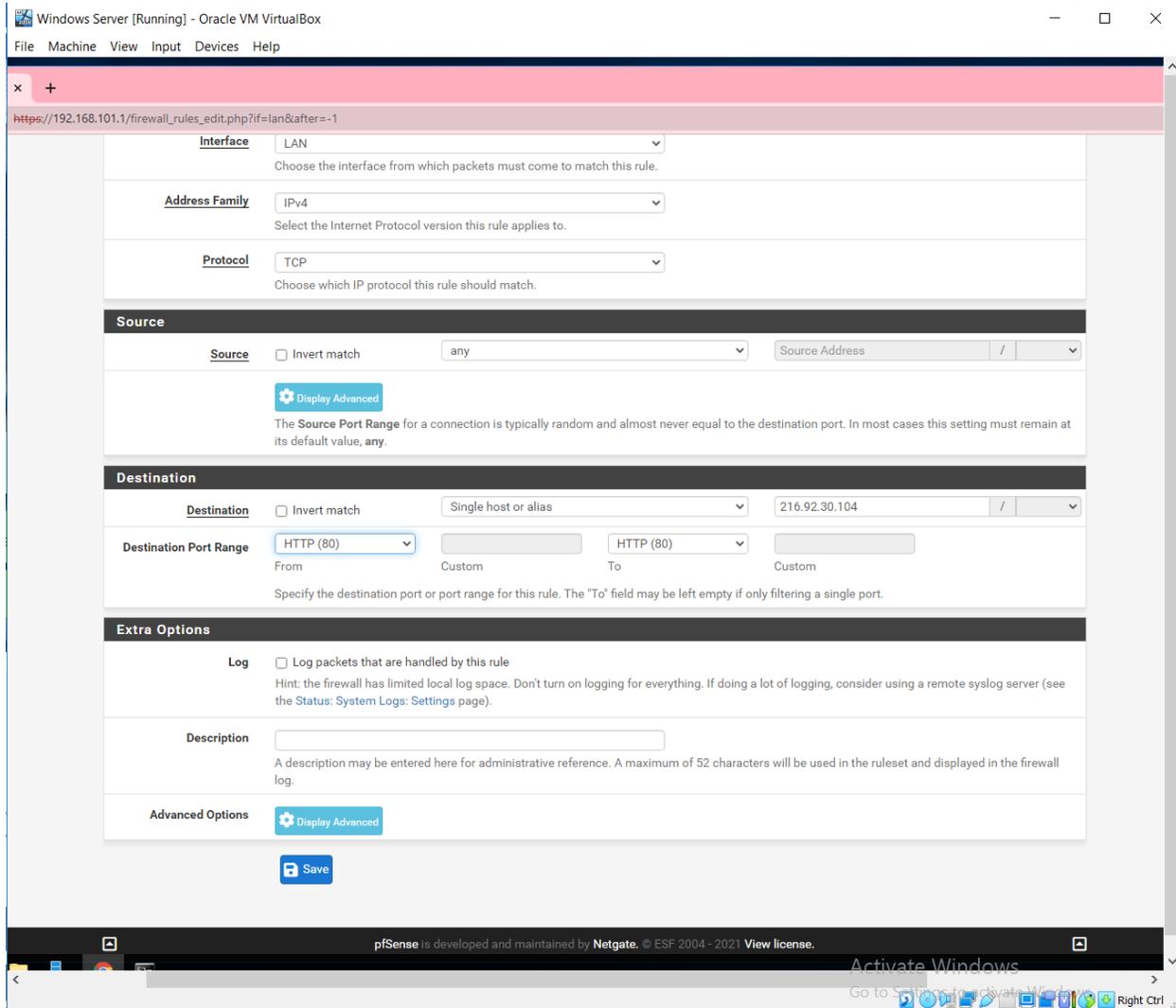
C:\Users\jlane003>girlsgeekout.org nslookup
'girlsgeekout.org' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\jlane003>nslookup girlsgeekout.org
Server: UnKnown
Address: 10.1.1.1

Non-authoritative answer:
Name:    girlsgeekout.org
Address: 216.92.30.104

C:\Users\jlane003>
```

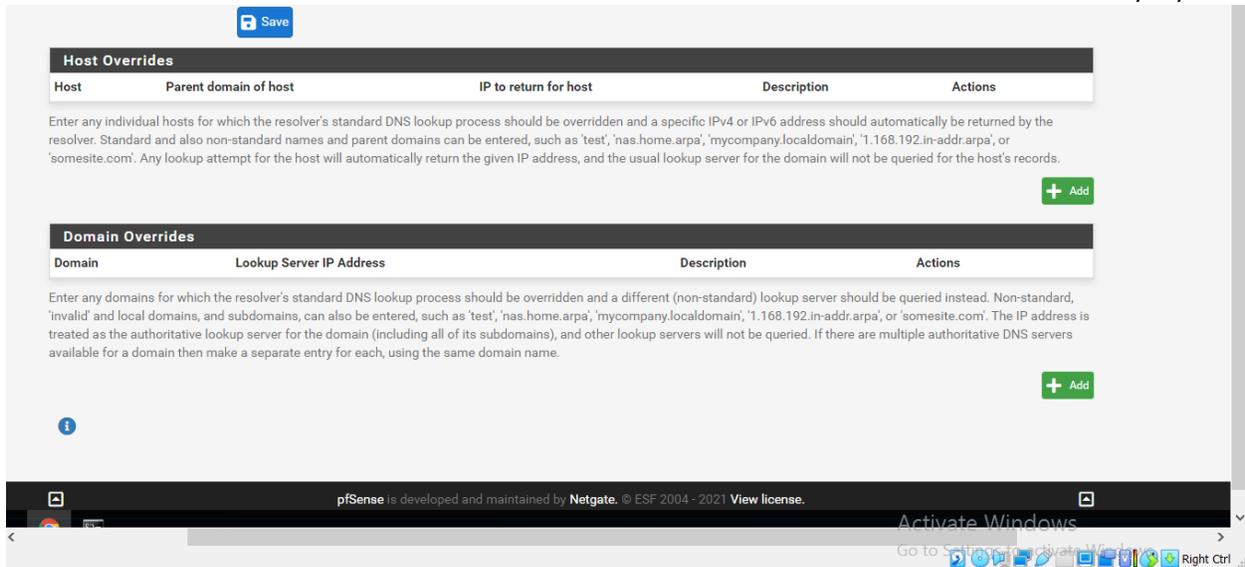
Now we go to the LAN interface of pfSense, and we add a rule blocking that specific IP address (216.92.30.104) as a destination. The source is set to “any”, and the port is set to 80 since the website is HTTP. This rule is shown on the next page.



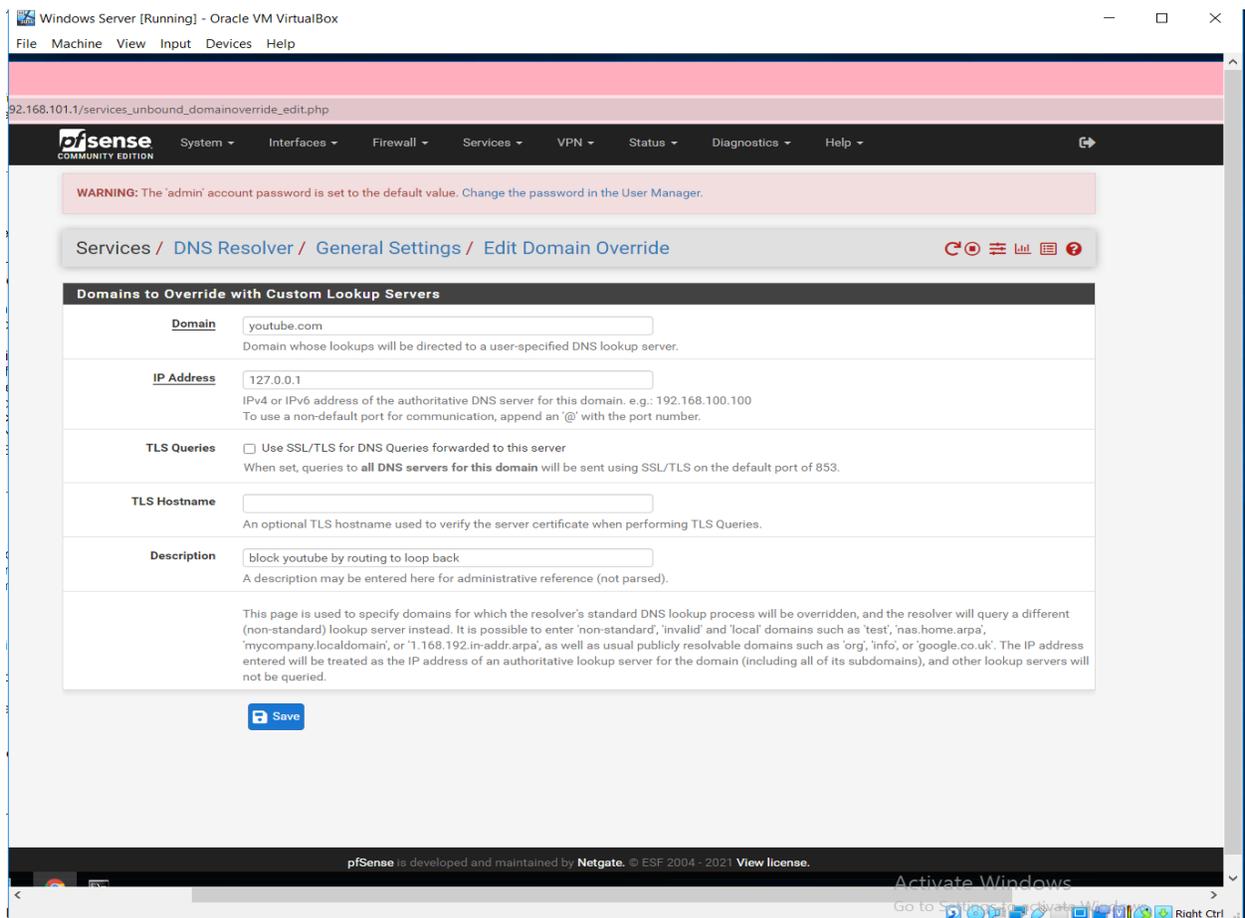
Hit save and apply changes (same as the rest of the rules).

Next, we look at blocking access to a popular site such as youtube.com. Here we want to use the domain override feature to simply show a "This site can't be reached" message to the client.

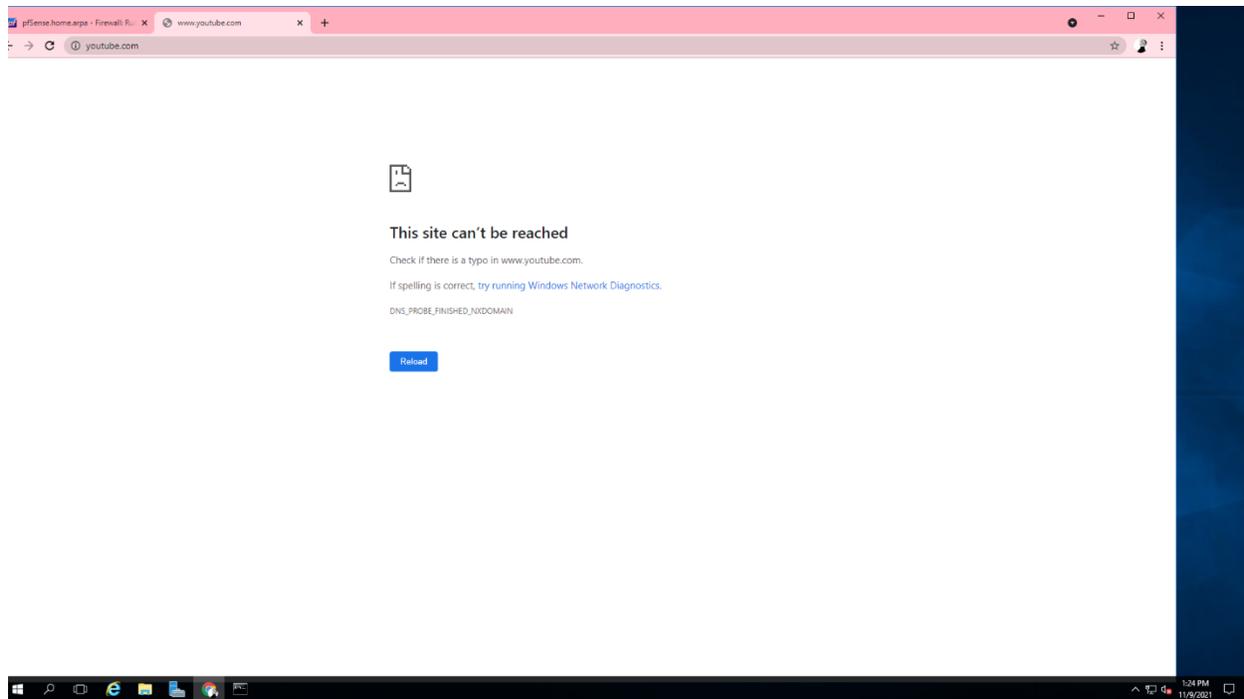
First, you select "Services" from the pfsense GUI, then select DNS Resolver>General Settings>add domain override. The screenshot on the next page shows the domain override location.



Next, set the domain entry to youtube.com, the IP address to 127.0.0.1, hit save and apply changes. This is shown below.



Once this is implemented, you can test it by trying to access youtube.com from inside the network. This is shown below.



In these ways, you can block access to risky sites or sites you simply do not want your clients accessing. This provides a more productive and safe work environment.