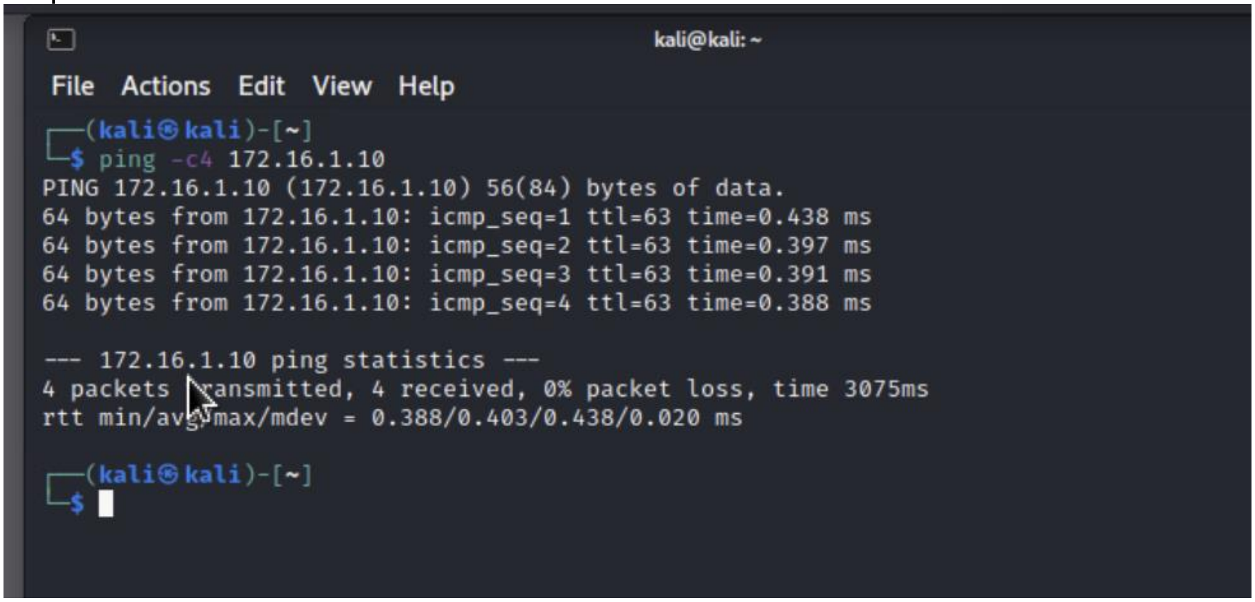
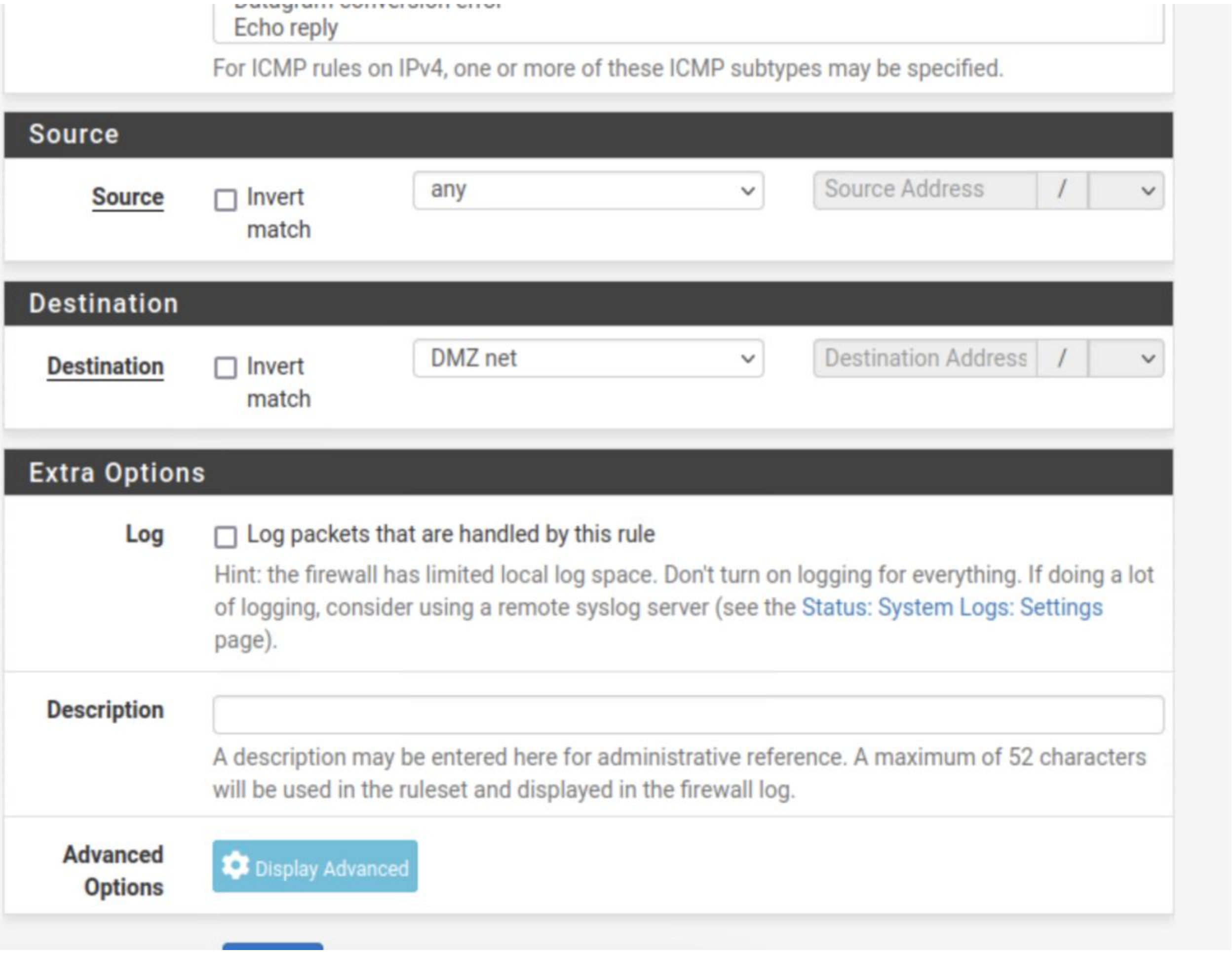
Peter Sanford
IT 2700
NetLab Lab 17
11/04/2023

1.1:
Step 8:



```
┌──(kali㉿kali)-[~]
└─$ ping -c4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=63 time=0.438 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=63 time=0.397 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=63 time=0.391 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=63 time=0.388 ms

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.388/0.403/0.438/0.020 ms

┌──(kali㉿kali)-[~]
└─$ 
```

Step 14:



Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source	□ Invert match	any	Source Address /

Destination

Destination	□ Invert match	DMZ net	Destination Address /

Extra Options

Log: □ Log packets that are handled by this rule

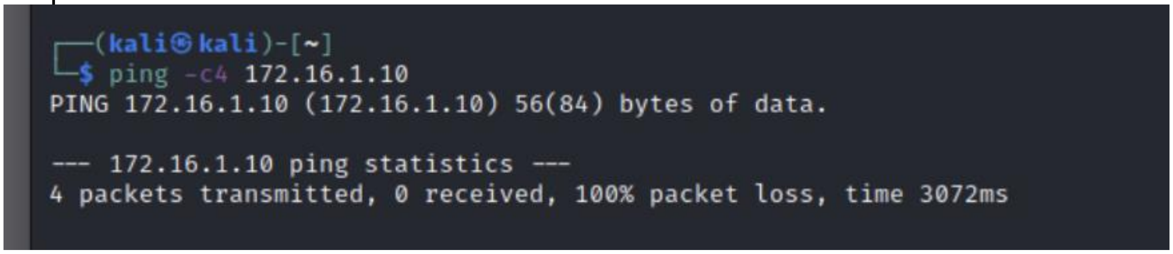
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description:

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.

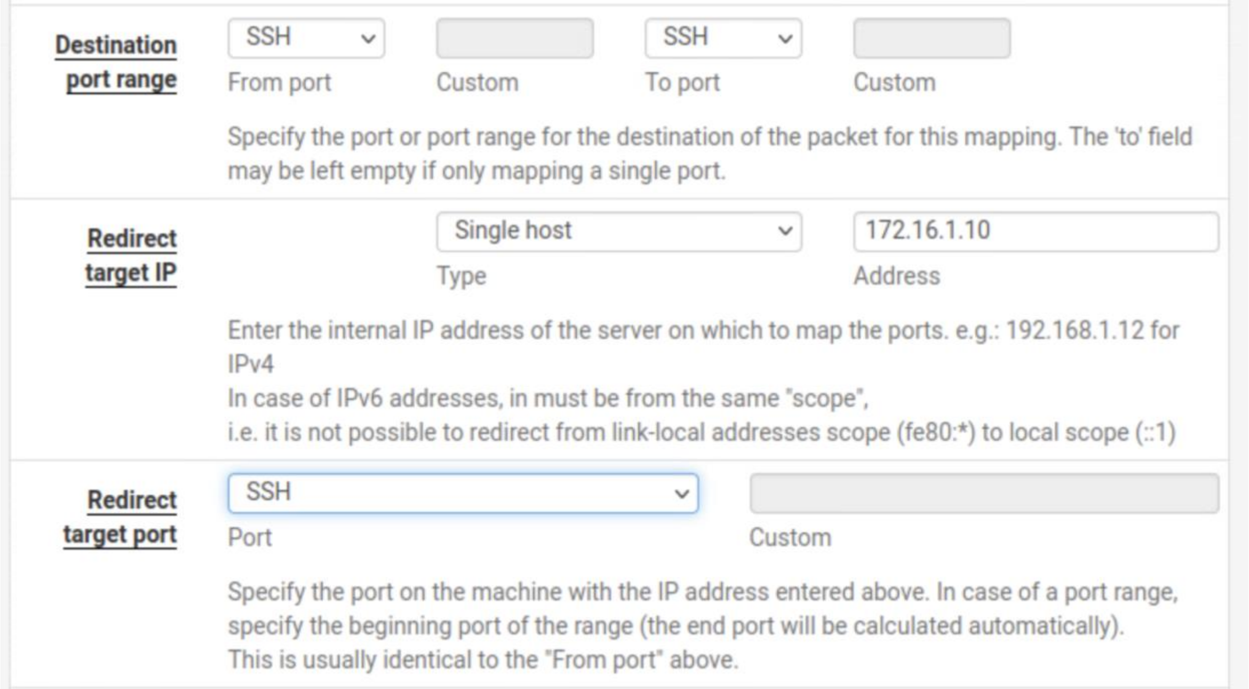
Advanced Options:

Step 20:



```
┌──(kali㉿kali)-[~]
└─$ ping -c4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3072ms
```

2.1:
Step 4c:



Destination port range

SSH — From port

Custom

SSH — To port

Custom

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 target IP

Single host — Type

172.16.1.10 — Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

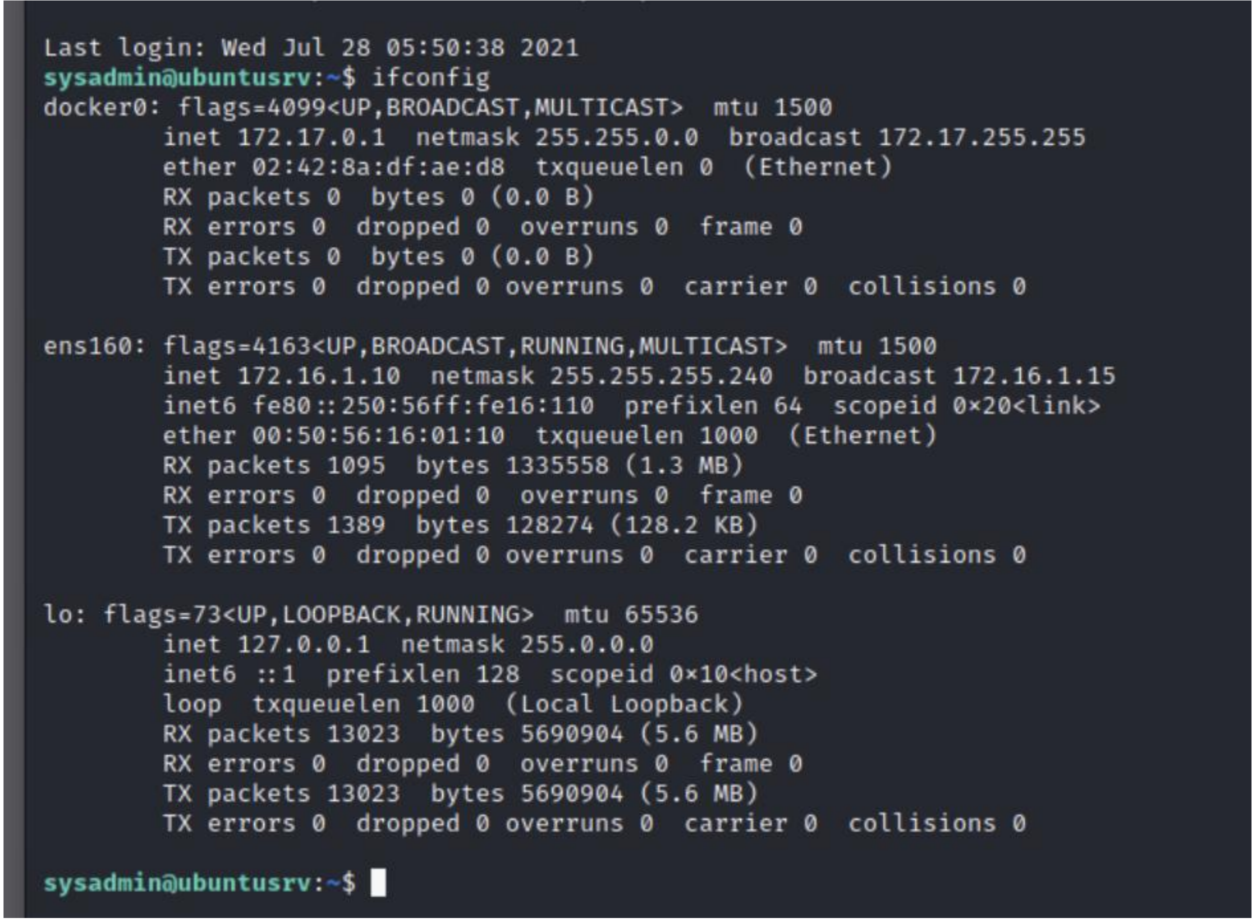
Redirect target port

SSH — Port

Custom

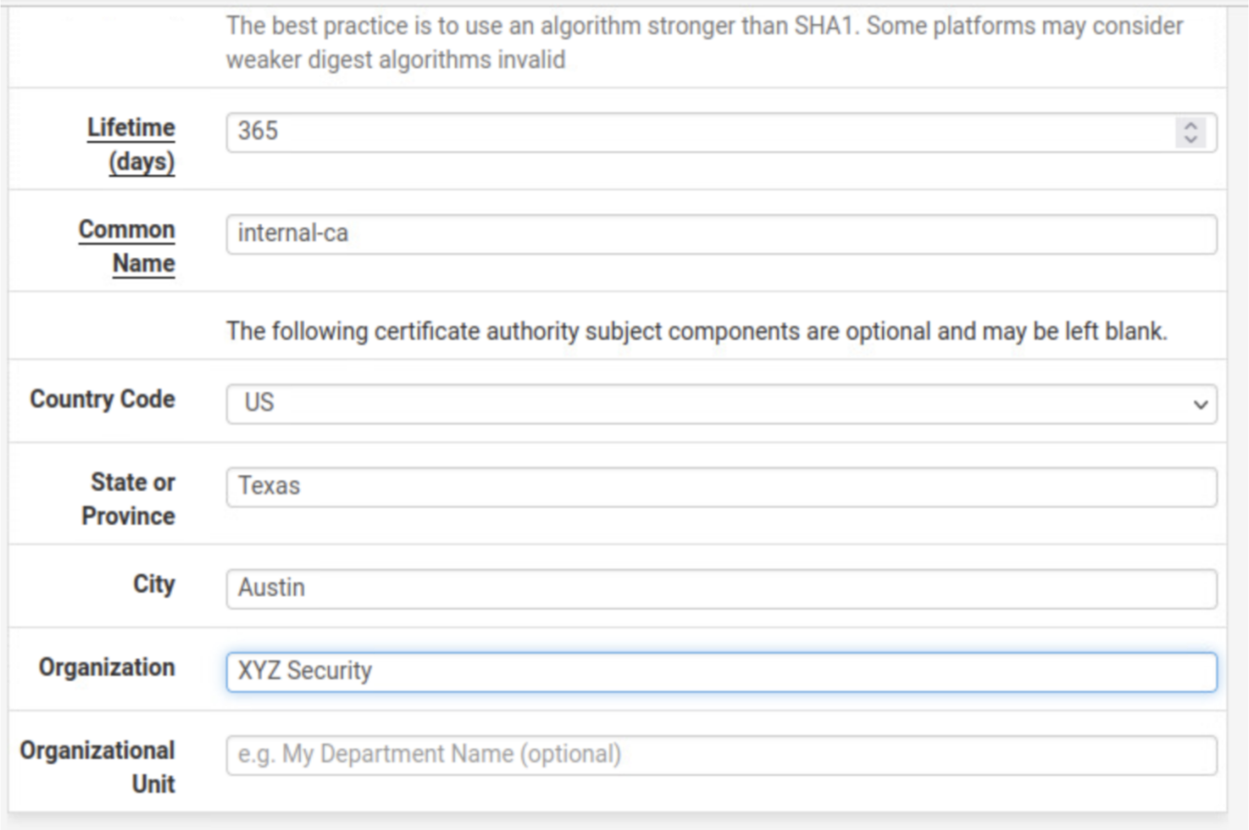
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

2.2:
Step 3:



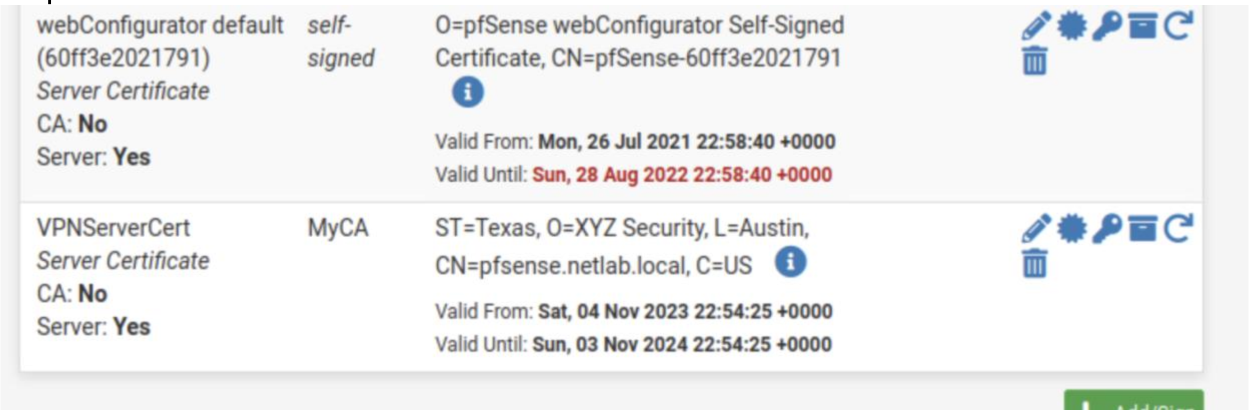
```
Last login: Wed Jul 28 05:50:38 2021
sysadmin@ubuntusrv:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:8a:df:ae:d8  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.10  netmask 255.255.255.240  broadcast 172.16.1.15
        inet6 fe80::250:56ff:fe16:110  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:16:01:10  txqueuelen 1000  (Ethernet)
        RX packets 1095  bytes 1335558 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1389  bytes 128274 (128.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13023  bytes 5690904 (5.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13023  bytes 5690904 (5.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sysadmin@ubuntusrv:~$ 
```

3.1:
Step 4e:



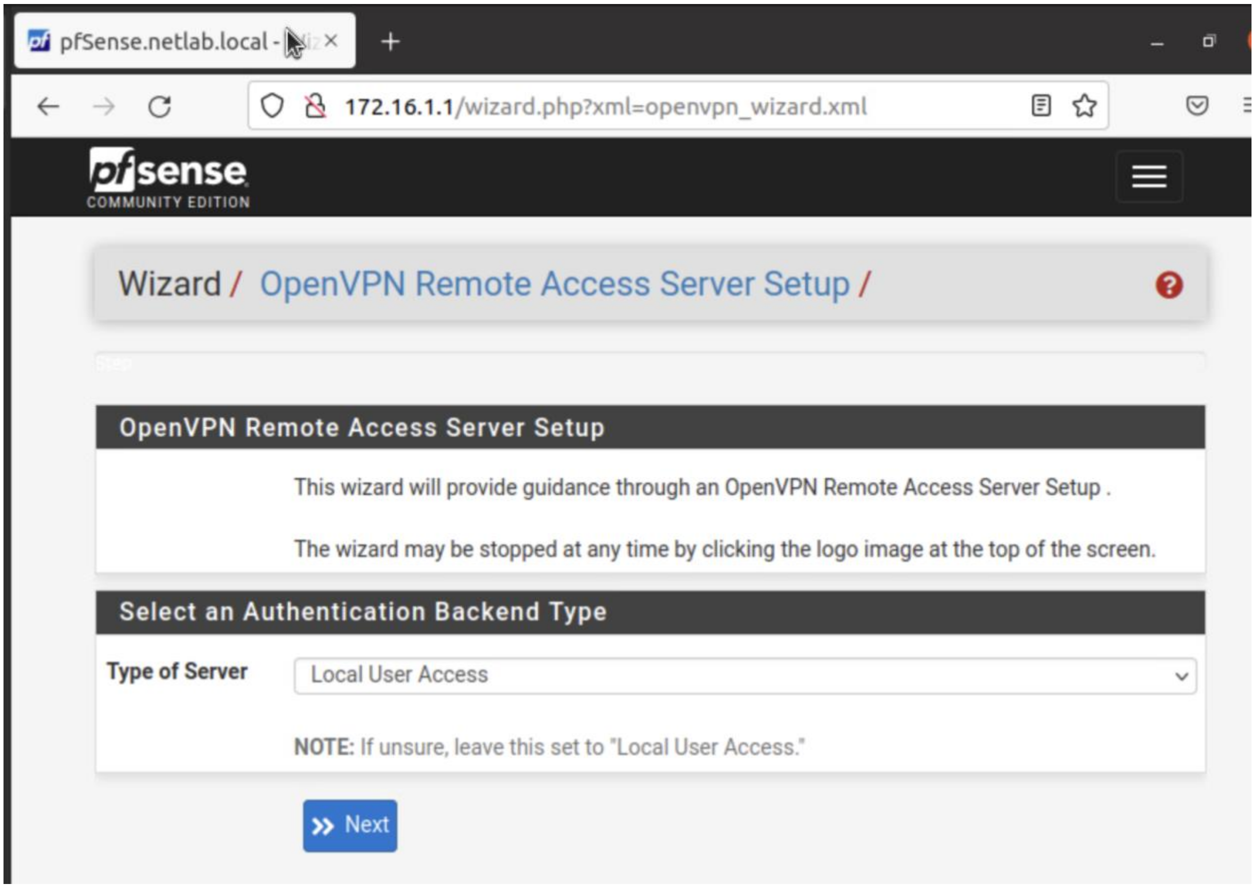
	The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)	365
Common Name	internal-ca
	The following certificate authority subject components are optional and may be left blank.
Country Code	US
State or Province	Texas
City	Austin
Organization	XYZ Security
Organizational Unit	e.g. My Department Name (optional)

Step 7f:



webConfigurator default (60ff3e2021791) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-60ff3e2021791 Valid From: **Mon, 26 Jul 2021 22:58:40 +0000** Valid Until: **Sun, 28 Aug 2022 22:58:40 +0000**	
VPNServerCert *Server Certificate* CA: **No** Server: **Yes**	MyCA	ST=Texas, O=XYZ Security, L=Austin, CN=pfsense.netlab.local, C=US Valid From: **Sat, 04 Nov 2023 22:54:25 +0000** Valid Until: **Sun, 03 Nov 2024 22:54:25 +0000**	

Step 12:


pfSense.netlab.local - Wiz
172.16.1.1/wizard.php?xml=openvpn_wizard.xml
pfsense COMMUNITY EDITION
Next

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

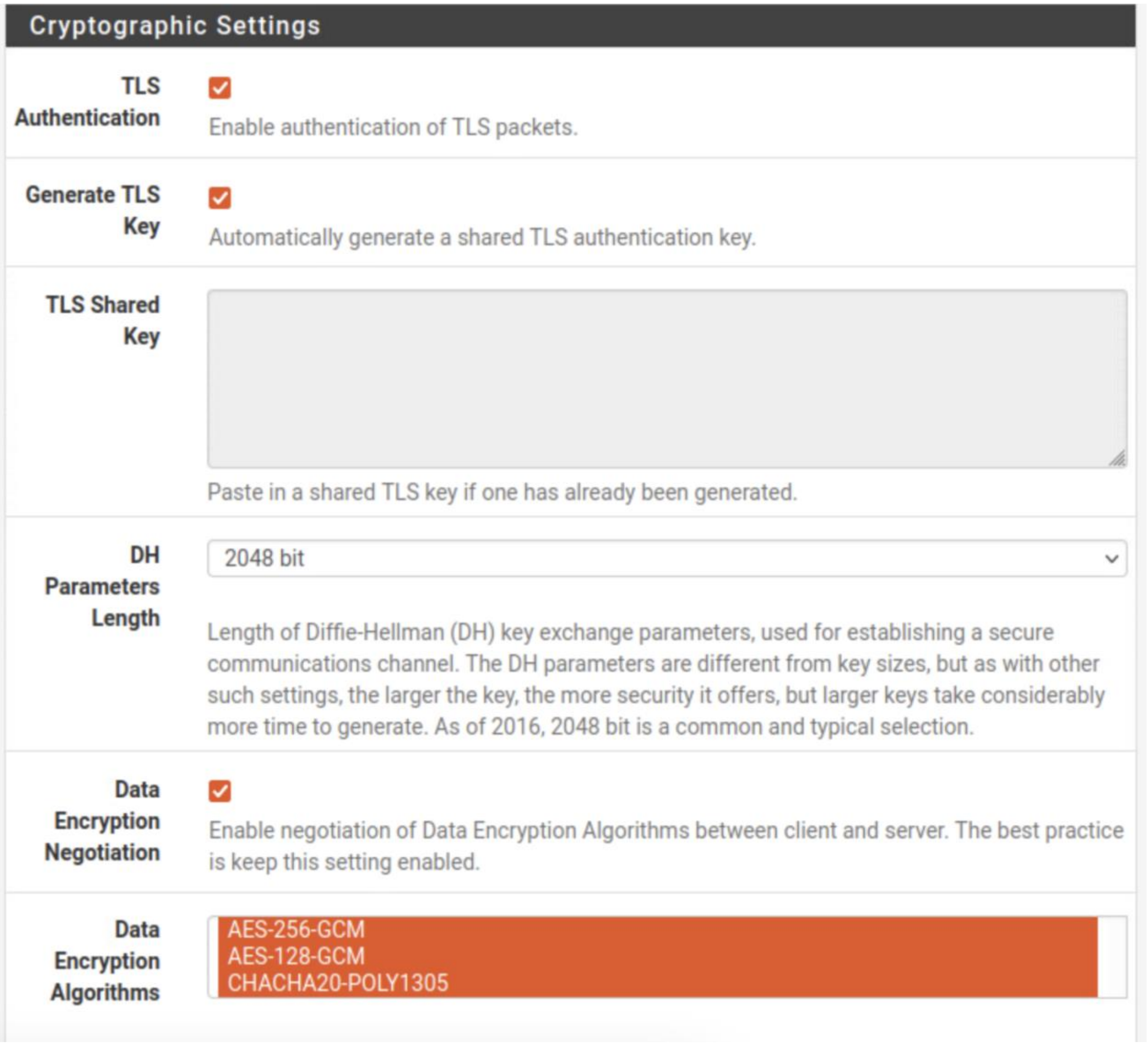
The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server: Local User Access

NOTE: If unsure, leave this set to "Local User Access."

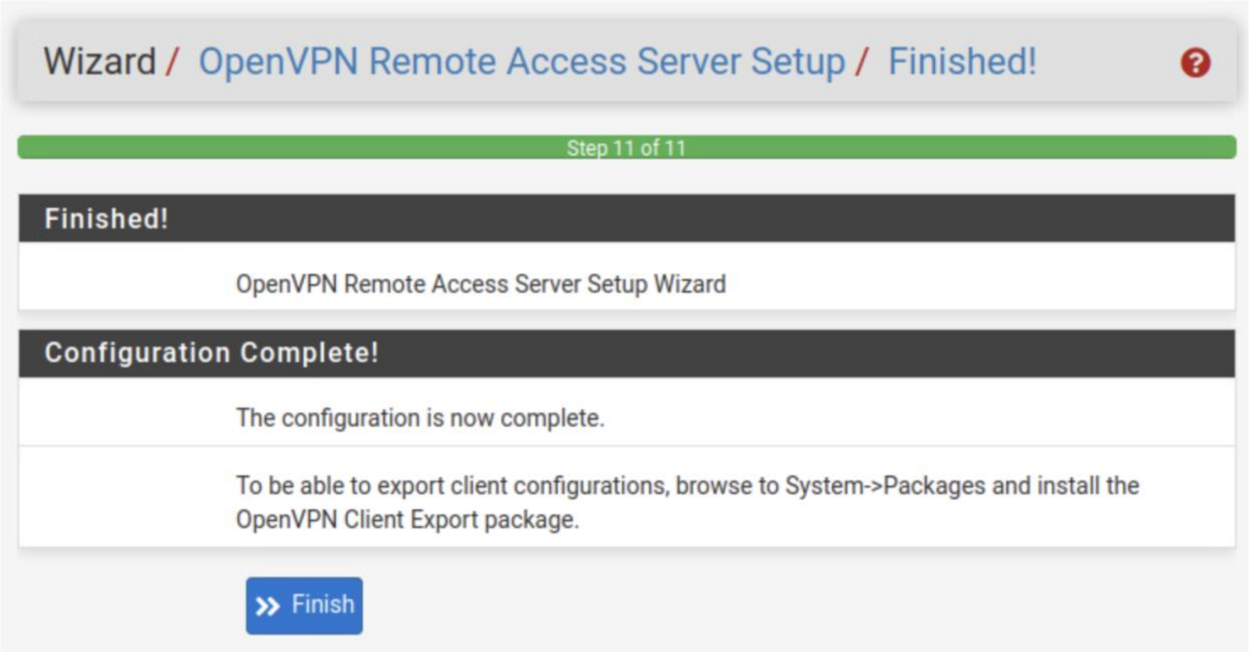
Step 16e:



Cryptographic Settings

TLS Authentication	☑ Enable authentication of TLS packets.
Generate TLS Key	☑ Automatically generate a shared TLS authentication key.
TLS Shared Key	Paste in a shared TLS key if one has already been generated.
DH Parameters Length	2048 bit Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation	☑ Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	AES-256-GCM AES-128-GCM CHACHA20-POLY1305

Step 17:



Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

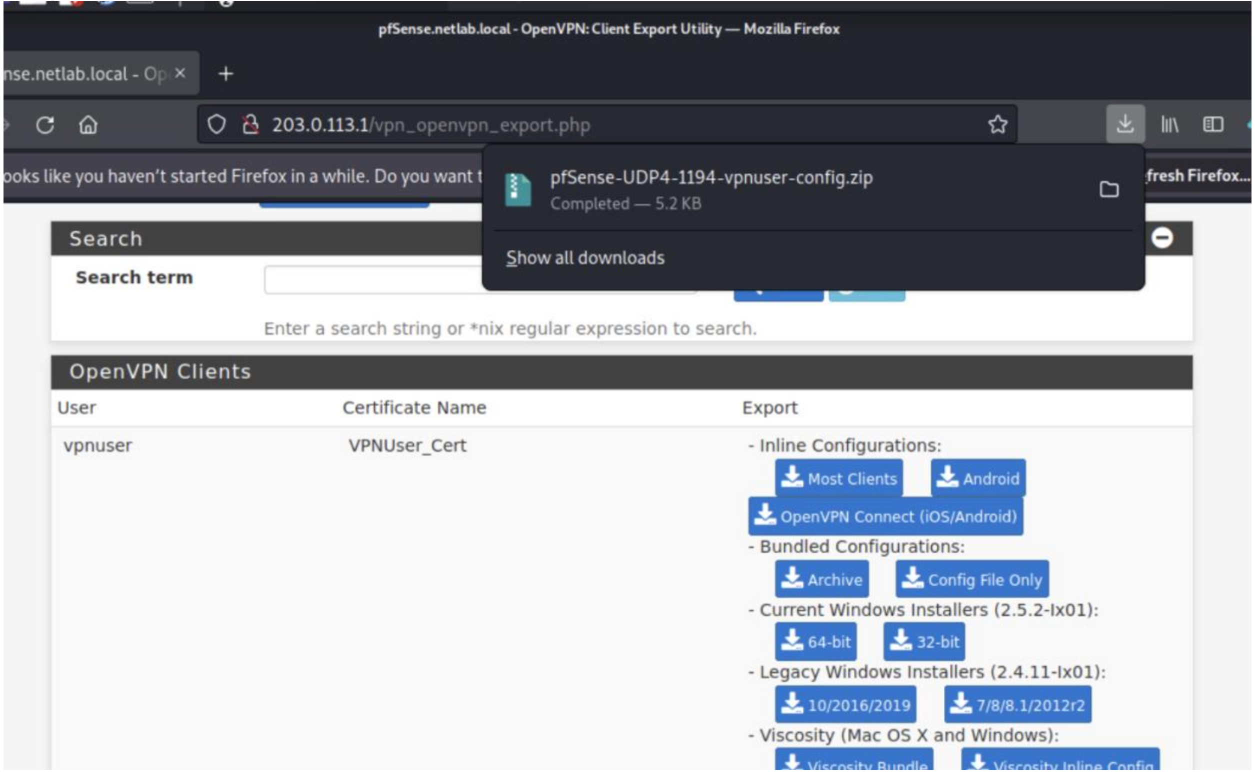
Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

3.2:

Step 5:



pfSense.netlab.local - OpenVPN: Client Export Utility — Mozilla Firefox

ooks like you haven't started Firefox in a while. Do you want t

fresh Firefox...

pfSense-UDP4-1194-vpnuser-config.zip
Completed — 5.2 KB

Search

Search term

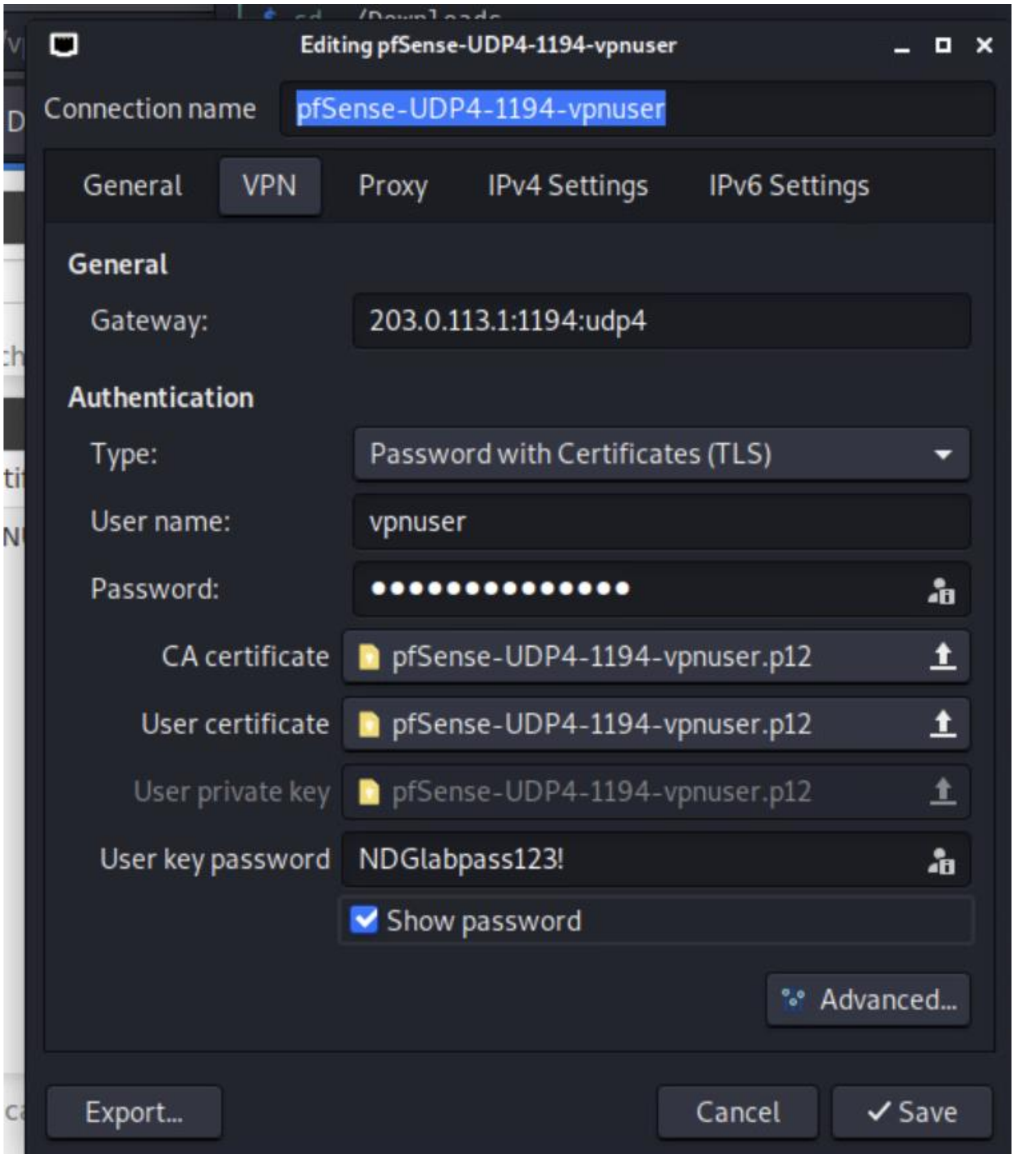
Enter a search string or *nix regular expression to search.

OpenVPN Clients

User	Certificate Name	Export
vpnuser	VPNUser_Cert	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.5.2-Ix01): 64-bit 32-bit - Legacy Windows Installers (2.4.11-Ix01): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

3.3:

Step 6:



Editing pfSense-UDP4-1194-vpnuser

Connection name: pfSense-UDP4-1194-vpnuser

General

Gateway: 203.0.113.1:1194:udp4

Authentication

Type: Password with Certificates (TLS)

User name: vpnuser

Password: ••••••••••••••

CA certificate: pfSense-UDP4-1194-vpnuser.p12

User certificate: pfSense-UDP4-1194-vpnuser.p12

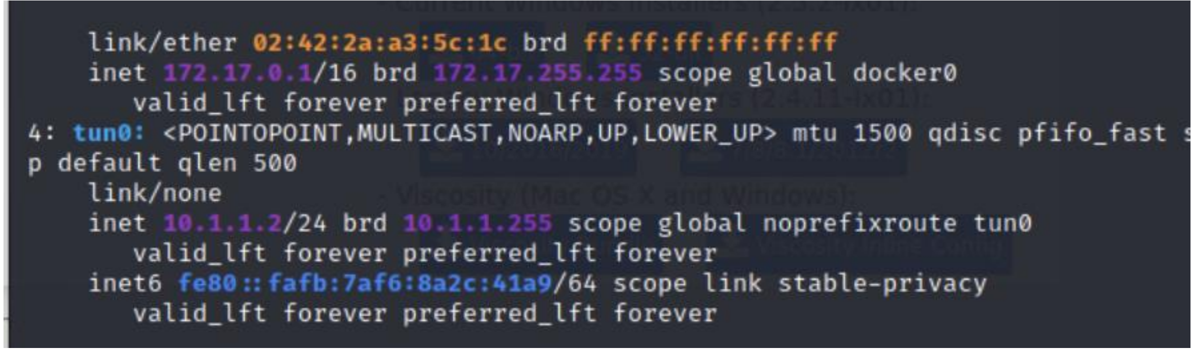
User private key: pfSense-UDP4-1194-vpnuser.p12

User key password: NDGlabpass123!

☑ Show password

3.4:

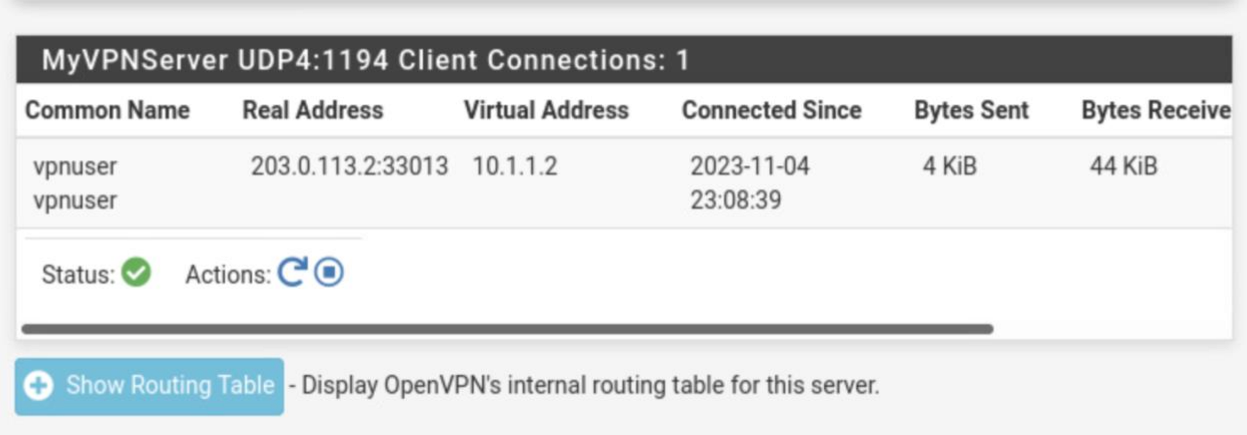
Step 3:



```
    link/ether 02:42:2a:a3:5c:1c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast s
p default qlen 500
    link/none
    inet 10.1.1.2/24 brd 10.1.1.255 scope global noprefixroute tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::fafb:7af6:8a2c:41a9/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

3.5:

Step 6:



MyVPNServer UDP4:1194 Client Connections: 1

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Receive
vpnuser vpnuser	203.0.113.2:33013	10.1.1.2	2023-11-04 23:08:39	4 KiB	44 KiB

Status: ✓ Actions:

- Display OpenVPN's internal routing table for this server.

Commentary:

In this lab we explored firewall rules and VPN’s. I learned that firewall rules are simple yet control your network and what people and do into and out of your network. Knowing this information, companies can configure their networks to behave the way they want them and increase security. They can also setup VPN’s for their employees to have encrypted traffic over the internet through a tunnel.