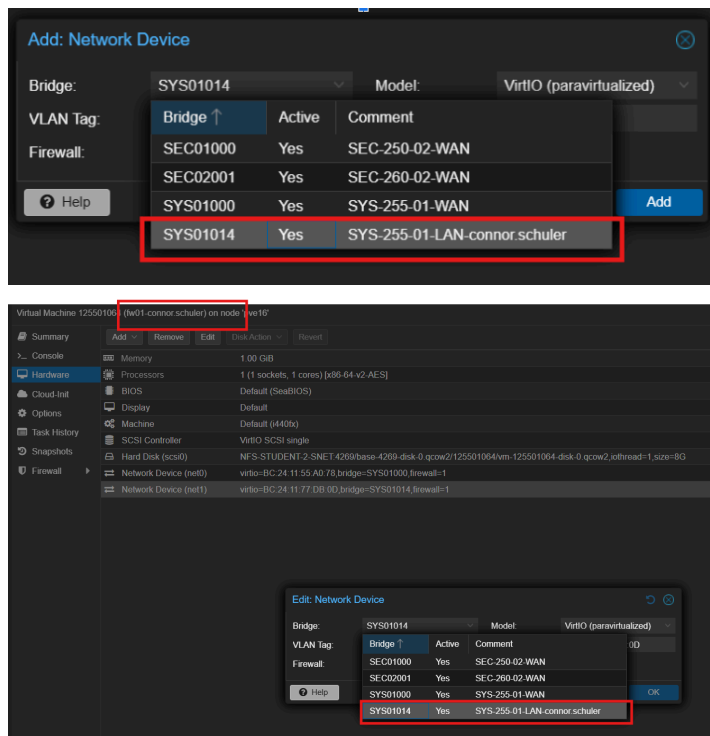


Connor Schuler
SYS-255-01
STR2026

Setup Screenshots

FW01 Interfaces:



FW01 IP Address Assignments:

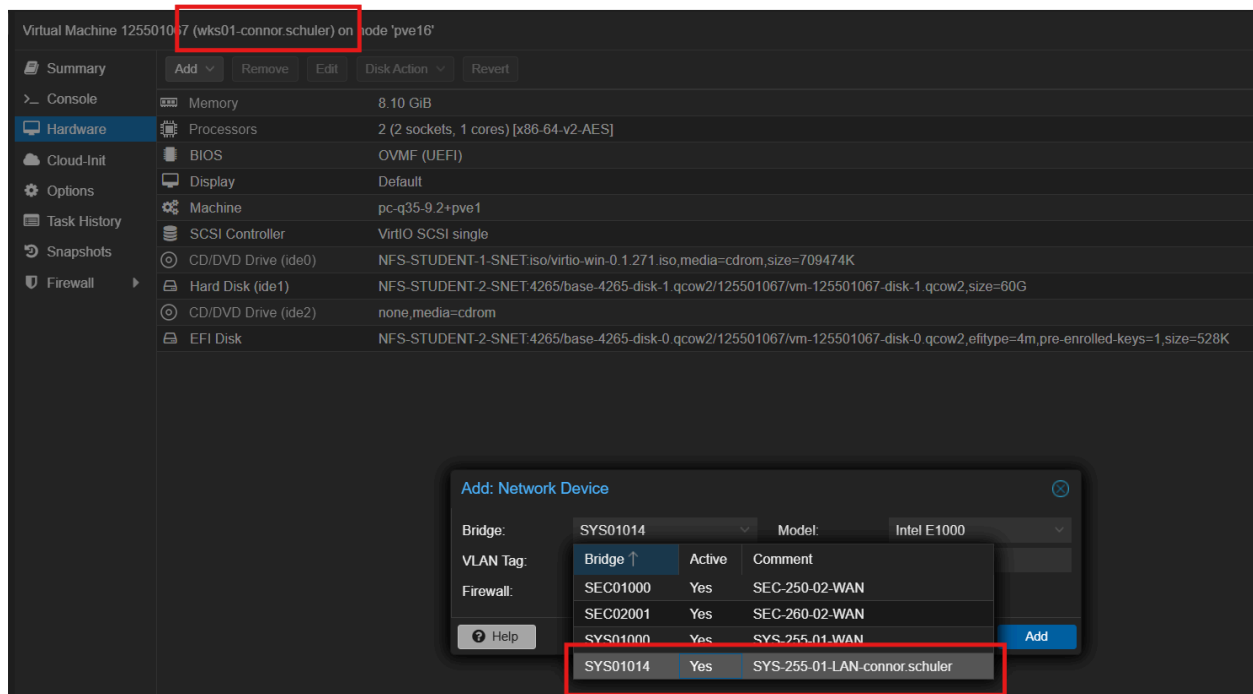
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4: 10.0.17.111/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24

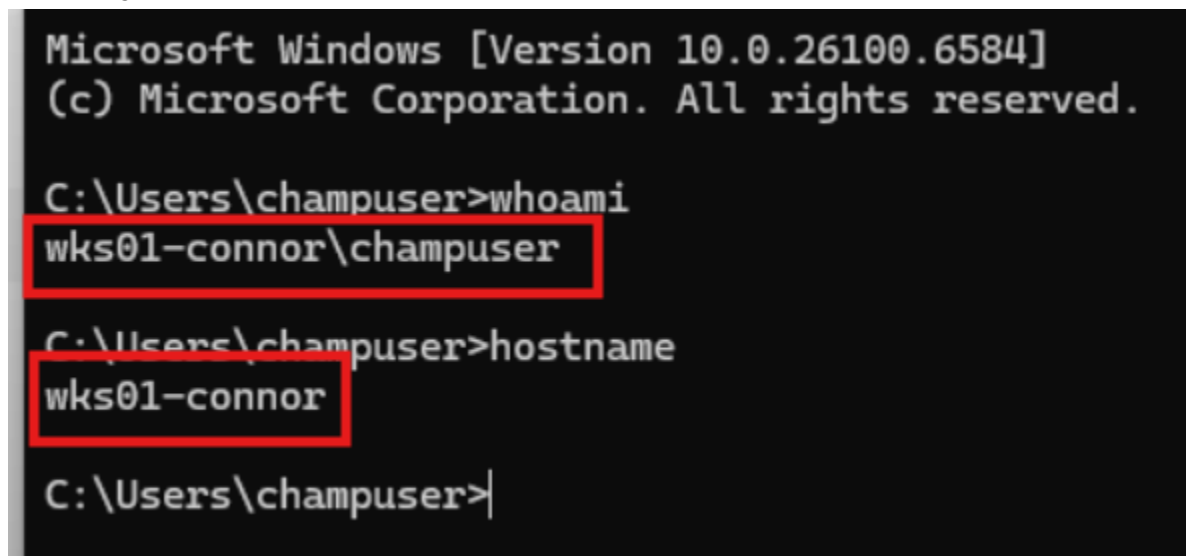
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Wks01 Interface:



Wks01 system name:



FW01 WebGUI Setup:

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

RFC1918 Networks

Block RFC1918 Private Networks ☐ Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (172.16/12, 192.168/16) as well as loopback addresses (127/8). This option is useful if your WAN network lies in such a private address space, too.

Wks01 IP Assignment:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK **Cancel**

Deliverables

Deliverable 1: Screenshot shows 7 transmitted and received ICMP pings to the domain champlain.edu. Each line shows 64 bytes sent and received, with zero packet loss. This indicated a successful ping.

```
[2.7.2-RELEASE][root@fw1-connor.connor.local]/root: ping champlain.edu
PING champlain.edu (23.185.0.3): 56 data bytes
64 bytes from 23.185.0.3: icmp_seq=0 ttl=54 time=14.025 ms
64 bytes from 23.185.0.3: icmp_seq=1 ttl=54 time=13.903 ms
64 bytes from 23.185.0.3: icmp_seq=2 ttl=54 time=14.211 ms
64 bytes from 23.185.0.3: icmp_seq=3 ttl=54 time=13.852 ms
64 bytes from 23.185.0.3: icmp_seq=4 ttl=54 time=14.206 ms
64 bytes from 23.185.0.3: icmp_seq=5 ttl=54 time=15.903 ms
64 bytes from 23.185.0.3: icmp_seq=6 ttl=54 time=13.965 ms
^C
--- champlain.edu ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 13.852/14.295/15.903/0.669 ms
[2.7.2-RELEASE][root@fw1-connor.connor.local]/root: █
```

Deliverable 2:

Image shows wks01 config, including hostname, IP address, gateway, and DNS server. These are highlighted by the rectangles.

```
PS C:\WINDOWS\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . wks01-connor
Primary Dns Suffix . . . . .
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : BC-24-11-12-C3-84
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::40eb:a746:8a49:9999%9(Preferred)
IPv4 Address. . . . . : 10.0.5.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.5.2
DHCPv6 IAID . . . . . : 112993297
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-FA-F8-56-BC-24-11-12-C3-84
DNS Servers . . . . . : 10.0.5.2
NetBIOS over Tcpip. . . . . : Enabled

PS C:\WINDOWS\system32> |
```

Image shows logged in user and computer hostname, both highlighted by red rectangle.

```
Microsoft Windows [Version 10.0.26100.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\champuser>whoami
wks01-connor\champuser

C:\Users\champuser>hostname
wks01-connor

C:\Users\champuser>
```

Image shows 1 successful 32 byte ICMP ping to [google.com](https://www.google.com).

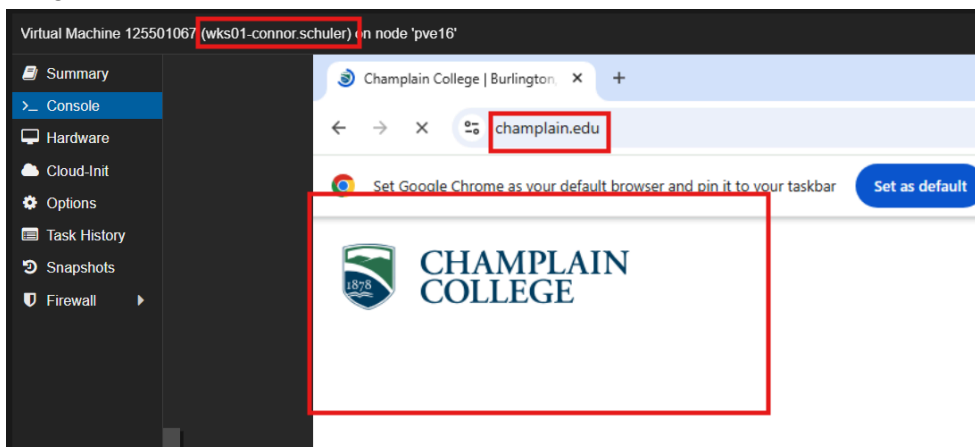
```
PS C:\WINDOWS\system32> ping -n 1 google.com

Pinging google.com [142.250.191.14] with 32 bytes of data:
Reply from 142.250.191.14: bytes=32 time=15ms TTL=113

Ping statistics for 142.250.191.14:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 15ms, Average = 15ms
PS C:\WINDOWS\system32>
```

Deliverable 3:

Image shows successful web connection to [champlain.edu](https://www.champlain.edu) from wks01.



Deliverable 4:

Image shows first 3 hops from wks01 to [champlain.edu](https://www.champlain.edu). Fw01 to the SYS-255 gateway, to the cyber.local external address domain.

```
C:\Users\connor.schuler>tracert -h 3 champlain.edu

Tracing route to champlain.edu [23.185.0.3]
over a maximum of 3 hops:
  1  <1 ms    <1 ms    <1 ms  fw1-connor.connor.local [10.0.5.2]
  2   1 ms     1 ms     1 ms   10.0.17.2
  3   3 ms     1 ms     1 ms   192.168.4.251

Trace complete.
```

Deliverable 5:

- Certain configurations did not apply until a reboot, is there a guide/list to what does and does not instantly apply?
- Most of the windows commands in the lab use powershell, but cmd also should work. Is there a reason powershell is used specifically?
- What do each of the 17 options in the pfsense CMD do/configure?

Deliverable 6: Document formatting

Deliverable 7: <https://journal.connorthenetworkjester.net/>