

# Proxy Services

—

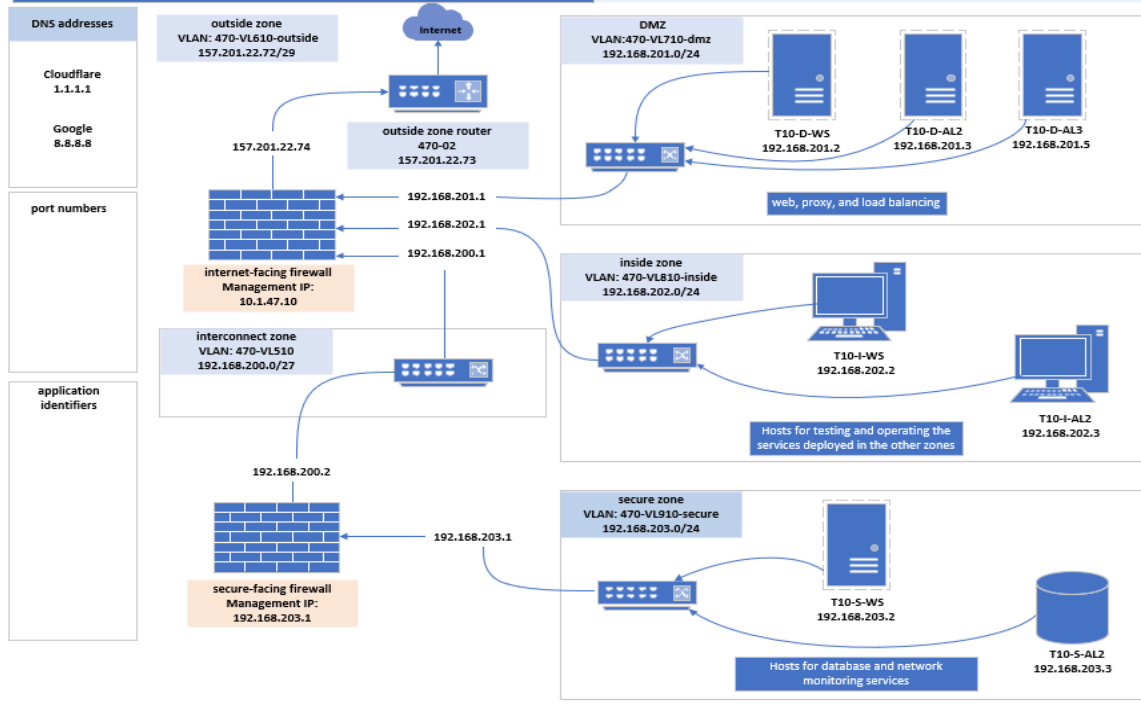
By Carlos Gerez Garcia, Christopher Ditto , and Mark Riley  
Slik

# cit470

## Task: Diagram

### team 10 Layer 3: outside zones' public IPv4 address assignments

public space (IPv4 subnet ID)	router	firewall (dynamic NAT)	static NAT	(broadcast)
157.201.22.72/29	157.201.22.73	157.201.22.74 470t10ra.cit.byui.edu	157.201.22.75- 157.201.22.78	157.201.22.79



## Team 10 network Diagram

# DNS resolution with unbound DNS Proxy

—

# Check ,Update ,and Install unbound

Run these commands to  
check for updates and  
install unbound

```
[rslik@t10-s-al2-localdomain ~]$ dnf check-update
```

```
[rslik@t10-s-al2-localdomain ~]$ sudo dnf -y update
```

```
[rslik@t10-s-al2-localdomain ~]$ dnf search unbound
```

```
unbound : unbound  
[rslik@t10-s-al2-localdomain ~]$ sudo dnf -y install unbound
```

```
Complete!
```

```
[rslik@t10-s-al2-localdomain ~]$ rpm -qi unbound  
Name : unbound
```

# Copy unbound.conf and edit

Cd into unbound  
and make a copy  
of the  
unbound.conf after  
making a copy  
open it in vi editor

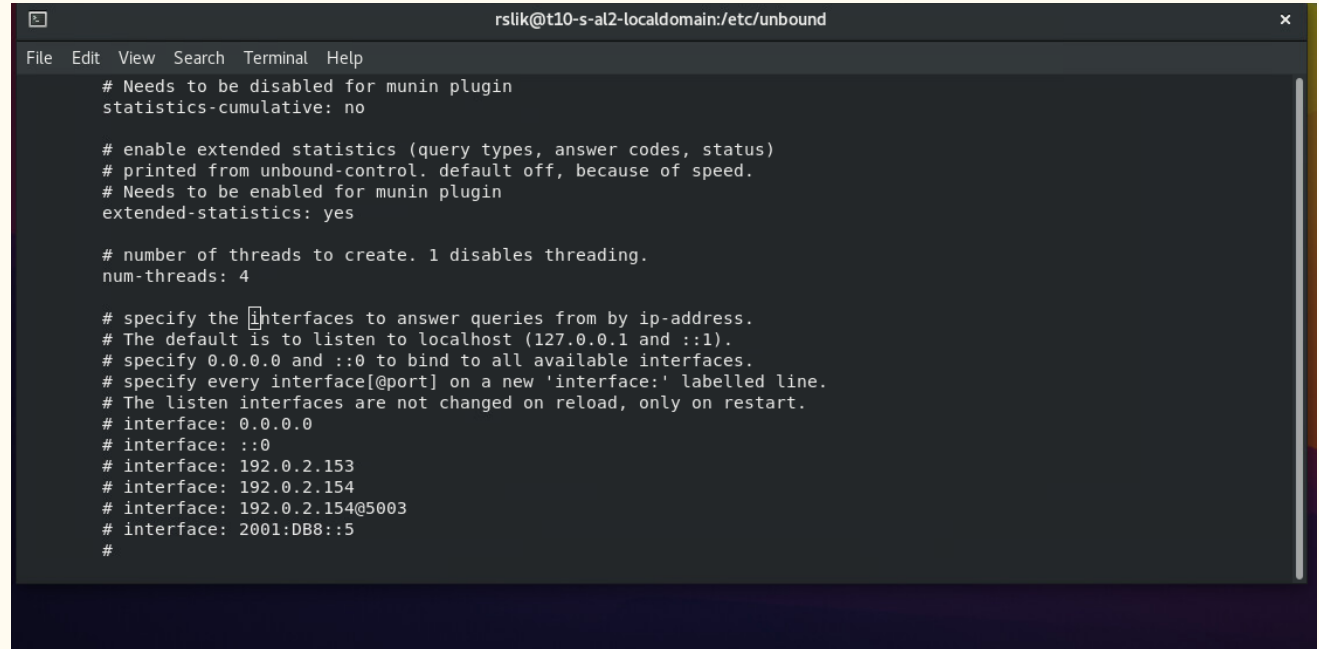
```
[rslik@t10-s-al2-localdomain ~]$ cd /etc/unbound
```

```
[rslik@t10-s-al2-localdomain unbound]$ sudo cp -p unbound.conf unbound.conf.orgin
```

```
[rslik@t10-s-al2-localdomain unbound]$ sudo vi unbound.conf
```

# Search for interface

Use / interface to  
search the  
document for  
interface



```
rslik@t10-s-al2-localdomain:/etc/unbound
File Edit View Search Terminal Help

# Needs to be disabled for munin plugin
statistics-cumulative: no

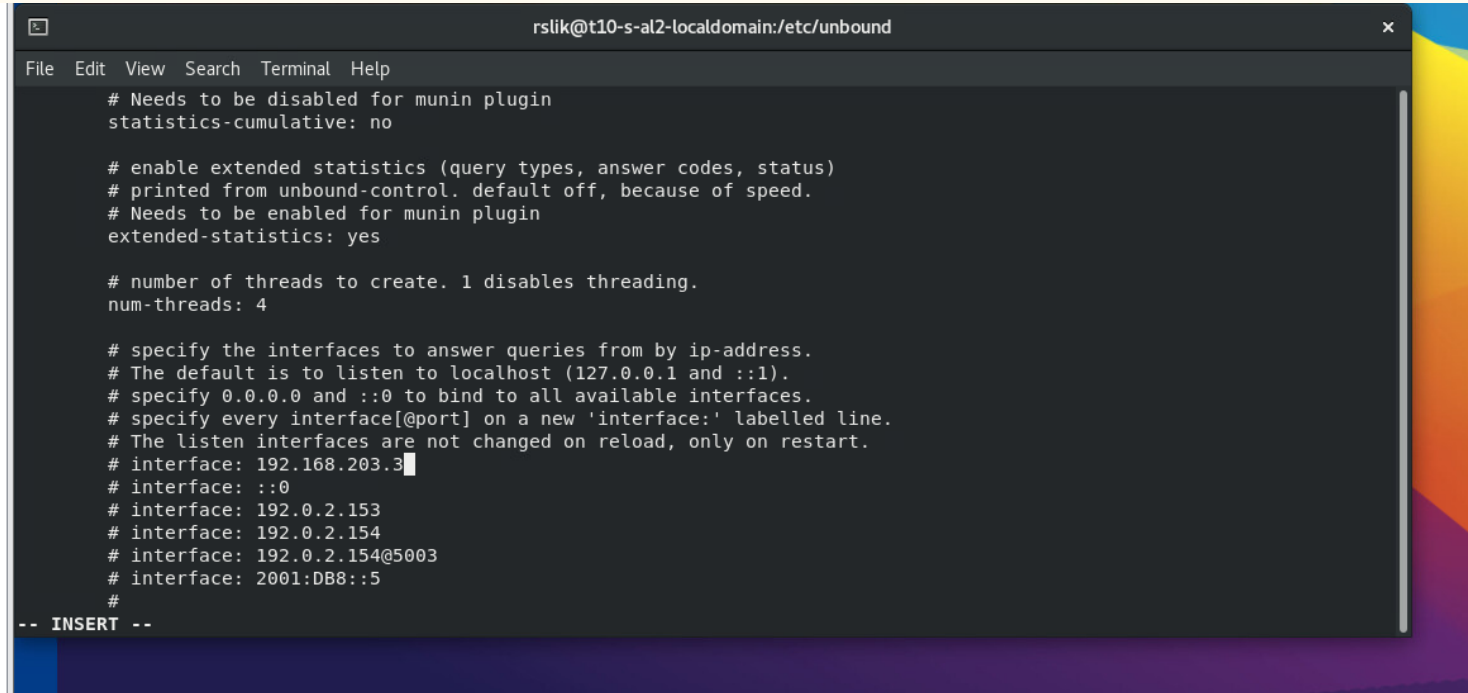
# enable extended statistics (query types, answer codes, status)
# printed from unbound-control. default off, because of speed.
# Needs to be enabled for munin plugin
extended-statistics: yes

# number of threads to create. 1 disables threading.
num-threads: 4

# specify the interfaces to answer queries from by ip-address.
# The default is to listen to localhost (127.0.0.1 and ::1).
# specify 0.0.0.0 and ::0 to bind to all available interfaces.
# specify every interface[@port] on a new 'interface:' labelled line.
# The listen interfaces are not changed on reload, only on restart.
# interface: 0.0.0.0
# interface: ::0
# interface: 192.0.2.153
# interface: 192.0.2.154
# interface: 192.0.2.154@5003
# interface: 2001:DB8::5
#
```

# Change interface too servers ip address

Use the vi editor to change the interface address to the servers address



```
rslik@t10-s-al2-localdomain:/etc/unbound
File Edit View Search Terminal Help
# Needs to be disabled for munin plugin
statistics-cumulative: no

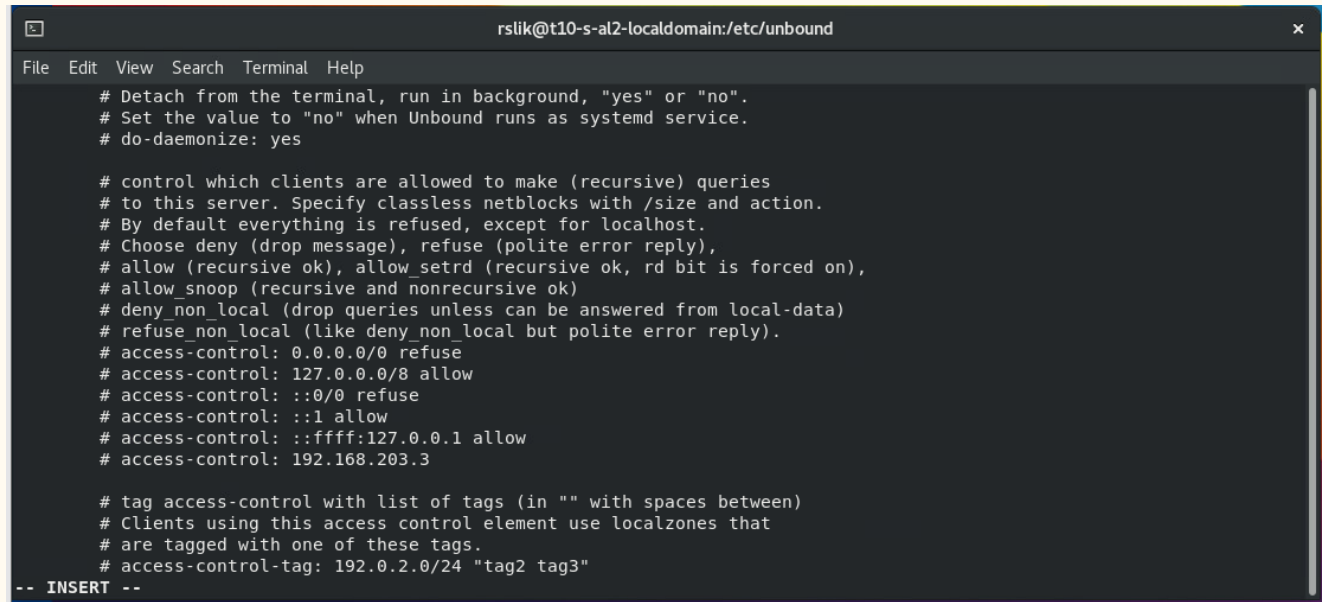
# enable extended statistics (query types, answer codes, status)
# printed from unbound-control. default off, because of speed.
# Needs to be enabled for munin plugin
extended-statistics: yes

# number of threads to create. 1 disables threading.
num-threads: 4

# specify the interfaces to answer queries from by ip-address.
# The default is to listen to localhost (127.0.0.1 and ::1).
# specify 0.0.0.0 and ::0 to bind to all available interfaces.
# specify every interface[@port] on a new 'interface:' labelled line.
# The listen interfaces are not changed on reload, only on restart.
# interface: 192.168.203.3
# interface: ::0
# interface: 192.0.2.153
# interface: 192.0.2.154
# interface: 192.0.2.154@5003
# interface: 2001:DB8::5
#
-- INSERT --
```

# Access control

Use /access-control to search the document. Add an access-control for the the DMZ sone



```
rslik@t10-s-al2-localdomain:/etc/unbound
File Edit View Search Terminal Help

# Detach from the terminal, run in background, "yes" or "no".
# Set the value to "no" when Unbound runs as systemd service.
# do-daemonize: yes

# control which clients are allowed to make (recursive) queries
# to this server. Specify classless netblocks with /size and action.
# By default everything is refused, except for localhost.
# Choose deny (drop message), refuse (polite error reply),
# allow (recursive ok), allow_setrd (recursive ok, rd bit is forced on),
# allow_snoop (recursive and nonrecursive ok)
# deny_non_local (drop queries unless can be answered from local-data)
# refuse_non_local (like deny_non_local but polite error reply).
# access-control: 0.0.0.0/0 refuse
# access-control: 127.0.0.0/8 allow
# access-control: ::0/0 refuse
# access-control: ::1 allow
# access-control: ::ffff:127.0.0.1 allow
# access-control: 192.168.203.3

# tag access-control with list of tags (in "" with spaces between)
# Clients using this access control element use localzones that
# are tagged with one of these tags.
# access-control-tag: 192.0.2.0/24 "tag2 tag3"

-- INSERT --
```



# Set forward address for dns

In the  
documents use  
/forward-zone

And the  
address for the  
dns.

Exit the  
document

```
# forward-zone:
#   name: "."
#   forward-addr: 8.8.8.8
#   forward-addr: 8.8.4.4
#
# You can now also dynamically create and
```

# Add DNS to the firewall

Use the commands as shown to check the firewall allow services and then add DNS if it is not there. Check to make sure it got added properly

```
[rslik@t10-s-al2-localdomain unbound]$ sudo firewall-cmd --list-services
```

```
[rslik@t10-s-al2-localdomain unbound]$ sudo firewall-cmd --add-service=dns --permanent
```

```
[rslik@t10-s-al2-localdomain unbound]$ sudo firewall-cmd --list-services  
cockpit dhcpv6-client dns mysql ssh
```

# Enable and Start

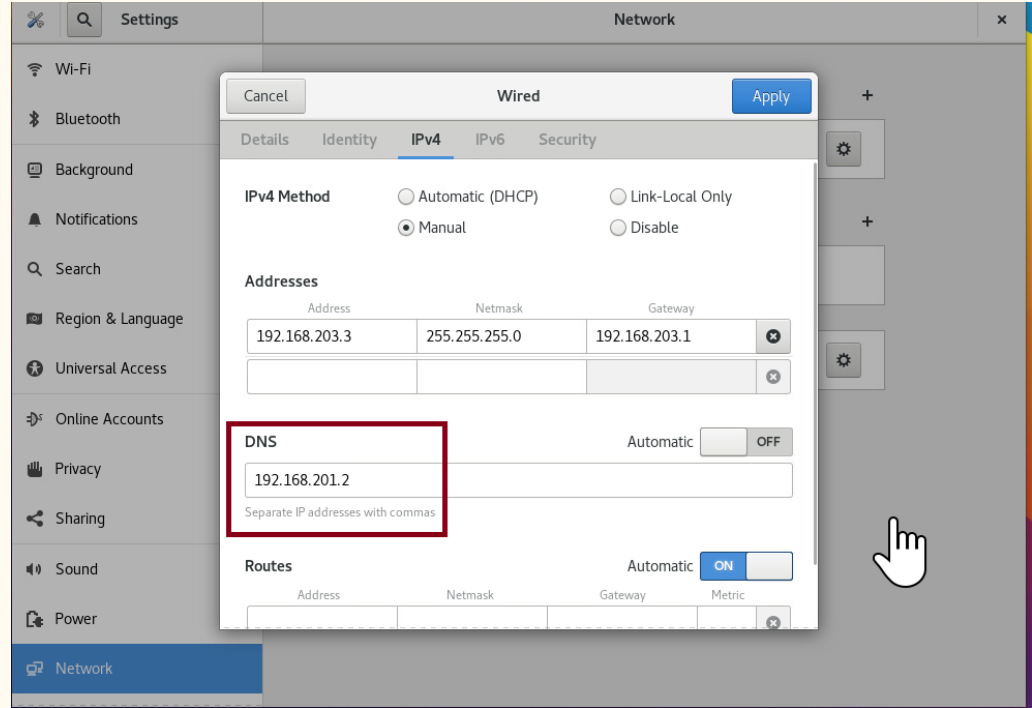
Use these  
commands to enable  
Unbound and Start  
unbound

```
[rslik@t10-s-al2-localdomain unbound]$ systemctl status unbound
● unbound.service - Unbound recursive Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/unbound.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

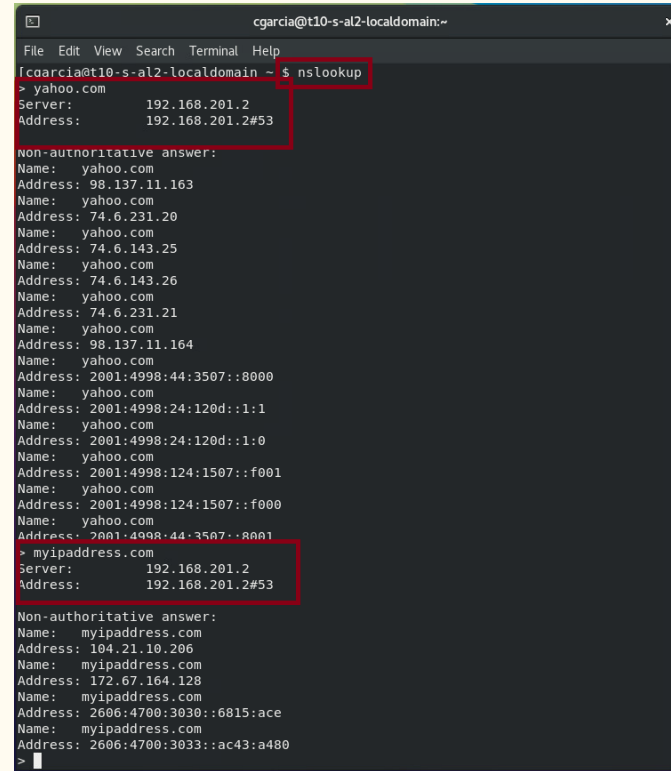
```
[rslik@t10-s-al2-localdomain unbound]$ sudo systemctl enable unbound
```

# Set unbound for DNS for linux DMZ

Check and make sure that the DNS setup for your DMZ linux machine



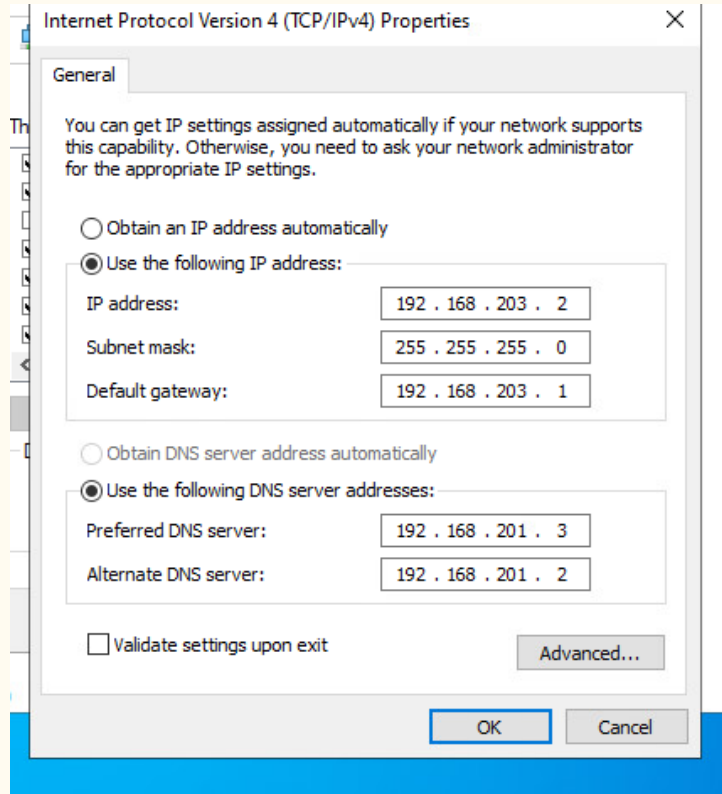
# You can also check in the terminal if it is working



```
cgarcia@t10-s-al2-localdomain:~  
File Edit View Search Terminal Help  
cgarcia@t10-s-al2-localdomain ~ $ nslookup  
> yahoo.com  
Server:      192.168.201.2  
Address:     192.168.201.2#53  
  
non-authoritative answer:  
Name:  yahoo.com  
Address: 98.137.11.163  
Name:  yahoo.com  
Address: 74.6.231.20  
Name:  yahoo.com  
Address: 74.6.143.25  
Name:  yahoo.com  
Address: 74.6.143.26  
Name:  yahoo.com  
Address: 74.6.231.21  
Name:  yahoo.com  
Address: 98.137.11.164  
Name:  yahoo.com  
Address: 2001:4998:44:3507::8000  
Name:  yahoo.com  
Address: 2001:4998:24:120d::1:1  
Name:  yahoo.com  
Address: 2001:4998:24:120d::1:0  
Name:  yahoo.com  
Address: 2001:4998:124:1507::f001  
Name:  yahoo.com  
Address: 2001:4998:124:1507::f000  
Name:  yahoo.com  
Address: 2001:4998:44:3507::8001  
> myipaddress.com  
Server:      192.168.201.2  
Address:     192.168.201.2#53  
  
Non-authoritative answer:  
Name:  myipaddress.com  
Address: 104.21.10.206  
Name:  myipaddress.com  
Address: 172.67.164.128  
Name:  myipaddress.com  
Address: 2606:4700:3030::6815:ace  
Name:  myipaddress.com  
Address: 2606:4700:3033::ac43:a480  
>
```

# Check DNS on Windows

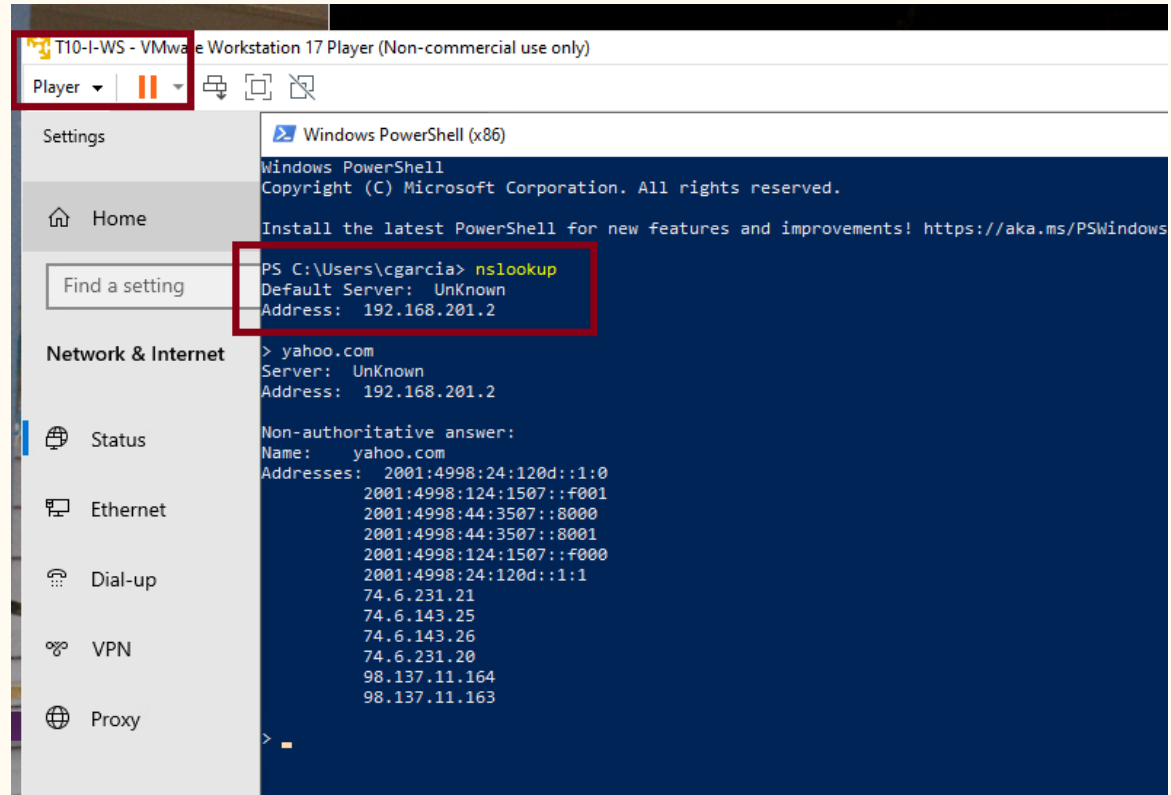
Check your Ipv4 address  
and make sure that the  
DNS address is set



# Check DNS on Windows

You can also check in the terminal if it is working using

nslookup



```
T10-I-WS - VMware Workstation 17 Player (Non-commercial use only)
Player
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy

Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\cgarcia> nslookup
Default Server: UnKnown
Address: 192.168.201.2

> yahoo.com
Server: UnKnown
Address: 192.168.201.2

Non-authoritative answer:
Name: yahoo.com
Addresses: 2001:4998:24:120d::1:0
           2001:4998:124:1507::f001
           2001:4998:44:3507::8000
           2001:4998:44:3507::8001
           2001:4998:124:1507::f000
           2001:4998:24:120d::1:1
           74.6.231.21
           74.6.143.25
           74.6.143.26
           74.6.231.20
           98.137.11.164
           98.137.11.163

>
```

Squid Proxy

—



# How to Download and install squid in Alma Linux

In a Linux terminal use this commands.

The first 2 commands check for updates. The third installs squid.

The final 2 commands check that those 2 files are identical. They are the configuration file and a backup. They are identical as you will noticed when running diff.

```
[cditto@T10-D-AL2 ~]$ dnf check-update
```

```
[cditto@T10-D-AL2 ~]$ sudo dnf -y update
```

```
[cditto@T10-D-AL2 ~]$ sudo dnf -y install squid
```

```
[cditto@T10-D-AL2 ~]$ cd /etc/squid
```

```
[cditto@T10-D-AL2 squid]$ sudo diff squid.conf squid.conf.default
```

# Firewall rules edition.

The first line confirm that squid is not included as allowed. The second command looks if is supported that you see is true. Then the third and fourth command change the configuration of this endpoint to allow request from squid.

```
[cditto@T10-D-AL2 squid]$ sudo firewall-cmd --list-services  
cockpit dhcpv6-client dns ssh
```

```
[cditto@T10-D-AL2 squid]$ sudo firewall-cmd --get-services
```

```
[cditto@T10-D-AL2 squid]$ sudo firewall-cmd --add-service=squid --permanent  
success
```

```
[cditto@T10-D-AL2 squid]$ sudo firewall-cmd --reload  
success
```

# Check status and start service.

Again the first command check if squid is enabled and active. Since is not enabled and is inactive as all new services in Linux, enable and start it with the final 2 commands.

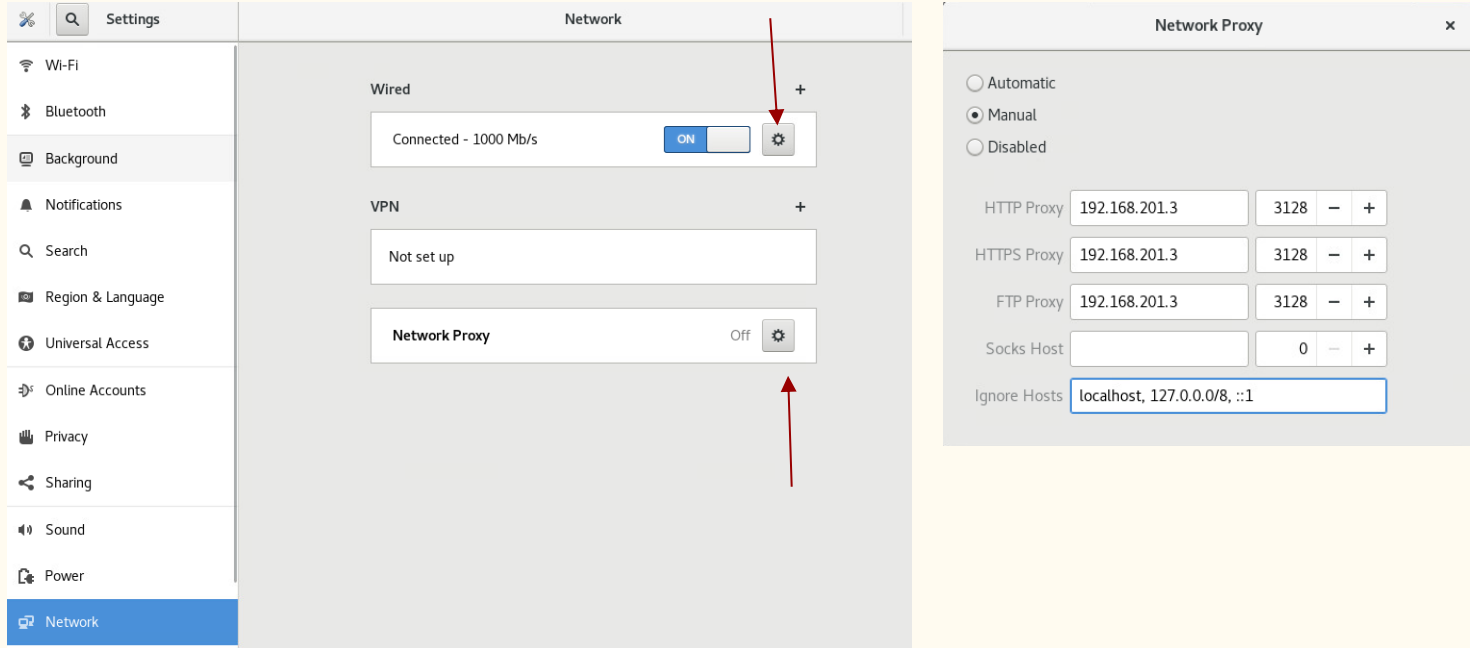
```
[cditto@T10-D-AL2 squid]$ systemctl status squid
```

```
[cditto@T10-D-AL2 squid]$ sudo systemctl enable squid  
[sudo] password for cditto: 
```

```
[cditto@T10-D-AL2 squid]$ sudo systemctl start squid
```

# Configure machines in the secure zone to use squid.

On the gui, in network select network proxy and then set the ip address of the Alma Linux in the DMZ zone configured with squid. Use the port 3128. Remember to turn off and on the interface to be sure the new configuration is applied.



Now you can update your Alma Linux server in the secure zone.

```
[cditto@t10-s-al2-localdomain ~]$ dnf check-update
```

```
[cditto@t10-s-al2-localdomain ~]$ dnf check-update
```

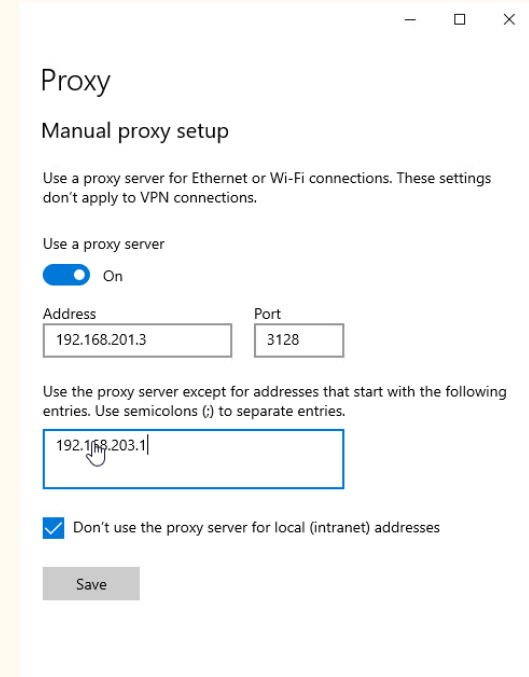
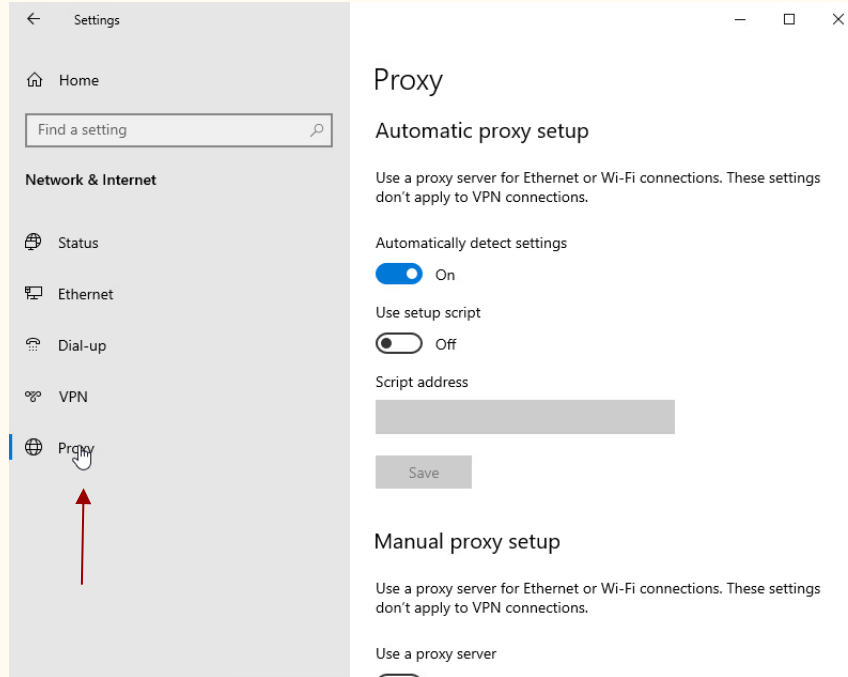
```
[cditto@t10-s-al2-localdomain ~]$ sudo dnf -y update
```

Remember to change the `/etc/dnf/dnf.conf` file and add in the last line:

```
proxy=http://192.168.201.3:3128
```

# Configuration of web services in a Windows system.

Turned off the automatic proxy detection and on Use a proxy server. Fill in the required information. Add the secure gateway as a proxy exception.



# Add a policy in the Palo Alto firewall to allow traffic for the squid services in the DMZ zone.

This rule is similar to the one we have from before, but this time we will select the squid service as the application to be allowed.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DE
5	01/28 18:07:30	deny	interconn...	dmz	192.168.203.2			192.168.201.3	
6	T10-secure-to-dmz-i...	none	universal	interconnect	192.168.20				
7	T10-to-Secure-Remo...	none	universal	dmz	192.168.20				
8	intrazone-default	none	intrazone	any	any				
9	interzone-default	none	interzone	any	any				

### Clone

Selected Rules

NAME
T10-secure-to-dmz-inside

Rule order: After Rule T10-secure-to-dmz-inside

☒ Error out on first detected error in validation

OK Cancel

+ Add - Delete Clone Override Revert Enable Disable Move

# Rename clone

Under the  
General tab  
enter the rule  
name using  
your team  
name  
followed by -  
squid-proxy

5	T10-secure-to-dmz-i...	none	universal	interconne
6	<u>T10-secure-to-dmz-inside-1</u> e v		universal	interconne

Security Policy Rule

**General** | Source | Destination | Application | Service/URL Category | Actions | Usage

Name T10-squid-proxy

Rule Type universal (default)

Description

Tags

Group Rules By Tag None

Audit Comment

[Audit Comment Archive](#)



# Start the rule by selecting policy and add a new service security policy.

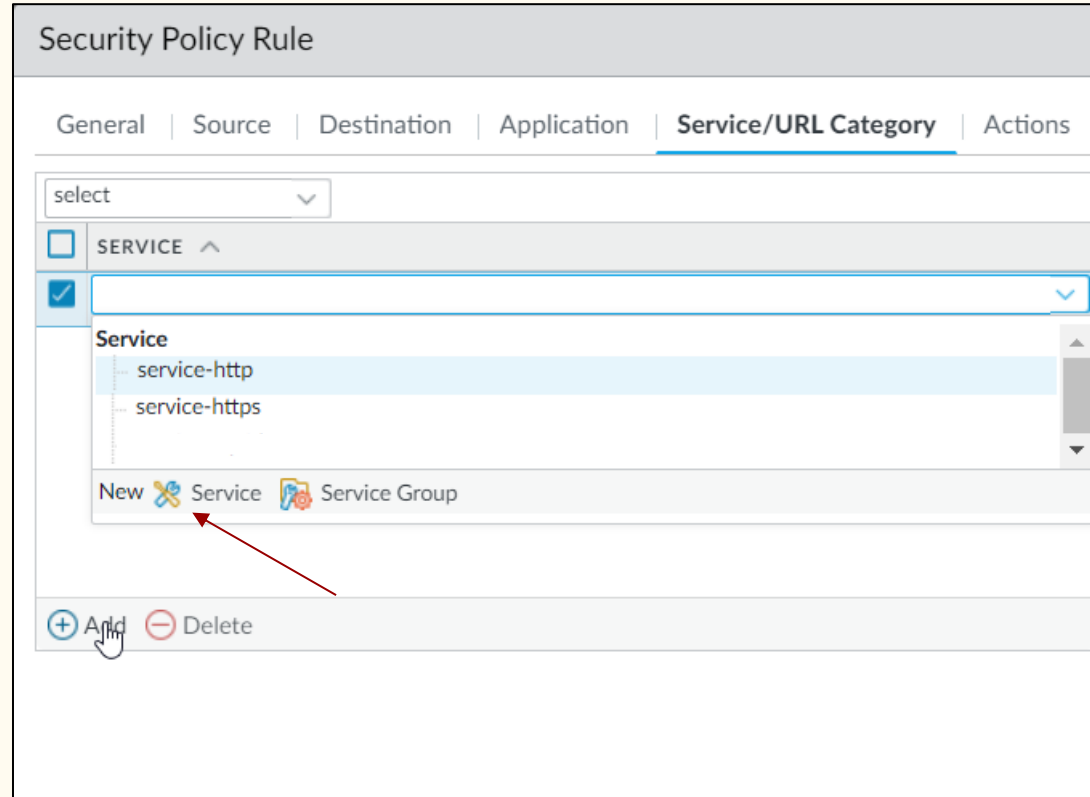
Under the service/URL Category tab, change from application default to select

The screenshot shows the 'Security Policy Rule' configuration window. It has a title bar 'Security Policy Rule' and a tabbed interface with 'General', 'Source', 'Destination', 'Application', 'Service/URL Category', and 'Actions'. The 'Service/URL Category' tab is selected and underlined. Below the tabs is a dropdown menu currently showing 'select'. Below the dropdown is a section header 'SERVICE' with an upward arrow. The main area is a large yellow rectangle. At the bottom, there are '+ Add' and '- Delete' buttons. Red arrows point to the title bar, the 'Service/URL Category' tab, the dropdown menu, and the '+ Add' button. A mouse cursor is hovering over the '+ Add' button.

General	Source	Destination	Application	<u>Service/URL Category</u>	Actions
<div>select</div> <div>SERVICE ^</div> <div></div> <div>+ Add - Delete</div>					

# Create a new service

In select click  
on new  
services to  
create a new  
service object.



# Set the name of the policy, the protocol and port.

Name the object  
service- squid.

Under Description  
insert squid.

Under the Destination  
port select 3128.

Under Tags enter  
Squid.

The reason we are  
doing this is because the  
firewall does not expect  
a web object to come  
through port 3128 and  
will deny that object  
type whereas, squid will  
run unhindered.

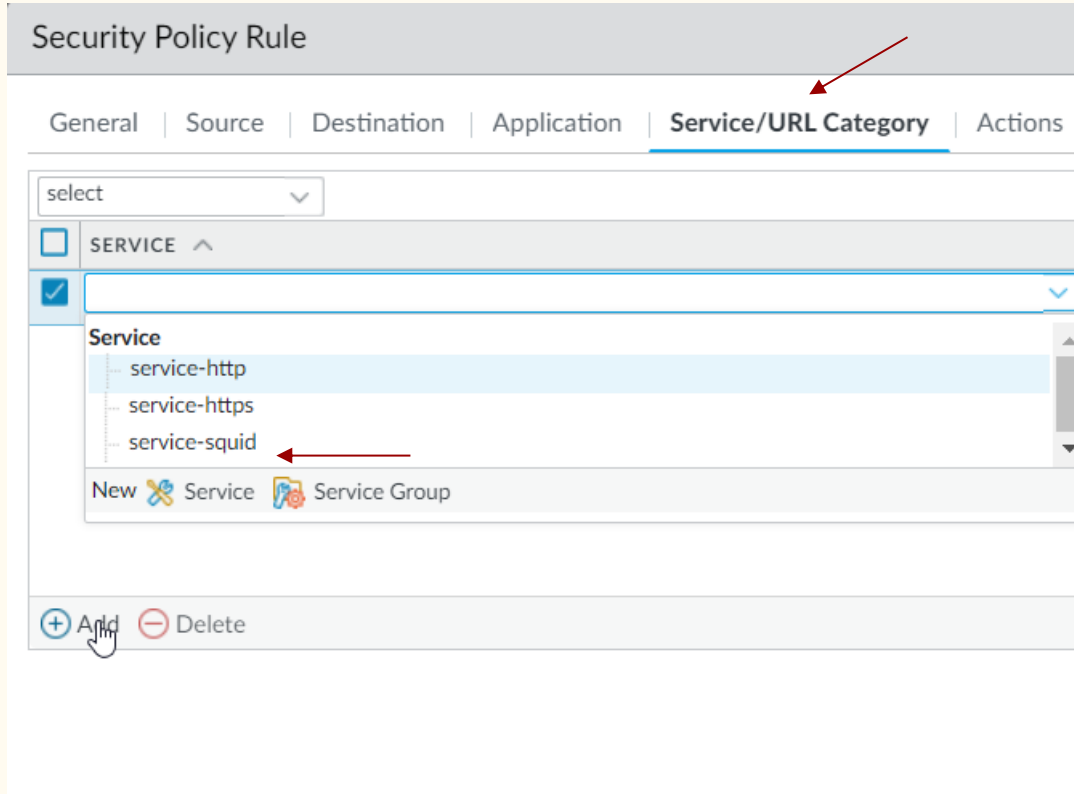
The screenshot shows a configuration form for a Service object. The fields are as follows:

- Name:** service-squid
- Description:** squid
- Protocol:** TCP (selected), UDP
- Destination Port:** 3128
- Source Port:** [ $\geq 0$ ]
- Session Timeout:** Inherit from application (selected), Override
- Tags:** squid X

Below the Source Port field, a note states: "Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)".

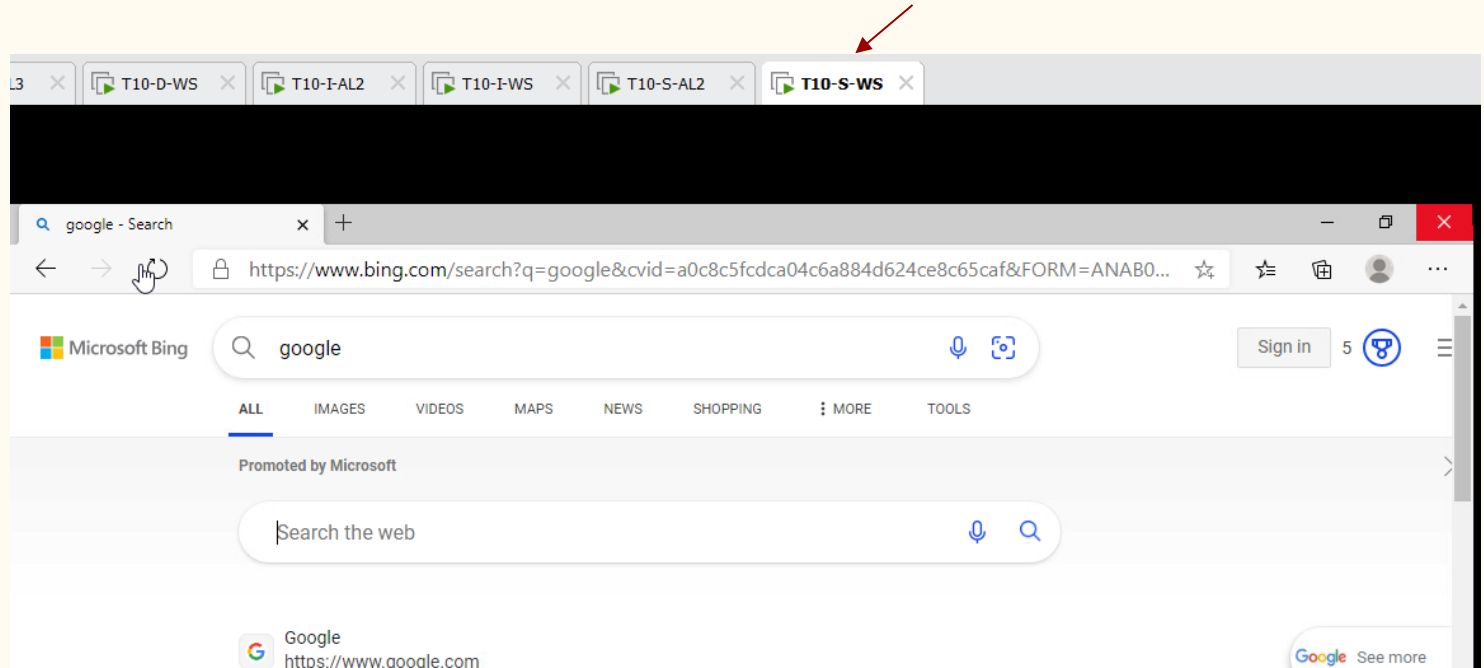
# In service/Url Category select service-squid.

Select the new  
object  
“service-squid”



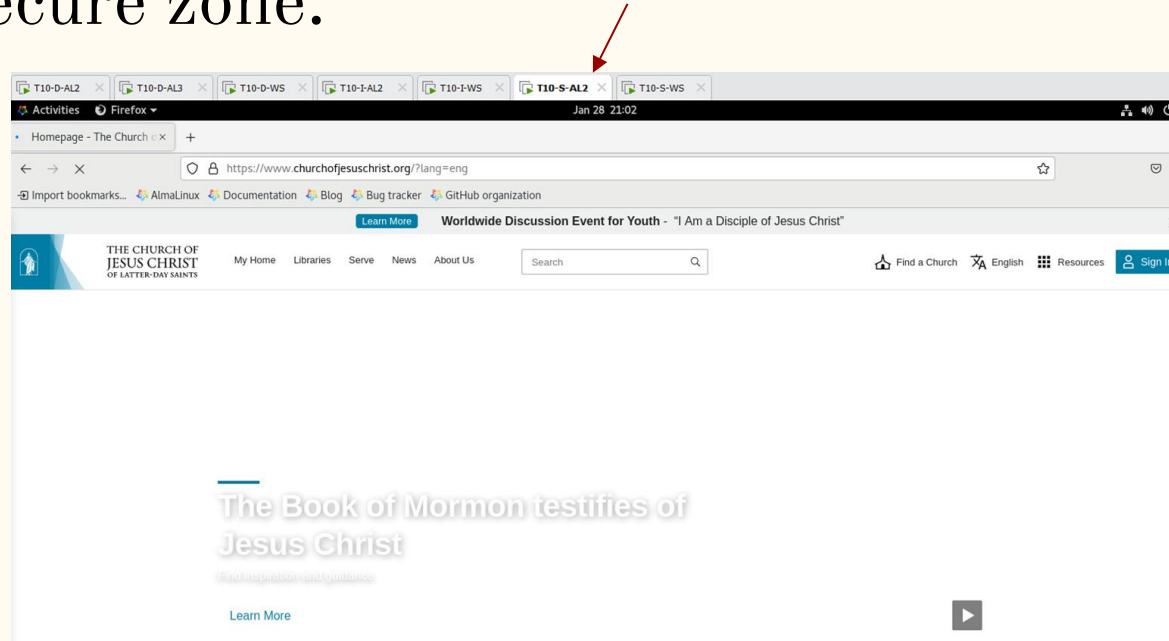
# Confirm connectivity in the secure zone Windows system.

With the firewalls configured we have internet connectivity to our Windows machine



# Confirmation of internet connection in the Alma Linux system in the secure zone.

As well as to  
our Linux  
machine.



# Configure updates from the proxy server on Windows.

In windows is a different proxy setting for administrative task as updates. This is the command for configure the settings on Windows.

```
PS C:\Windows\system32> netsh winhttp show proxy  
  
Current WinHTTP proxy settings:  
  
    Direct access (no proxy server).  
PS C:\Windows\system32> netsh winhttp set proxy 192.168.201.3:3128_
```

Challenges we  
faced



# It was necessary to create an object tailored for the squid services to grant access through the Palo Alto firewall.

The only issue that I ran into was learning how to create an object and then due to having to make some changes, how to delete an object. Neither was difficult it just took a minute to puzzle it out.

