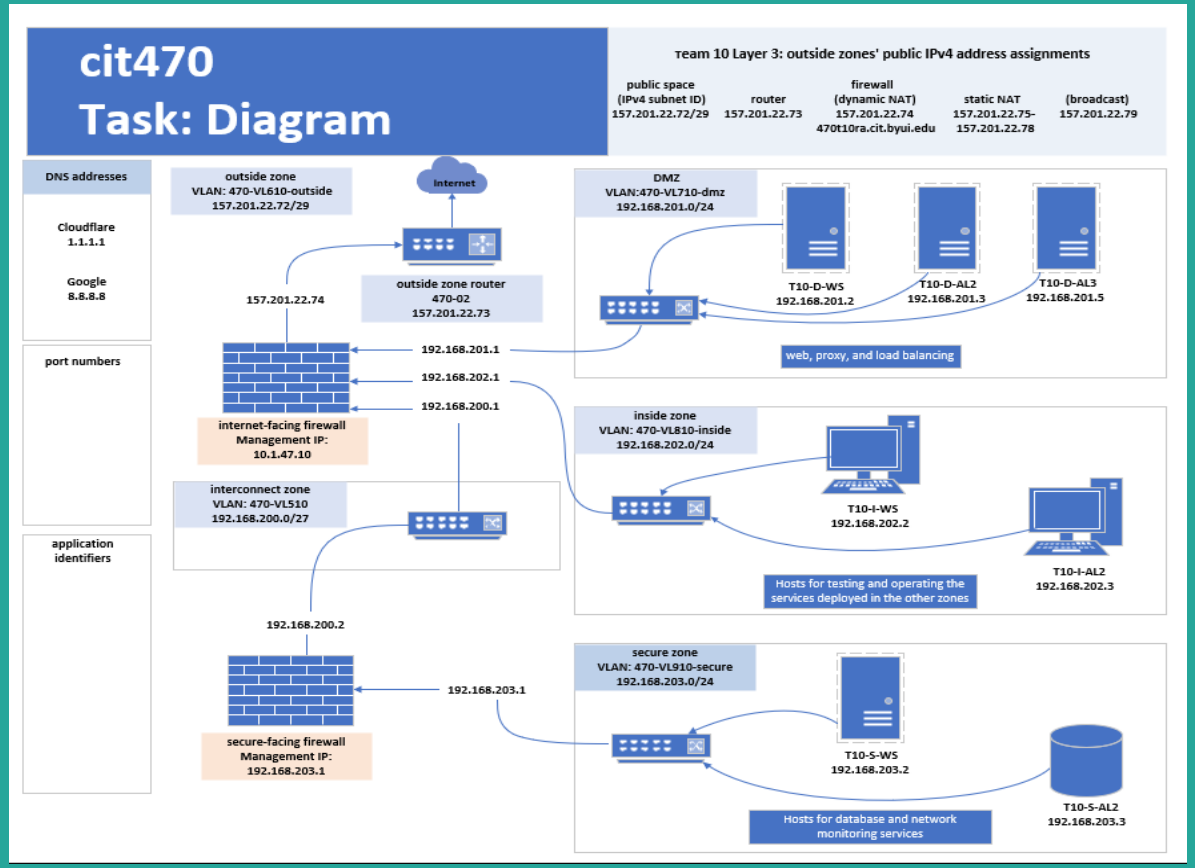
Proxy Services

—

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



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
```

```
[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
#
```

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

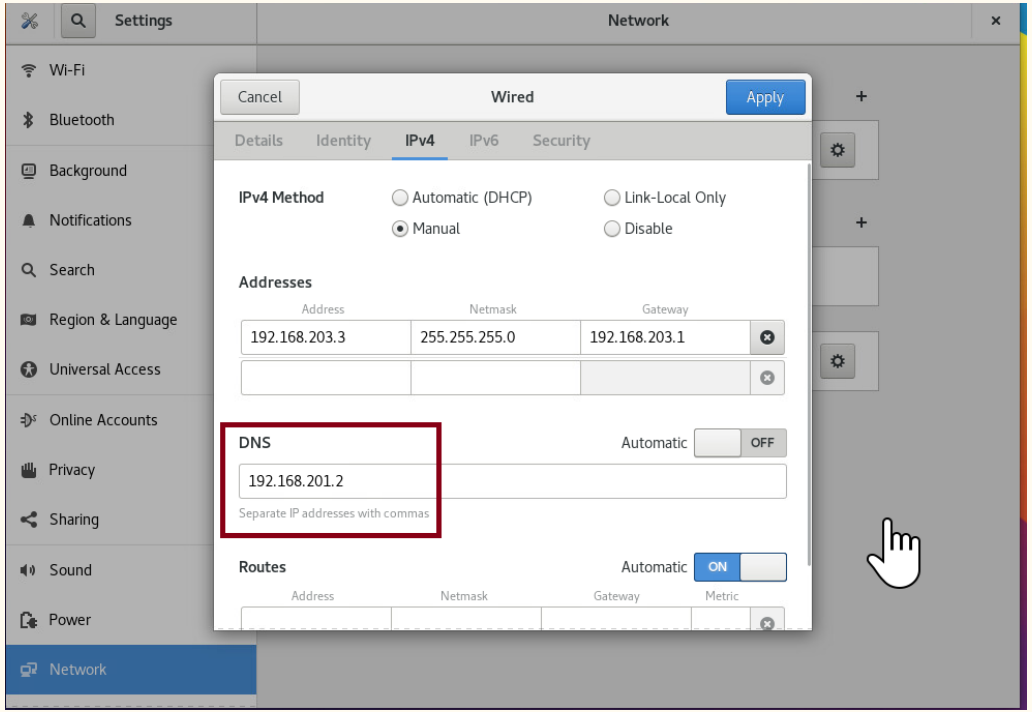
Use these commands to enable Unbound and Start unbound

```
[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)
```

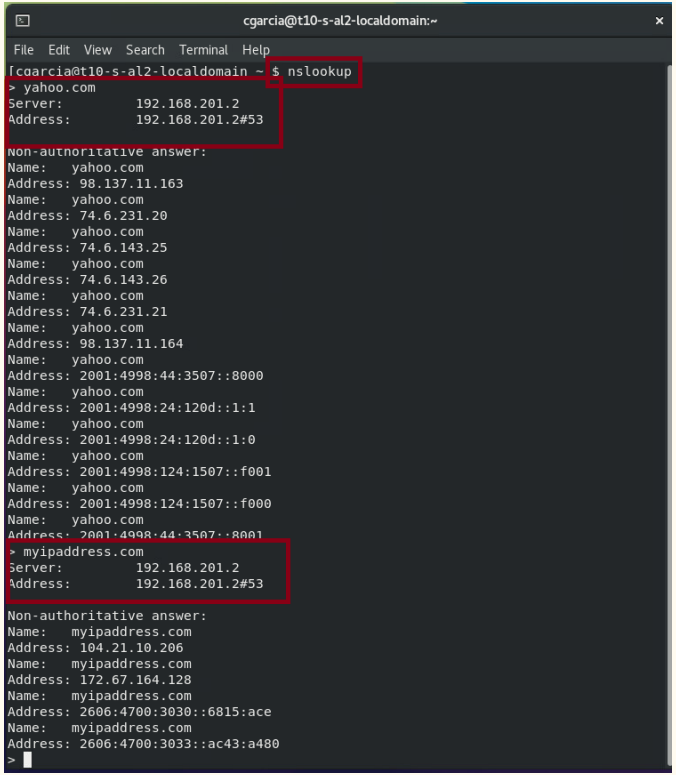
```
[rslik@t10-s-al2-localdomain unbound]$ sudo systemctl enable unbound
```

Set unbound for DNS for linux DMZ

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

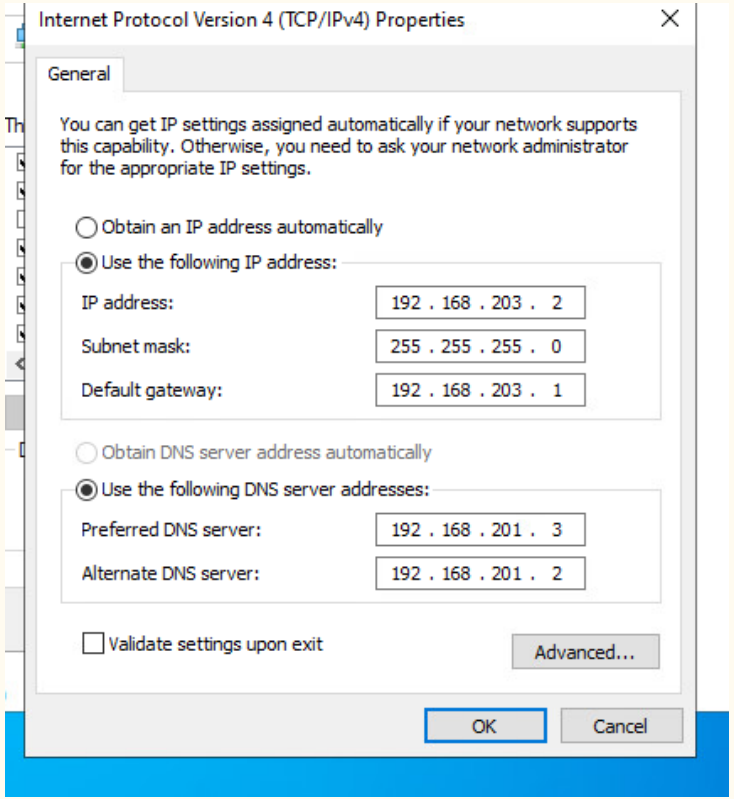


You can also check in the terminal if it is working



Check DNS on Windows

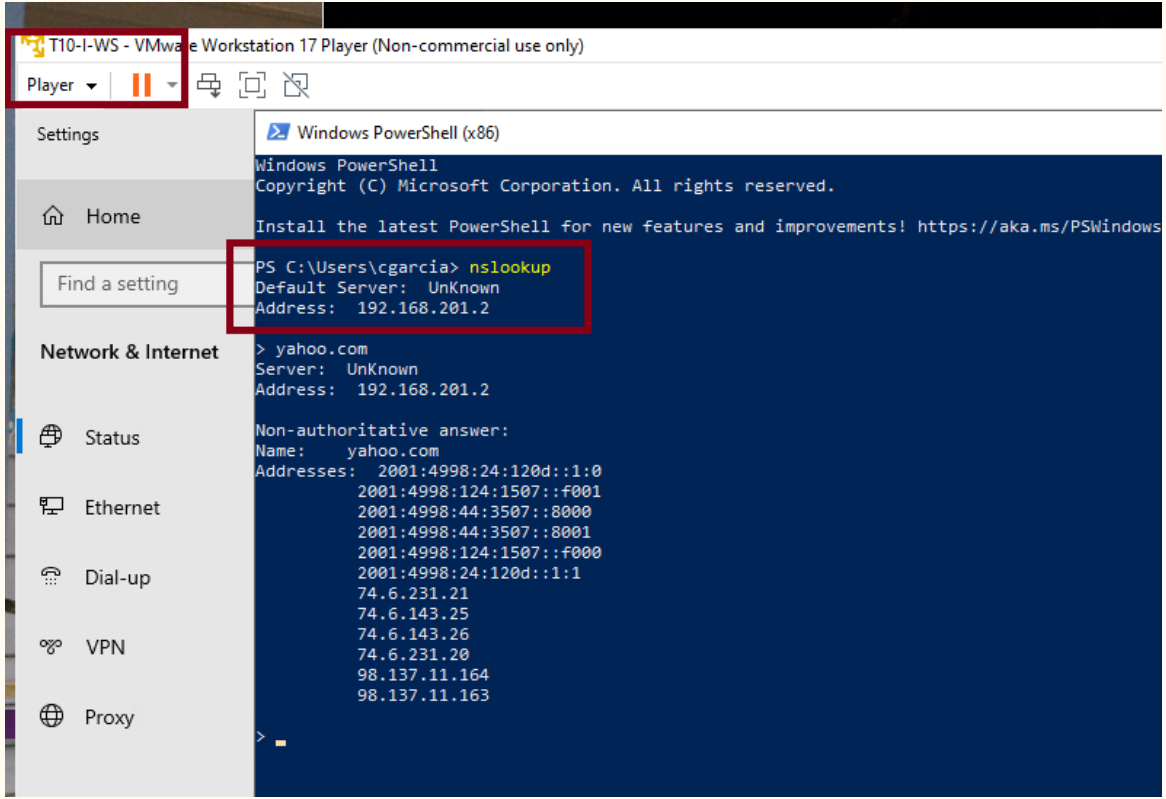
Check your Ipv4 address and make sure that the DNS address is set



Check DNS on Windows

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

nslookup



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.

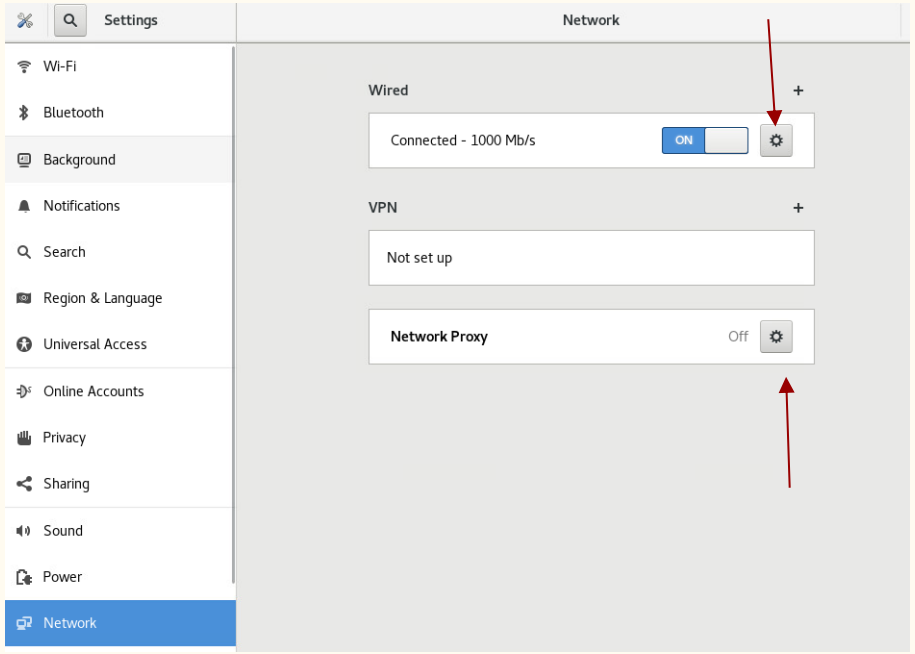
```
[cditto@T10-D-AL2 squid]$ systemctl status squid
```

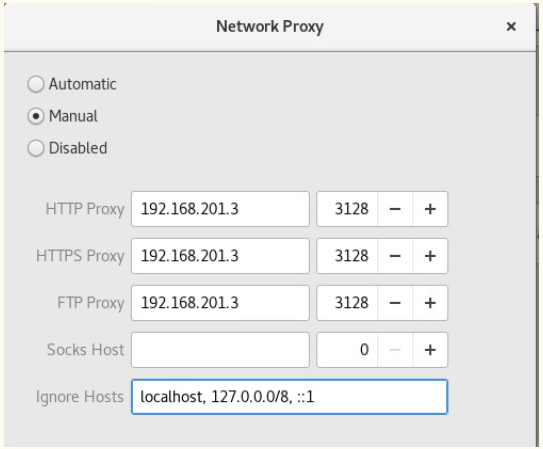
```
[cditto@T10-D-AL2 squid]$ sudo systemctl enable squid
[sudo] password for cditto:
```

```
[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
```

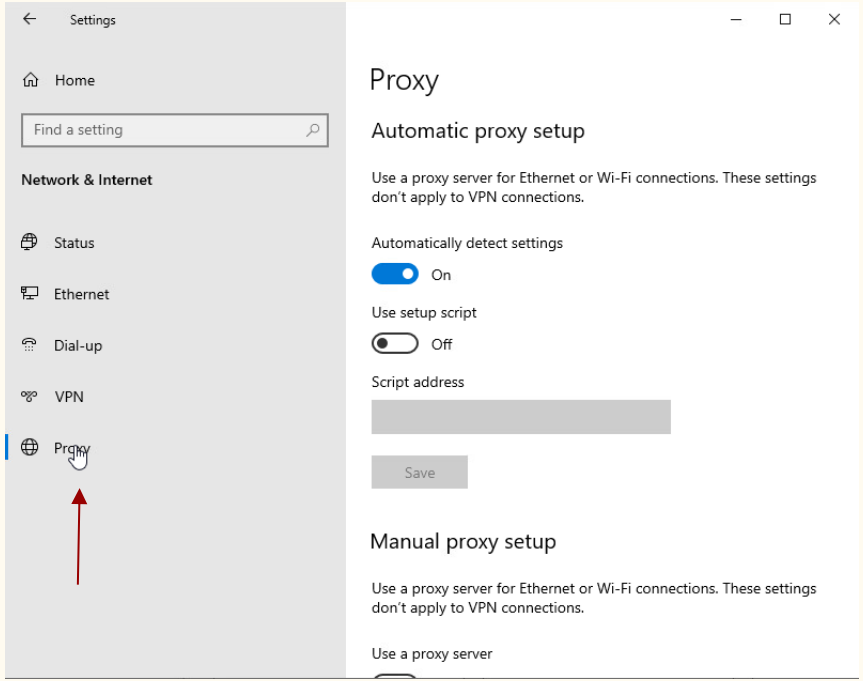
```
[cditto@t10-s-al2-localdomain ~]$ dnf check-update
```

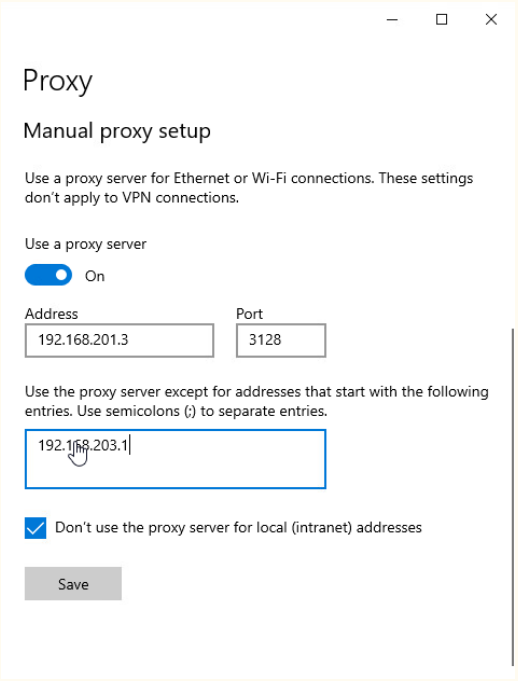
```
[cditto@t10-s-al2-localdomain ~]$ sudo dnf -y update
```

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	DES DYN AD
	01/28 18:07:30	deny	interconn...	dmz	192.168.203.2			192.168.201.3	

5	T10-secure-to-dmz-i...	none	universal	interconnect	192.168.20
6	T10-to-Secure-Remo...	none	universal	dmz inside	192.168.20 192.168.20
7	intrazone-default	none	intrazone	any	any
8	interzone-default	none	interzone	any	any

Add Delete Clone Override Revert Enable Disable Move

Clone

Selected Rules

NAME
T10-secure-to-dmz-inside

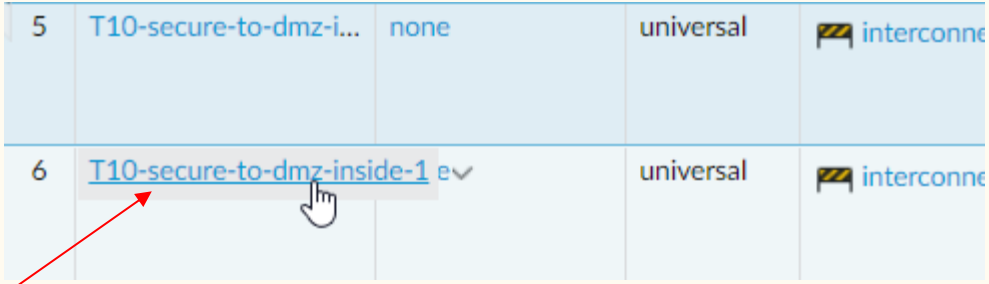
Rule order: After Rule — T10-secure-to-dmz-inside

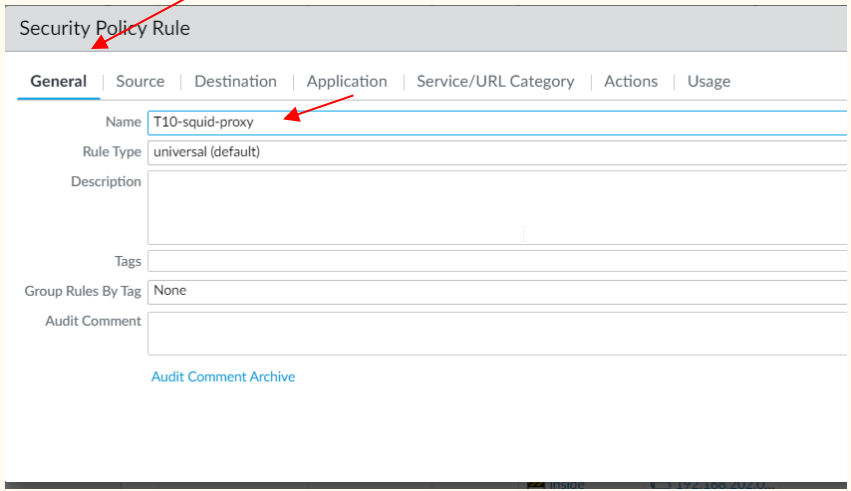
Error out on first detected error in validation

OK Cancel

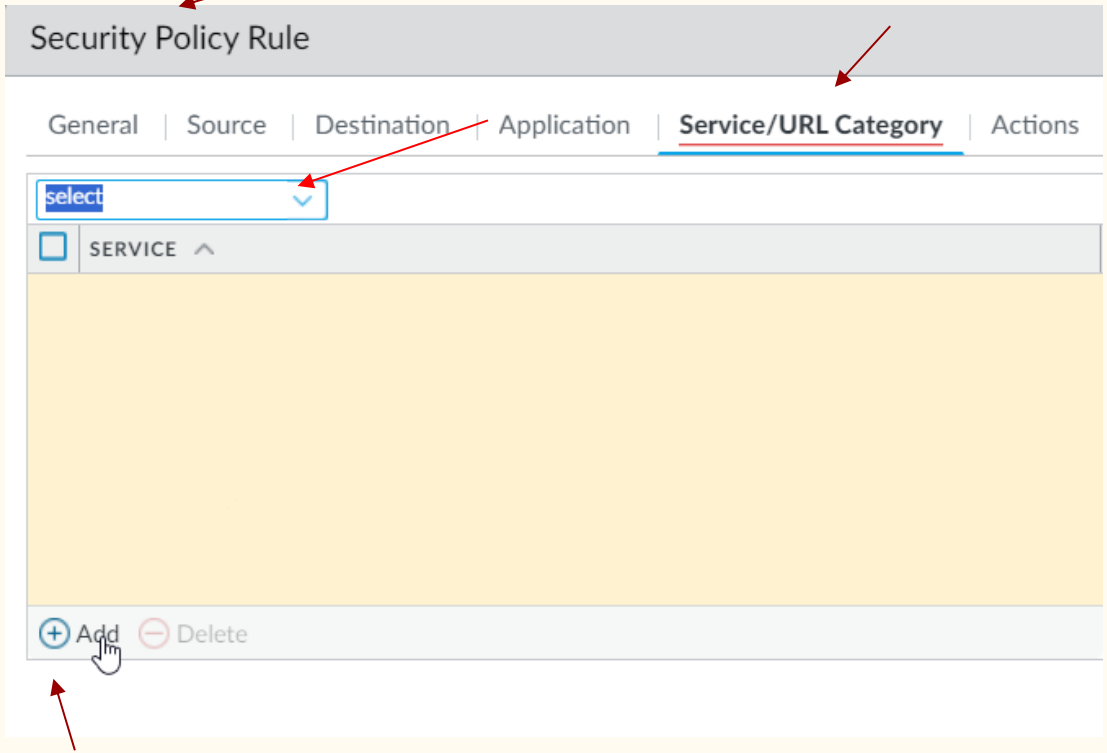
Rename clone

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





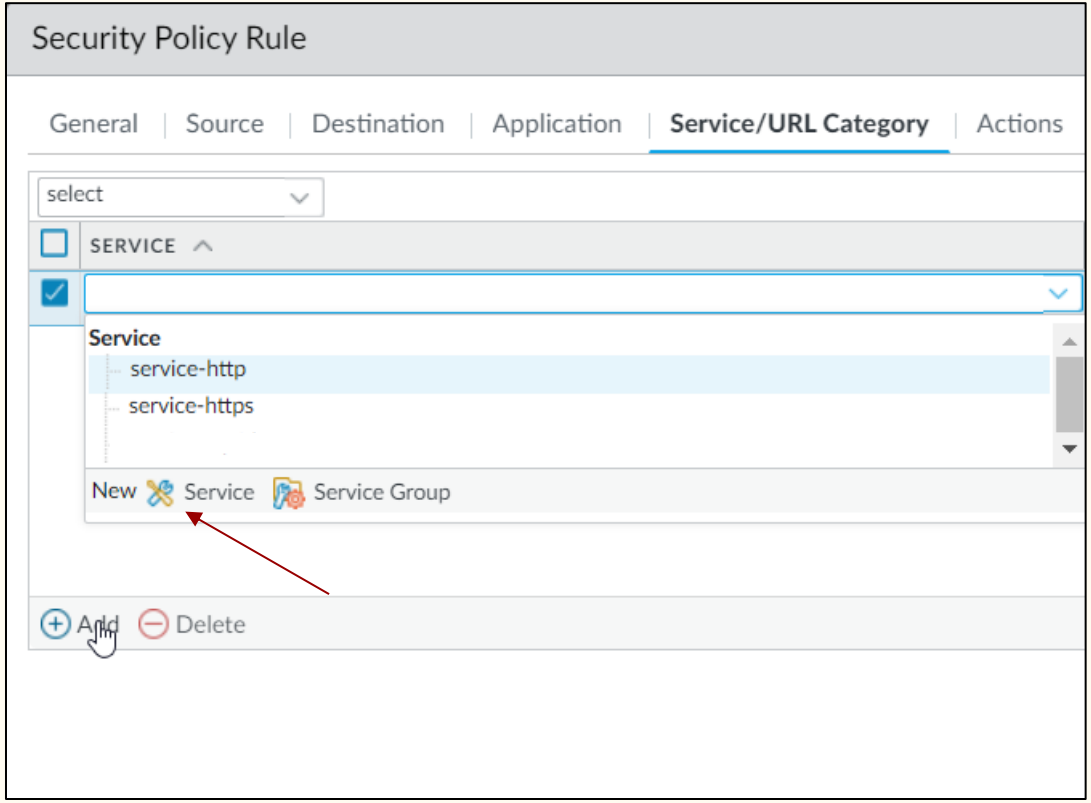
Start the rule by selecting policy and add a new service security policy.



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

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.

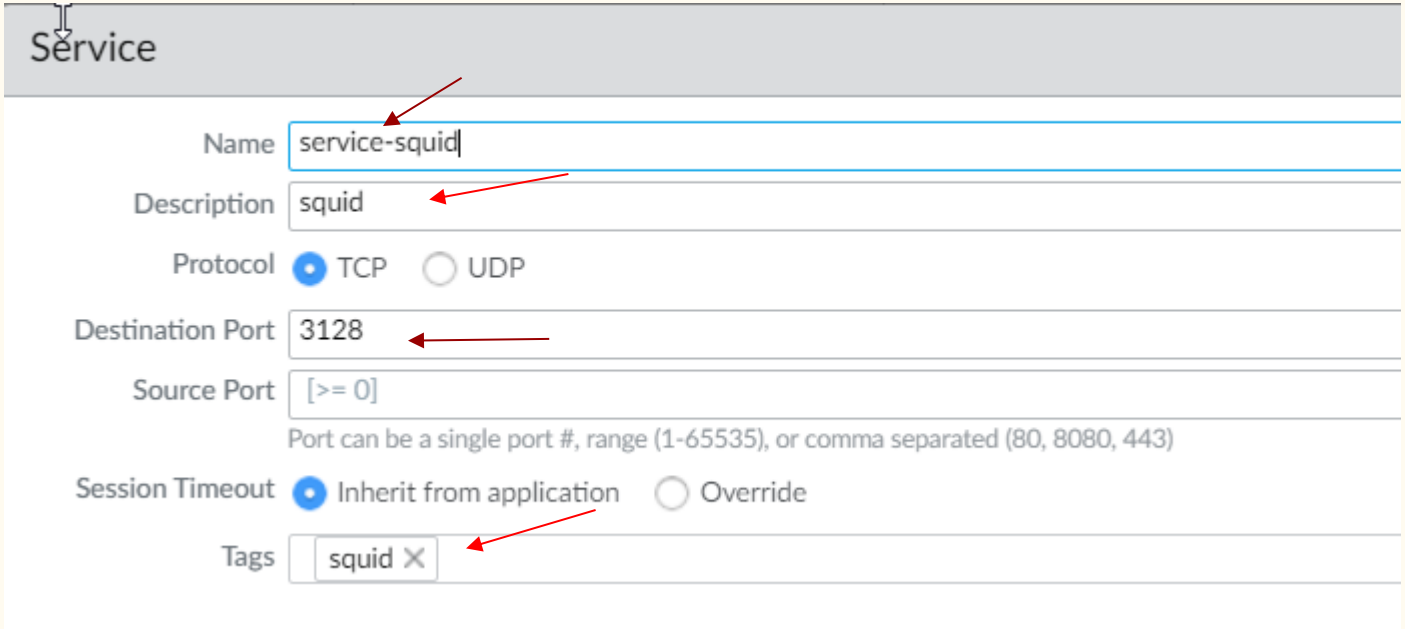
Name the object service- squid.

Under Description insert squid.

Under the Destination port select 3128.

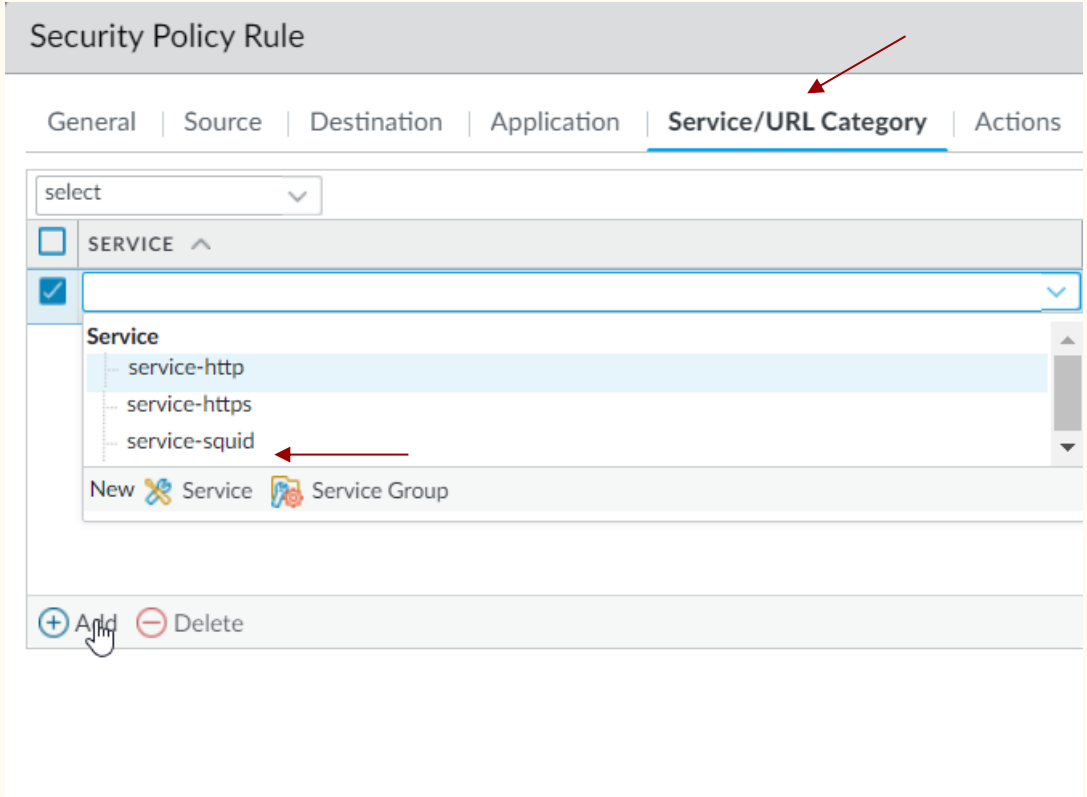
Under Tags enter Squid.

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.



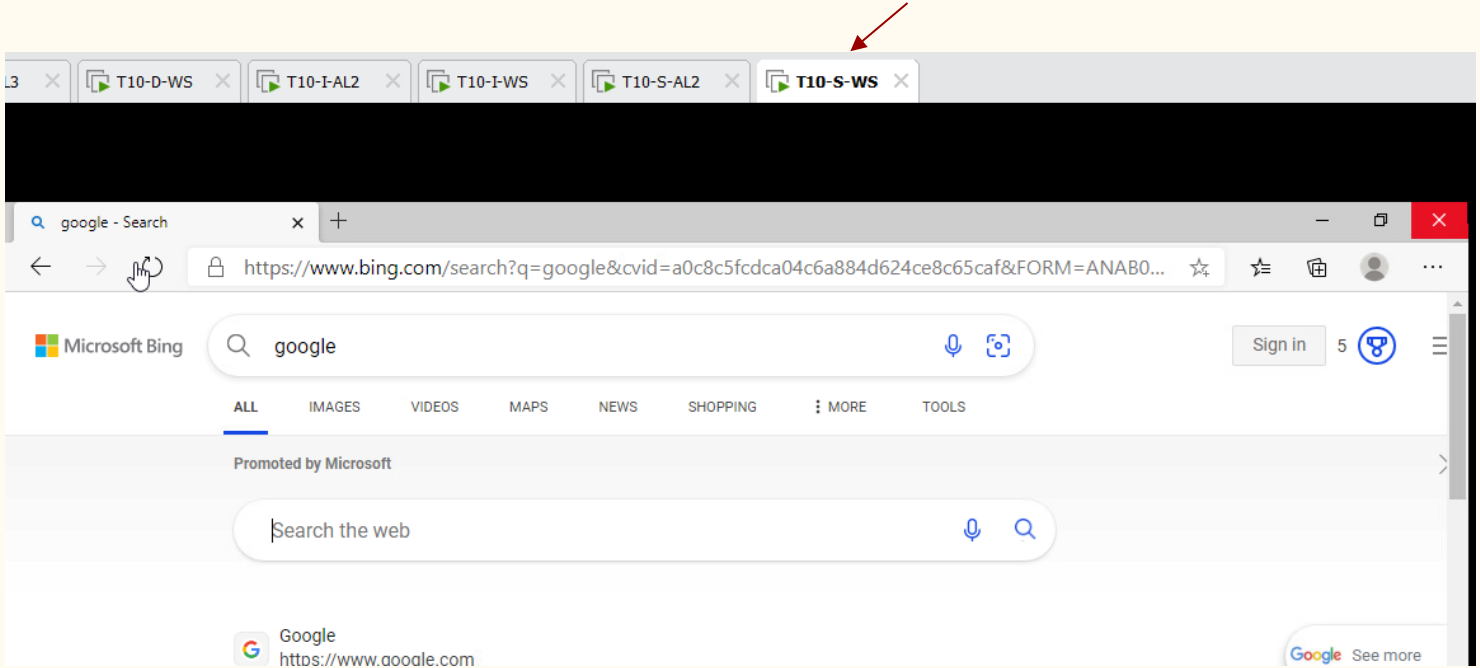
In service/Url Category select service-squid.

Select the new object “service-squid”



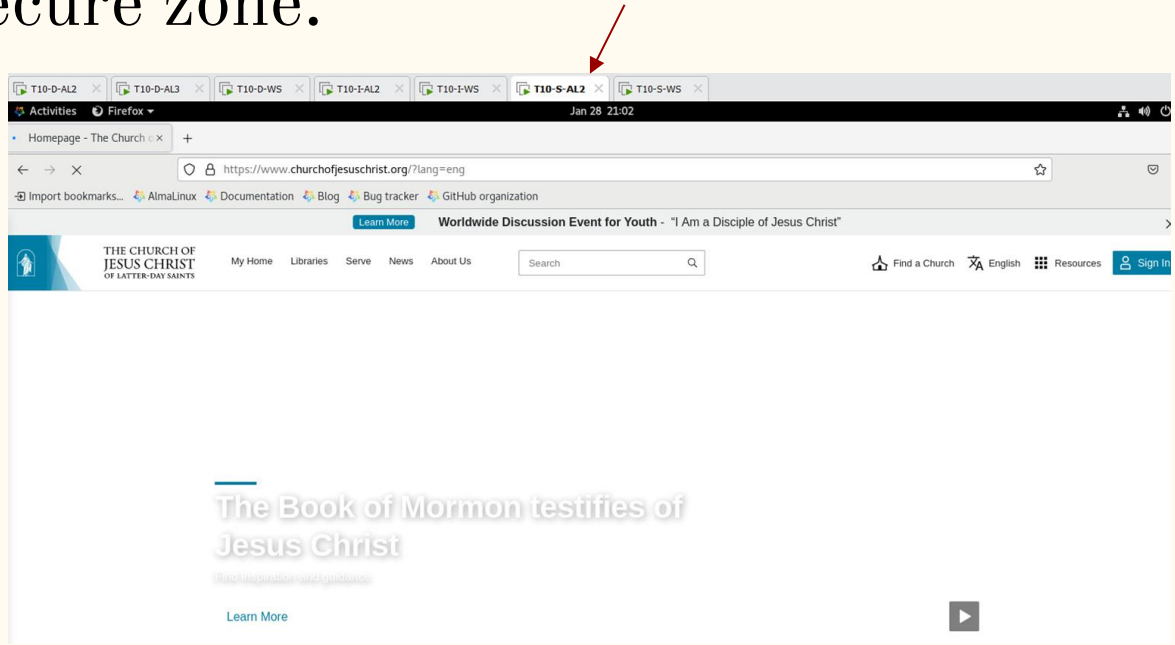
Confirm connectivity in the secure zone Windows system.

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 and object. Neither was difficult it just took a minute to puzzle it out.