

# Acrylic dns and privoxy web proxy services installation and configuration.

---

Carlos Gerez

Acrylic dns.

—

Carlos Gerez

# Acrylic installation on a Windows server.

Use your browser to go to:

<https://sourceforge.net/projects/acrylic/>

This is the download page for Acrylic.

The screenshot shows the SourceForge project page for Acrylic DNS Proxy. The page has a dark theme with orange accents. At the top, there's a navigation bar with 'SOURCEFORGE' and links for 'Open Source Software', 'Business Software', 'Resources', 'For Vendors', 'Help', 'Create', 'Join', and 'Login'. A search bar is on the right. Below the navigation bar, there's a banner for 'BetterComm' PIM and Order Management Software. The main content area features the project title 'Acrylic DNS Proxy' with a description: 'A local DNS proxy which improves the performance of your computer Brought to you by: mayakron'. It shows a star rating of 4.5 (17 Reviews), download statistics (479 This Week), and the last update date (2022-08-06). There are buttons for 'Download', 'Get Updates', and 'Share This'. Below this, there's a tabbed interface with 'Summary', 'Files', 'Reviews', 'Support', and 'CVS'. The 'Summary' tab is active, showing a detailed description of the software's functionality. On the right side, there are several advertisements for other SourceForge projects like 'Inspired Portal' and 'Red Software'.

Home / Browse Open Source / Communications / Acrylic DNS Proxy

## Acrylic DNS Proxy

A local DNS proxy which improves the performance of your computer  
Brought to you by: [mayakron](#)

★★★★★ 17 Reviews Downloads: 479 This Week Last Update: 2022-08-06

[Download](#) [Get Updates](#) [Share This](#)

Windows

Summary	Files	Reviews	Support	CVS
---------	-------	---------	---------	-----

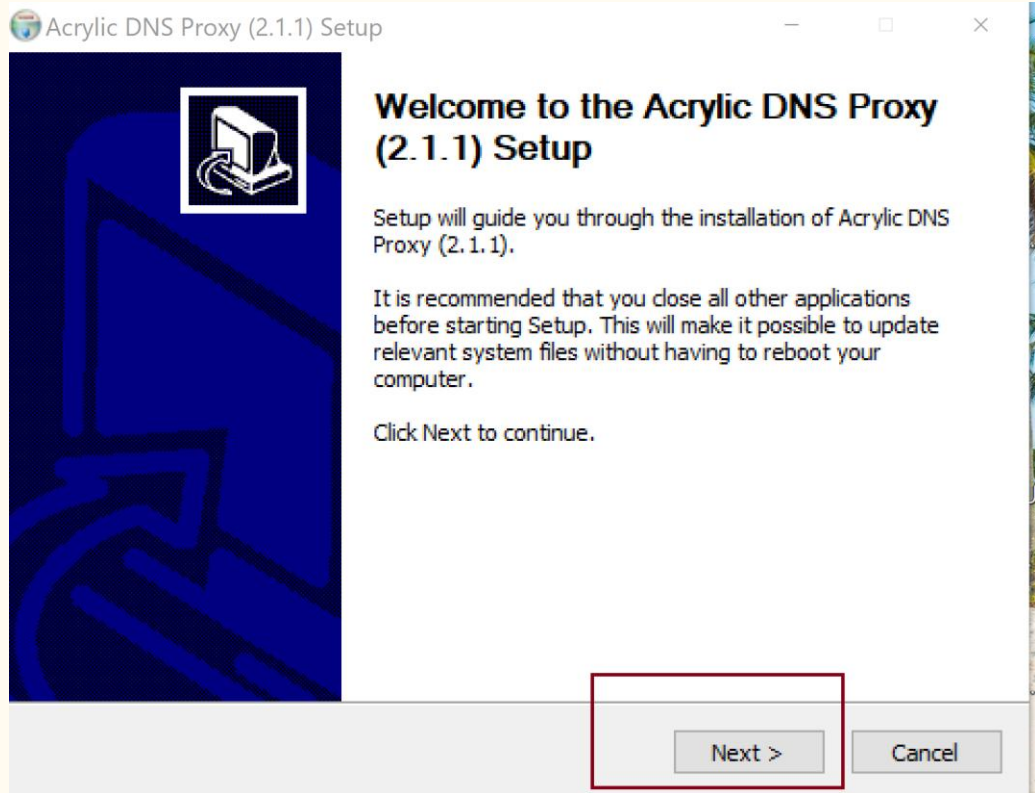
Acrylic is a local DNS proxy for Windows which improves the performance of your computer by caching the responses coming from your DNS servers and helps you fight unwanted ads through the use of a custom HOSTS file (optimized for handling hundreds of thousands of domain names) with support for wildcards and regular expressions.

When you browse a web page a portion of the loading time is dedicated to name resolution while the rest is dedicated to the transfer of the web page contents. What Acrylic does is to reduce the time dedicated to name resolution for frequently visited addresses closest to zero possible. Furthermore Acrylic's sliding expiration caching mechanism and DNS silent updates are able to improve the browsing experience independently of the browser.

[Learn More](#)

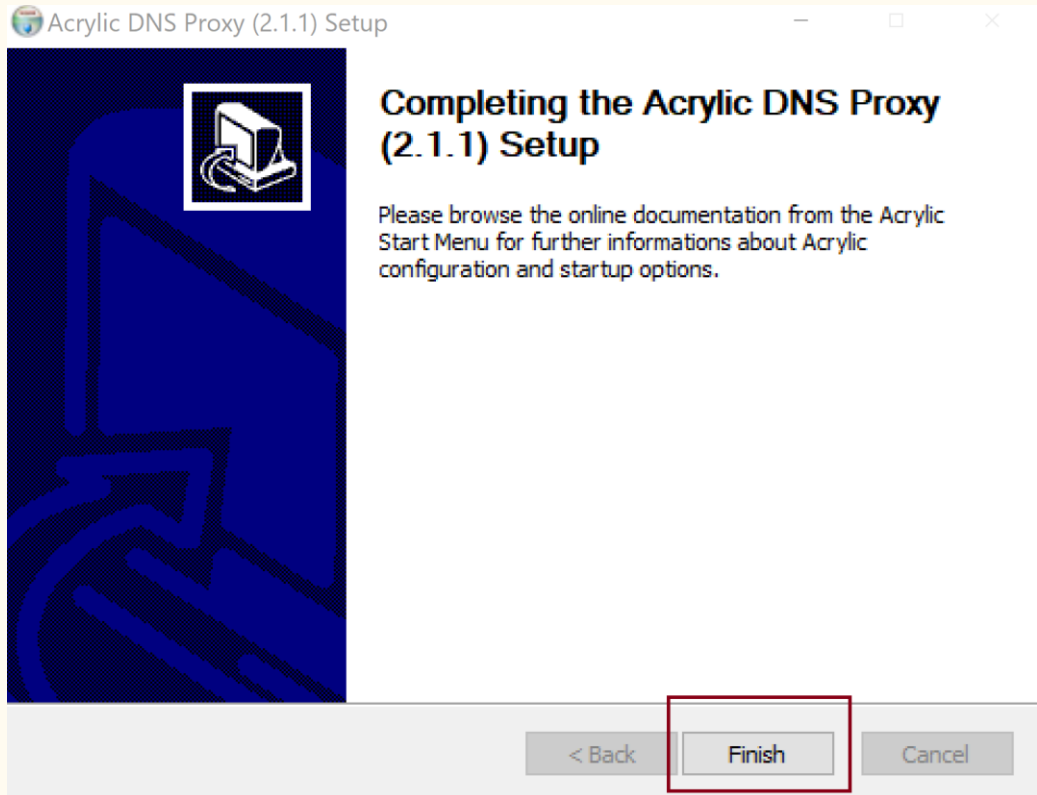
# Acrylic installation on a Windows server.

After download open the installation file and follow the steps.



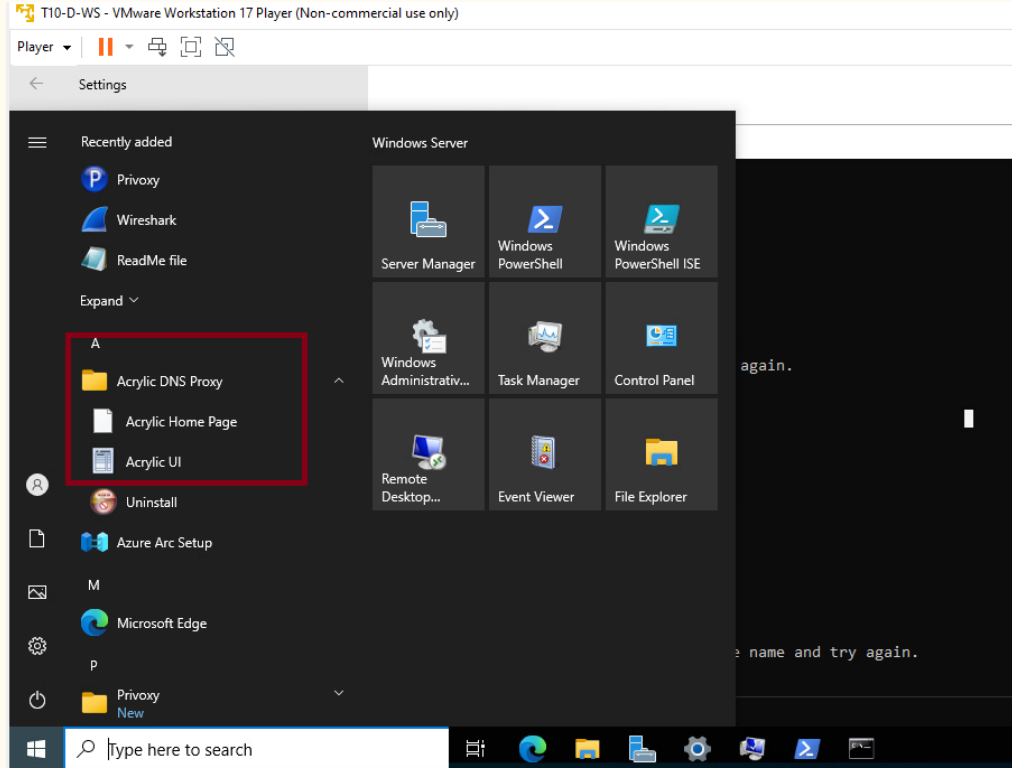
# Acrylic installation on a Windows server.

Use all the default configurations pressing next in each window until finish.



# Acrylic installation on a Windows server.

Upon finishing you will have the app in your app list.



# Acrylic installation on a Windows server.

The new app on your list of apps on windows is called Acrylic UI. Open the app.

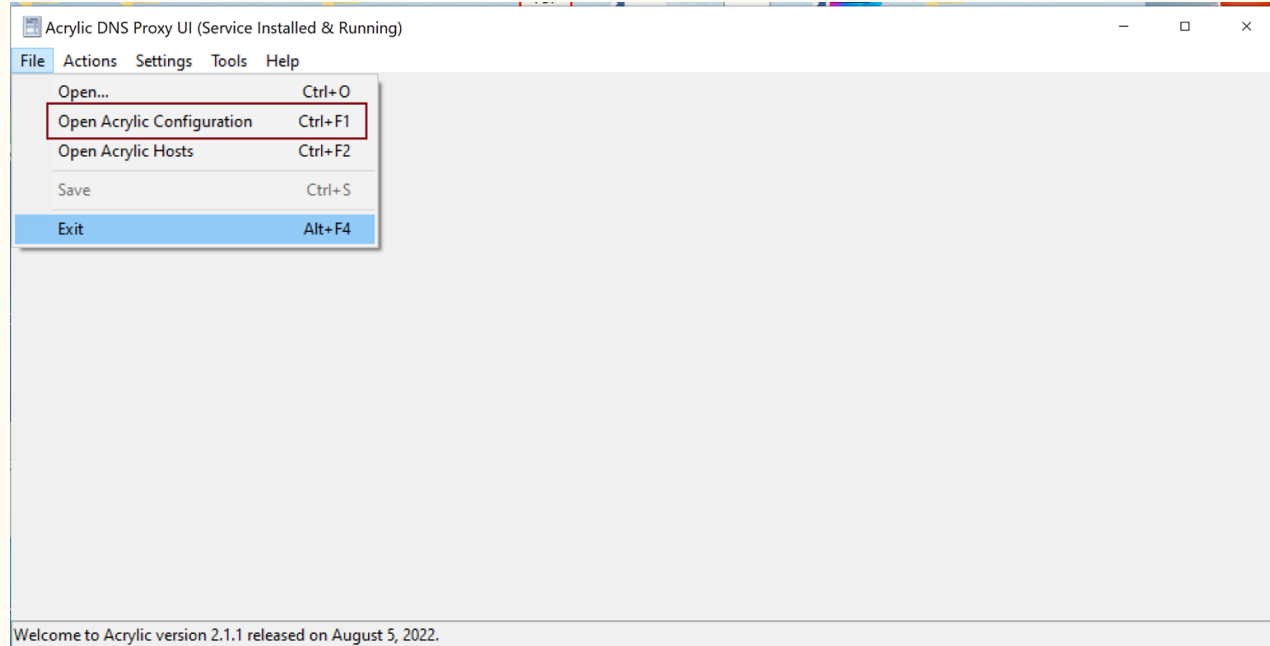


Acrylic UI

ms-resource:appDisplayName  
System

# Acrylic installation on a Windows server.

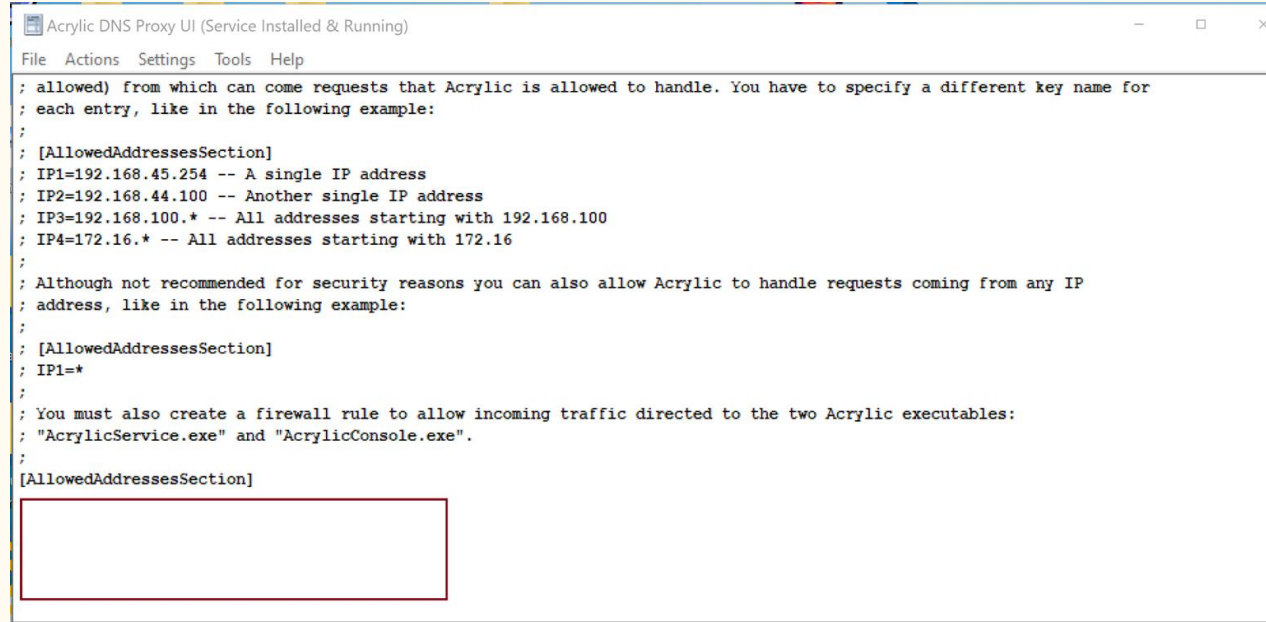
This page is the UI for acrylic. Select file, and open Acrylic Configuration to configure Acrylic on this computer.





# Acrylic installation on a Windows server.

Go to the last line of the file and add under the AllowedAddressSection the ip address from your computer. All the lines that start with ; are commented lines and will not be used by the app.

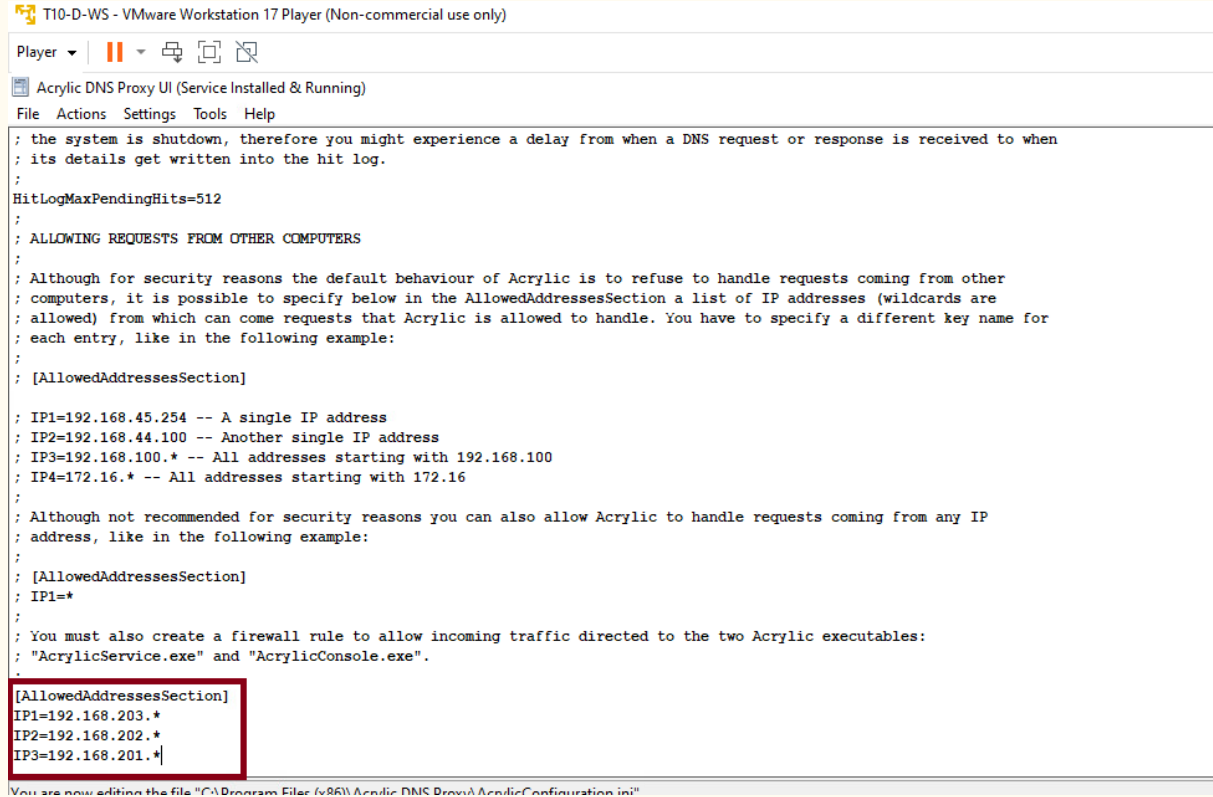


```
Acrylic DNS Proxy UI (Service Installed & Running)
File Actions Settings Tools Help

; allowed) from which can come requests that Acrylic is allowed to handle. You have to specify a different key name for
; each entry, like in the following example:
;
; [AllowedAddressesSection]
; IP1=192.168.45.254 -- A single IP address
; IP2=192.168.44.100 -- Another single IP address
; IP3=192.168.100.* -- All addresses starting with 192.168.100
; IP4=172.16.* -- All addresses starting with 172.16
;
; Although not recommended for security reasons you can also allow Acrylic to handle requests coming from any IP
; address, like in the following example:
;
; [AllowedAddressesSection]
; IP1=*
;
; You must also create a firewall rule to allow incoming traffic directed to the two Acrylic executables:
; "AcrylicService.exe" and "AcrylicConsole.exe".
;
[AllowedAddressesSection]
```

# Acrylic installation on a Windows server.

Go to the last line of the file and add under the AllowedAddressSection the ip address that you will allow to receive requests from, in this case the \* means all the machines on that subnet.



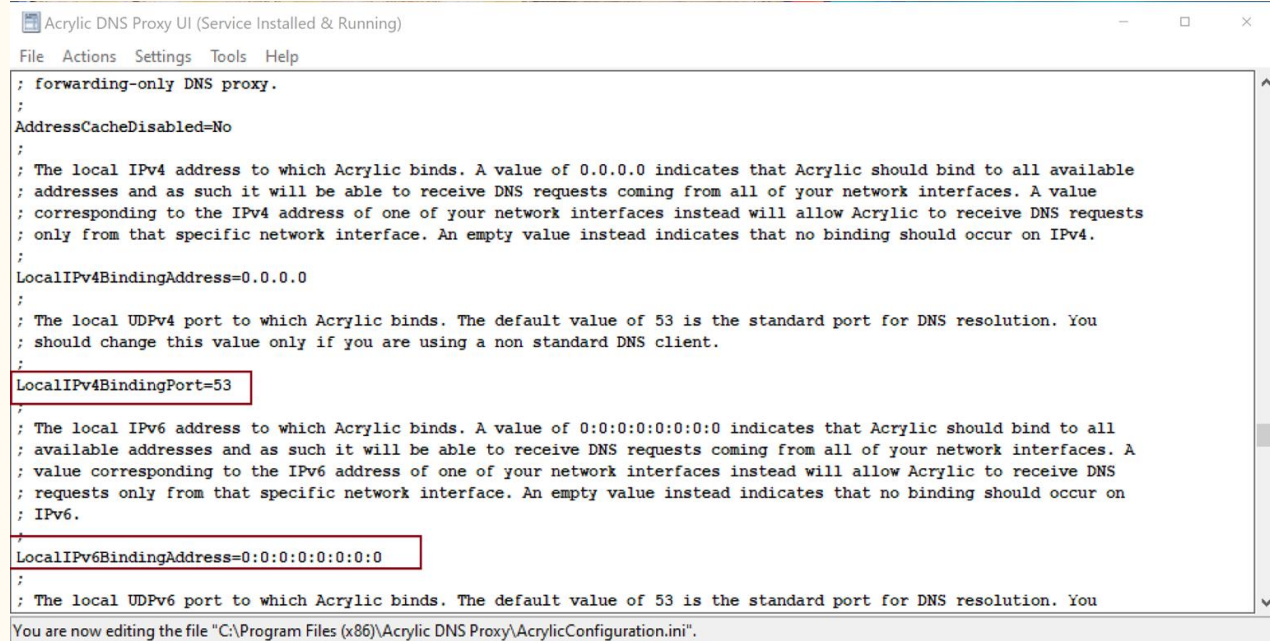
The screenshot shows a VMware Workstation 17 Player window titled "T10-D-WS - VMware Workstation 17 Player (Non-commercial use only)". Inside the player, the "Acrylic DNS Proxy UI (Service Installed & Running)" application is open. The application has a menu bar with "File", "Actions", "Settings", "Tools", and "Help". The main window displays the configuration file "AcrylicConfiguration.ini". The file content is as follows:

```
; the system is shutdown, therefore you might experience a delay from when a DNS request or response is received to when  
; its details get written into the hit log.  
;  
HitLogMaxPendingHits=512  
;  
; ALLOWING REQUESTS FROM OTHER COMPUTERS  
;  
; Although for security reasons the default behaviour of Acrylic is to refuse to handle requests coming from other  
; computers, it is possible to specify below in the AllowedAddressesSection a list of IP addresses (wildcards are  
; allowed) from which can come requests that Acrylic is allowed to handle. You have to specify a different key name for  
; each entry, like in the following example:  
;  
; [AllowedAddressesSection]  
;  
; IP1=192.168.45.254 -- A single IP address  
; IP2=192.168.44.100 -- Another single IP address  
; IP3=192.168.100.* -- All addresses starting with 192.168.100  
; IP4=172.16.* -- All addresses starting with 172.16  
;  
; Although not recommended for security reasons you can also allow Acrylic to handle requests coming from any IP  
; address, like in the following example:  
;  
; [AllowedAddressesSection]  
; IP1=*  
;  
; You must also create a firewall rule to allow incoming traffic directed to the two Acrylic executables:  
; "AcrylicService.exe" and "AcrylicConsole.exe".  
;  
[AllowedAddressesSection]  
IP1=192.168.203.*  
IP2=192.168.202.*  
IP3=192.168.201.*
```

The last three lines of the configuration file are highlighted with a red box. At the bottom of the window, a status bar indicates: "You are now editing the file 'C:\Program Files (x86)\Acrylic DNS Proxy\AcrylicConfiguration.ini'".

# Acrylic installation on a Windows server.

There are several other configurations lines in this file that is good to know. In the LocalIPv4BindingPort, the number 53 means that is the port used by this application.

The screenshot shows a window titled "Acrylic DNS Proxy UI (Service Installed & Running)". It has a menu bar with "File", "Actions", "Settings", "Tools", and "Help". The main area displays the contents of the "AcrylicConfiguration.ini" file. The file is a text-based configuration file with several settings. Two settings are highlighted with red boxes: "LocalIPv4BindingPort=53" and "LocalIPv6BindingAddress=0:0:0:0:0:0:0:0". The status bar at the bottom indicates the file path: "You are now editing the file \"C:\\Program Files (x86)\\Acrylic DNS Proxy\\AcrylicConfiguration.ini\"."

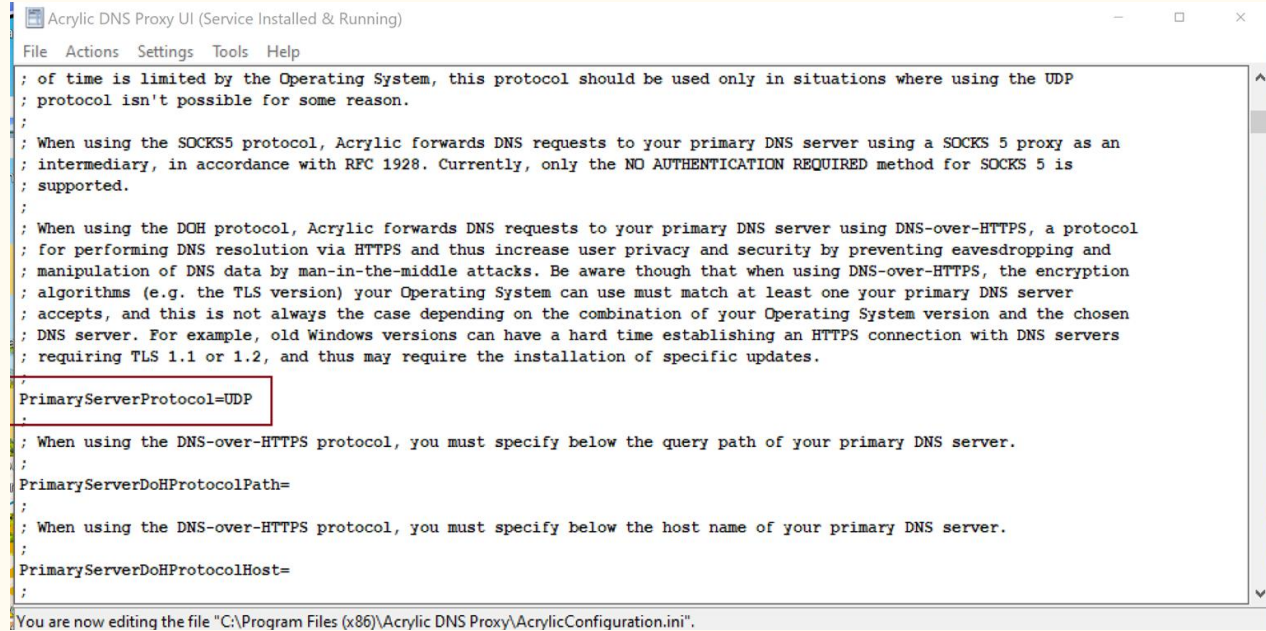
```
; forwarding-only DNS proxy.
;
AddressCacheDisabled=No
;
; The local IPv4 address to which Acrylic binds. A value of 0.0.0.0 indicates that Acrylic should bind to all available
; addresses and as such it will be able to receive DNS requests coming from all of your network interfaces. A value
; corresponding to the IPv4 address of one of your network interfaces instead will allow Acrylic to receive DNS requests
; only from that specific network interface. An empty value instead indicates that no binding should occur on IPv4.
;
LocalIPv4BindingAddress=0.0.0.0
;
; The local UDPv4 port to which Acrylic binds. The default value of 53 is the standard port for DNS resolution. You
; should change this value only if you are using a non standard DNS client.
;
LocalIPv4BindingPort=53
;
; The local IPv6 address to which Acrylic binds. A value of 0:0:0:0:0:0:0:0 indicates that Acrylic should bind to all
; available addresses and as such it will be able to receive DNS requests coming from all of your network interfaces. A
; value corresponding to the IPv6 address of one of your network interfaces instead will allow Acrylic to receive DNS
; requests only from that specific network interface. An empty value instead indicates that no binding should occur on
; IPv6.
;
LocalIPv6BindingAddress=0:0:0:0:0:0:0:0
;
; The local UDPv6 port to which Acrylic binds. The default value of 53 is the standard port for DNS resolution. You
```

You are now editing the file "C:\Program Files (x86)\Acrylic DNS Proxy\AcrylicConfiguration.ini".

# Acrylic installation on a Windows server.

Primary protocol used in default is UDP.

There are more allowed protocol listed in the file in the previous lines.



The screenshot shows a window titled "Acrylic DNS Proxy UI (Service Installed & Running)". The window contains a text editor with the following content:

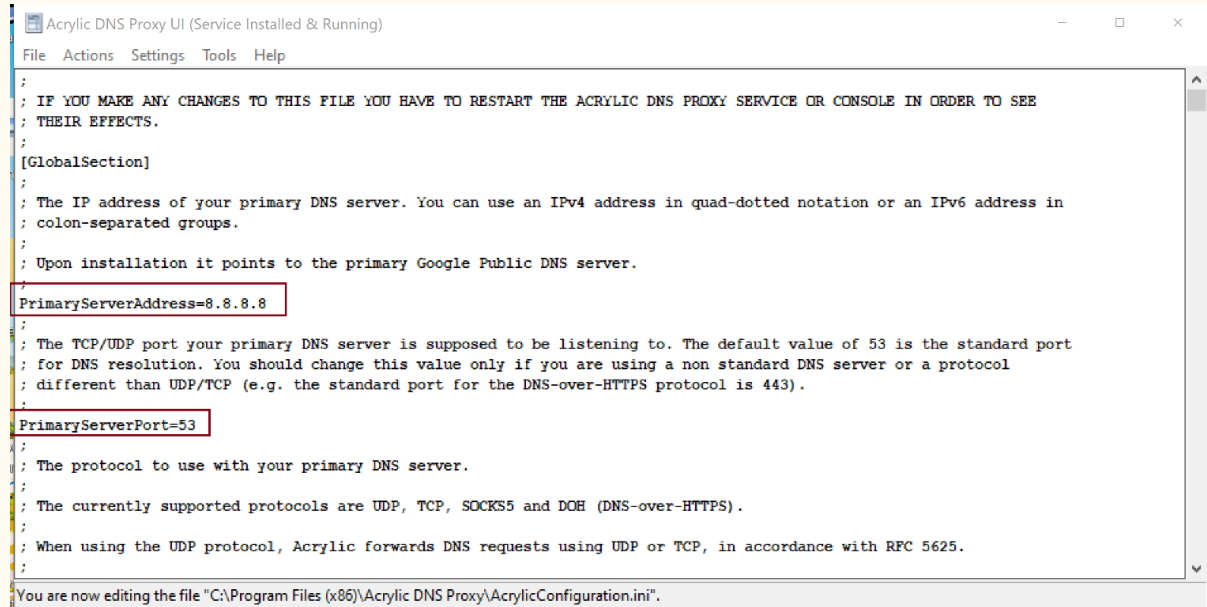
```
File Actions Settings Tools Help

; of time is limited by the Operating System, this protocol should be used only in situations where using the UDP
; protocol isn't possible for some reason.
;
; When using the SOCKS5 protocol, Acrylic forwards DNS requests to your primary DNS server using a SOCKS 5 proxy as an
; intermediary, in accordance with RFC 1928. Currently, only the NO AUTHENTICATION REQUIRED method for SOCKS 5 is
; supported.
;
; When using the DOH protocol, Acrylic forwards DNS requests to your primary DNS server using DNS-over-HTTPS, a protocol
; for performing DNS resolution via HTTPS and thus increase user privacy and security by preventing eavesdropping and
; manipulation of DNS data by man-in-the-middle attacks. Be aware though that when using DNS-over-HTTPS, the encryption
; algorithms (e.g. the TLS version) your Operating System can use must match at least one your primary DNS server
; accepts, and this is not always the case depending on the combination of your Operating System version and the chosen
; DNS server. For example, old Windows versions can have a hard time establishing an HTTPS connection with DNS servers
; requiring TLS 1.1 or 1.2, and thus may require the installation of specific updates.
;
PrimaryServerProtocol=UDP
;
; When using the DNS-over-HTTPS protocol, you must specify below the query path of your primary DNS server.
;
PrimaryServerDoHProtocolPath=
;
; When using the DNS-over-HTTPS protocol, you must specify below the host name of your primary DNS server.
;
PrimaryServerDoHProtocolHost=
;

You are now editing the file "C:\Program Files (x86)\Acrylic DNS Proxy\AcrylicConfiguration.ini".
```

# Acrylic installation on a Windows server.

Here is defined the primary server that resolve the addresses, and the primary server port.



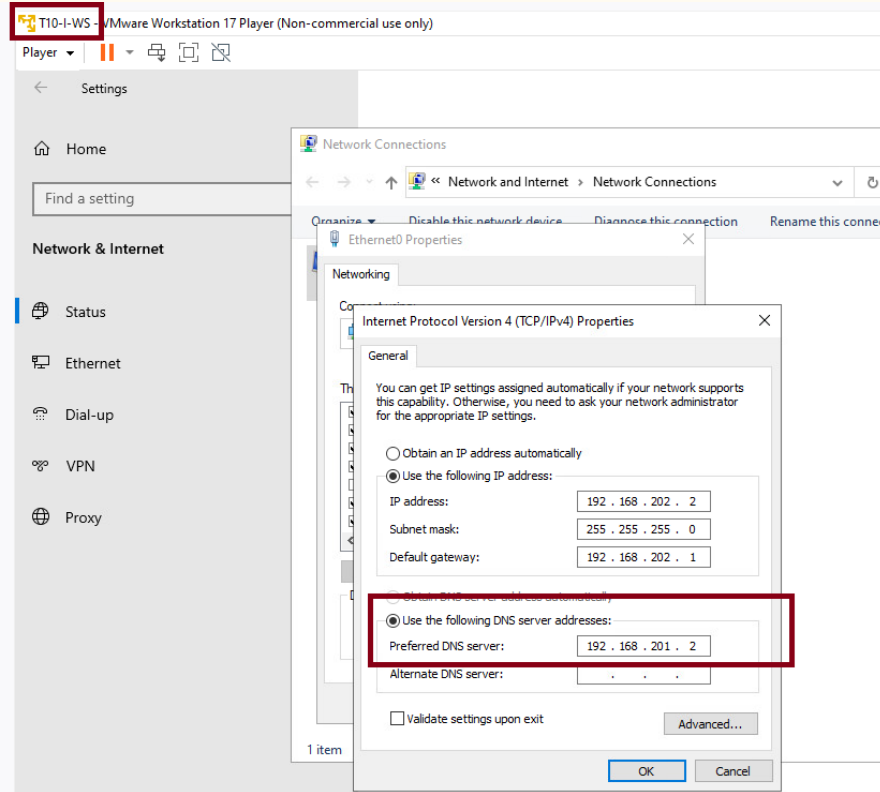
```
Acrylic DNS Proxy UI (Service Installed & Running)
File Actions Settings Tools Help

;
; IF YOU MAKE ANY CHANGES TO THIS FILE YOU HAVE TO RESTART THE ACRYLIC DNS PROXY SERVICE OR CONSOLE IN ORDER TO SEE
; THEIR EFFECTS.
;
[GlobalSection]
;
; The IP address of your primary DNS server. You can use an IPv4 address in quad-dotted notation or an IPv6 address in
; colon-separated groups.
;
; Upon installation it points to the primary Google Public DNS server.
PrimaryServerAddress=8.8.8.8
;
; The TCP/UDP port your primary DNS server is supposed to be listening to. The default value of 53 is the standard port
; for DNS resolution. You should change this value only if you are using a non standard DNS server or a protocol
; different than UDP/TCP (e.g. the standard port for the DNS-over-HTTPS protocol is 443).
PrimaryServerPort=53
;
; The protocol to use with your primary DNS server.
;
; The currently supported protocols are UDP, TCP, SOCKS5 and DOH (DNS-over-HTTPS).
;
; When using the UDP protocol, Acrylic forwards DNS requests using UDP or TCP, in accordance with RFC 5625.
;

You are now editing the file "C:\Program Files (x86)\Acrylic DNS Proxy\AcrylicConfiguration.ini".
```

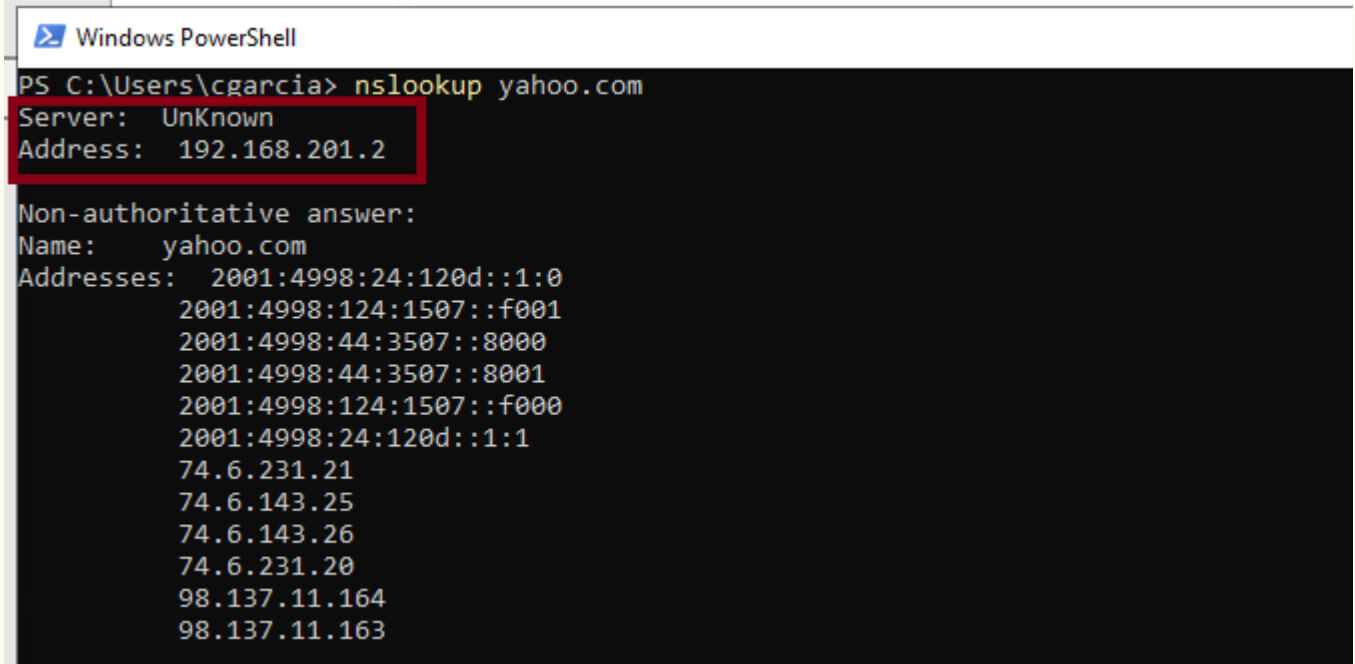
# Using the dns service from a computer in the intern zone.

Here we change the dns on a machine to get their dns from the machine in the DMZ.



# Testing the dns service resolution.

On a windows powershell we can use nslookup to resolve yahoo.com and receive the addresses of servers linked to that domain. In the top is the server that resolve those addresses on the DMZ.



```
Windows PowerShell
PS C:\Users\cgarcia> nslookup 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
```

# privoxy web proxy services installation and configuration.

---

Carlos Gerez

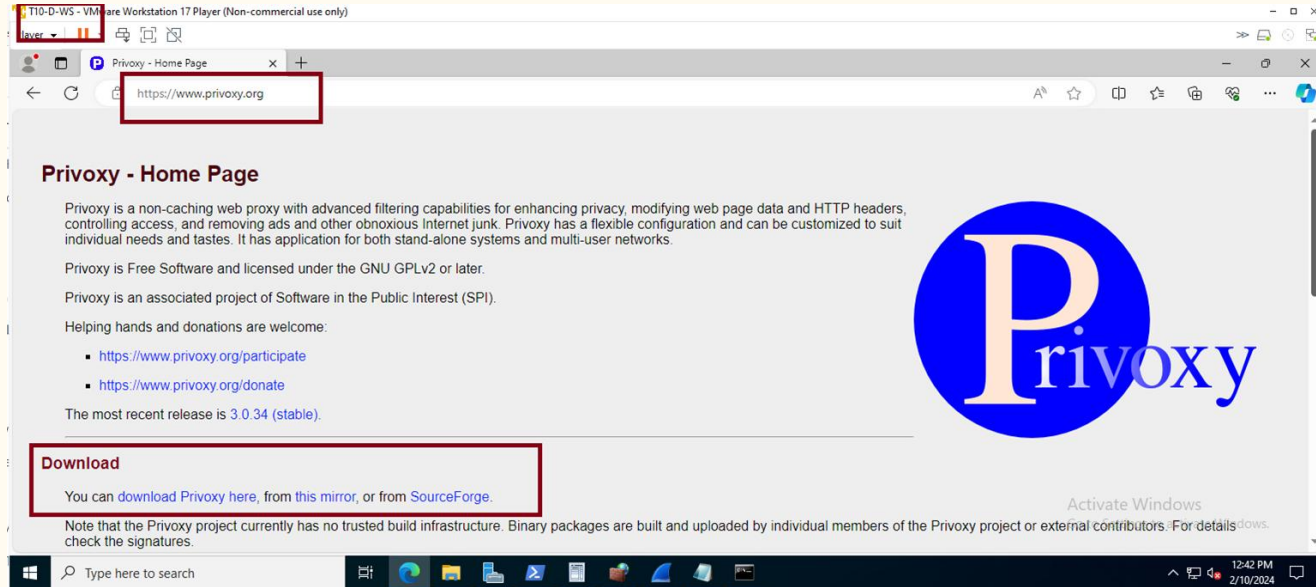


# Privoxy installation in a Windows server.

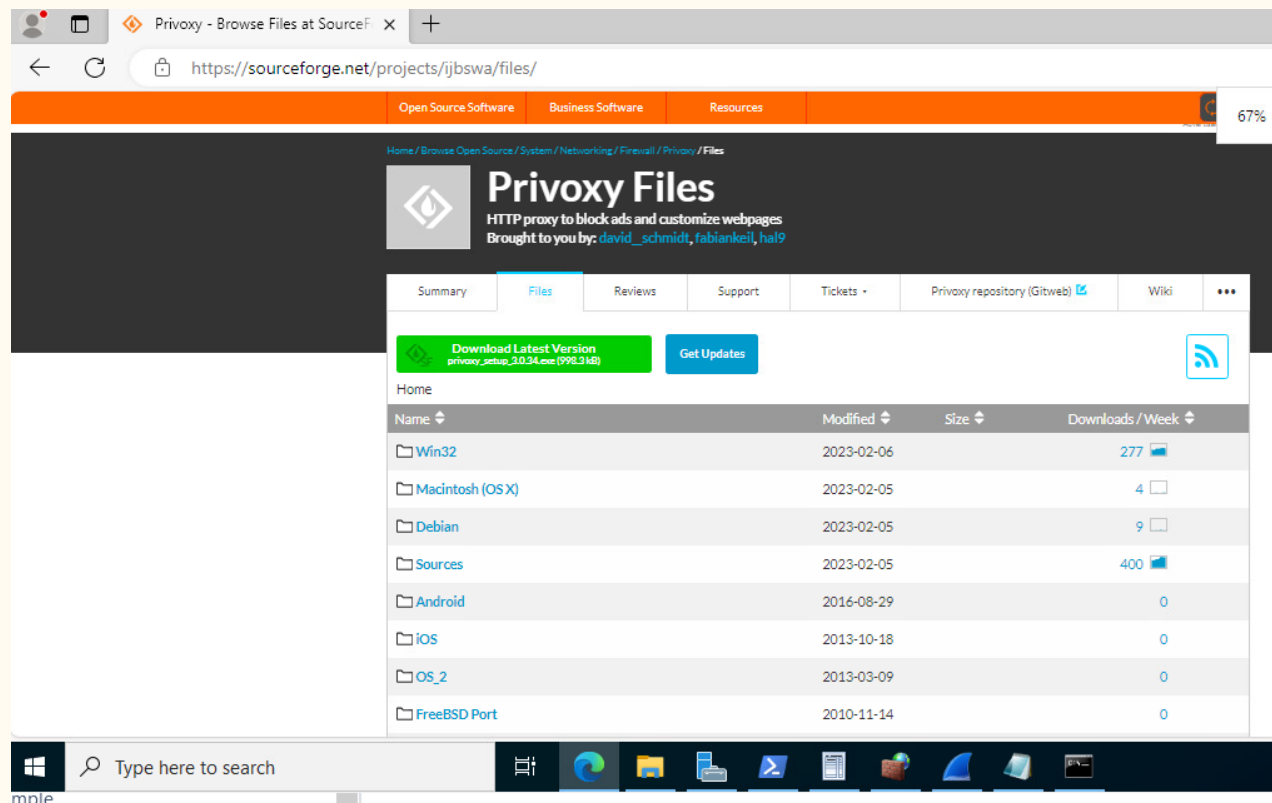
On a browser on the computer in that you want to install the service search for

<http://www.privoxy.org/>

Select download from SourceForge.



# Privoxy installation in a Windows server.



The screenshot shows a web browser window displaying the SourceForge page for Privoxy Files. The browser's address bar shows the URL <https://sourceforge.net/projects/ijbswa/files/>. The page has an orange navigation bar with links for Open Source Software, Business Software, and Resources. Below this, the page title is "Privoxy Files" with a subtitle "HTTP proxy to block ads and customize webpages" and credits "Brought to you by: david\_schmidt, fabiankeil, hal9". The page is divided into tabs: Summary, Files (selected), Reviews, Support, Tickets, and a link to the Privoxy repository on Gitweb. A green button labeled "Download Latest Version" (privoxy\_setup\_3.0.34.exe (998.3 kB)) and a blue "Get Updates" button are visible. Below the buttons is a table listing various operating system and platform folders.

Name	Modified	Size	Downloads / Week
Win32	2023-02-06		277
Macintosh (OS X)	2023-02-05		4
Debian	2023-02-05		9
Sources	2023-02-05		400
Android	2016-08-29		0
iOS	2013-10-18		0
OS_2	2013-03-09		0
FreeBSD Port	2010-11-14		0

# Privoxy installation in a Windows server.

https://sourceforge.net/projects/ijbswa/files/Win32/

Open Source Software Business Software Resources

Boberdoo Learn More

Home / Browse Open Source / System / Networking / Firewall / Privoxy / Files

## Privoxy Files

HTTP proxy to block ads and customize webpages  
Brought to you by: david\_schmidt, fabiankeil, hal9

Summary Files Reviews Support Tickets + Privacy repository (Gitweb) Wiki

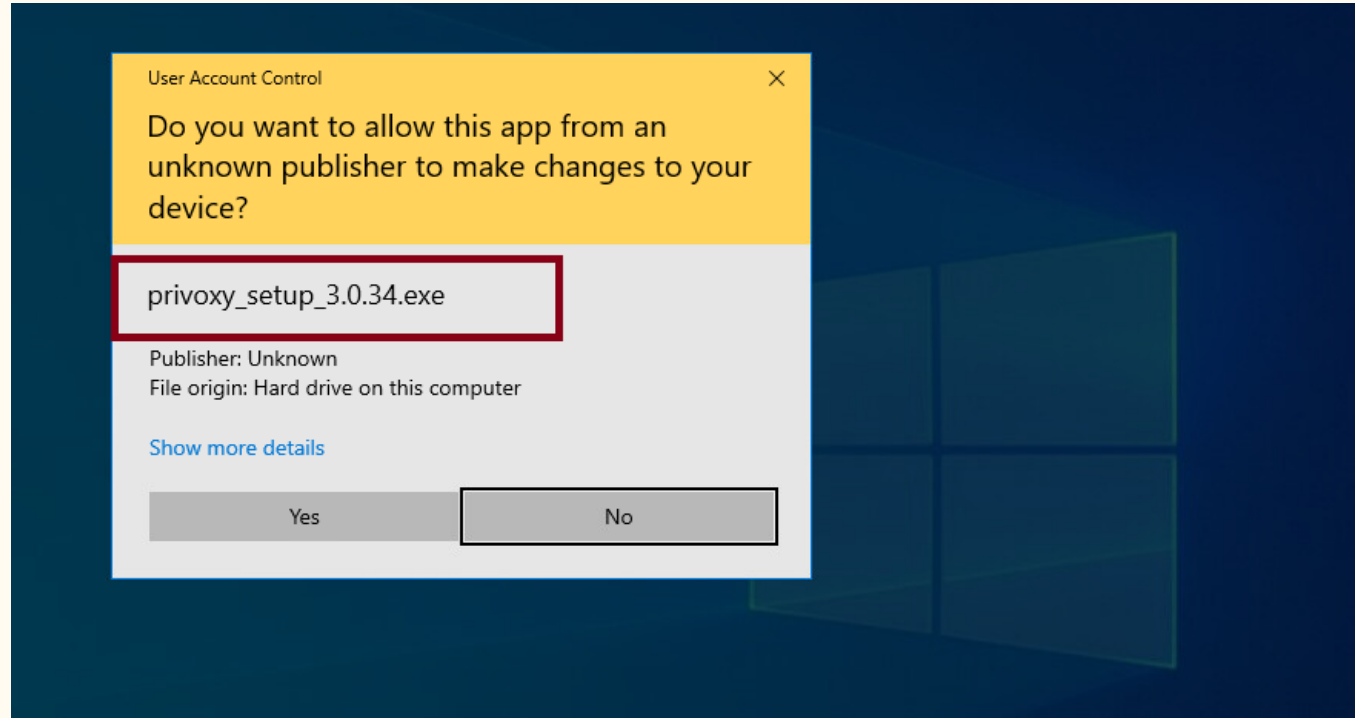
**Download Latest Version**  
privoxy\_setup\_3.0.34.exe (998.3 kB)

Get Updates

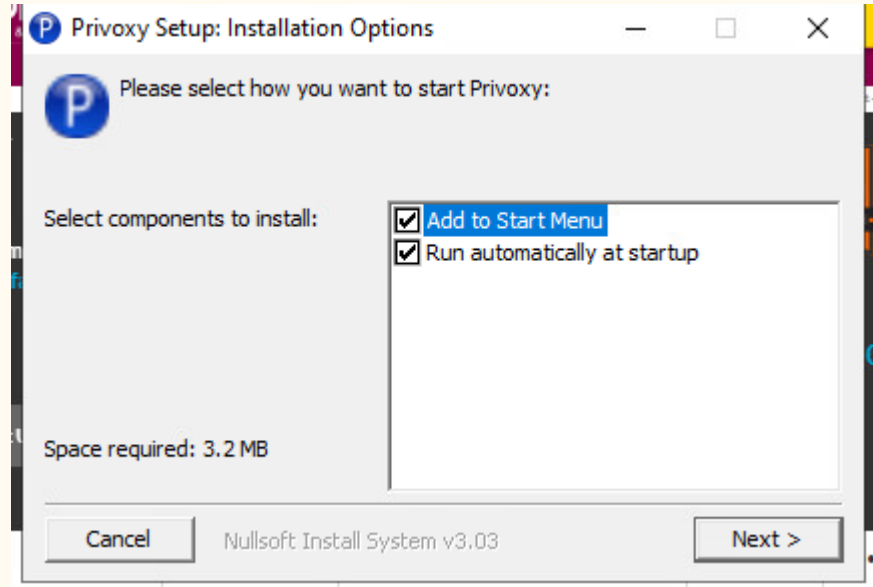
Home / Win32

Name	Modified	Size	Downloads / Week
Parent folder			
3.0.34 (stable)	2023-02-06		273
3.0.33 (stable)	2021-12-08		0
3.0.32 (stable)	2021-02-27		0
3.0.31 (stable)	2021-01-31		0
3.0.29 (stable)	2020-11-29		0
3.0.28 (stable)	2018-12-31		0

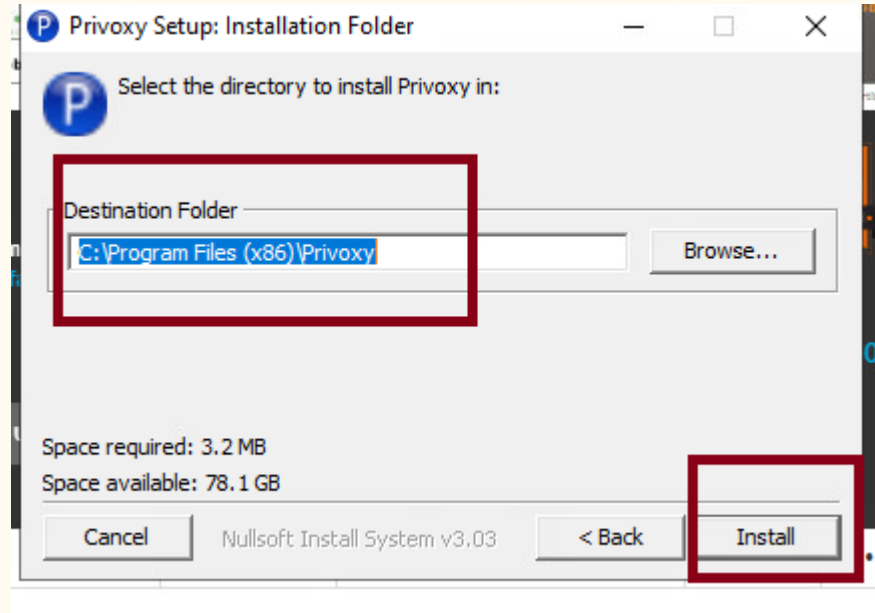
# Privoxy installation in a Windows server.



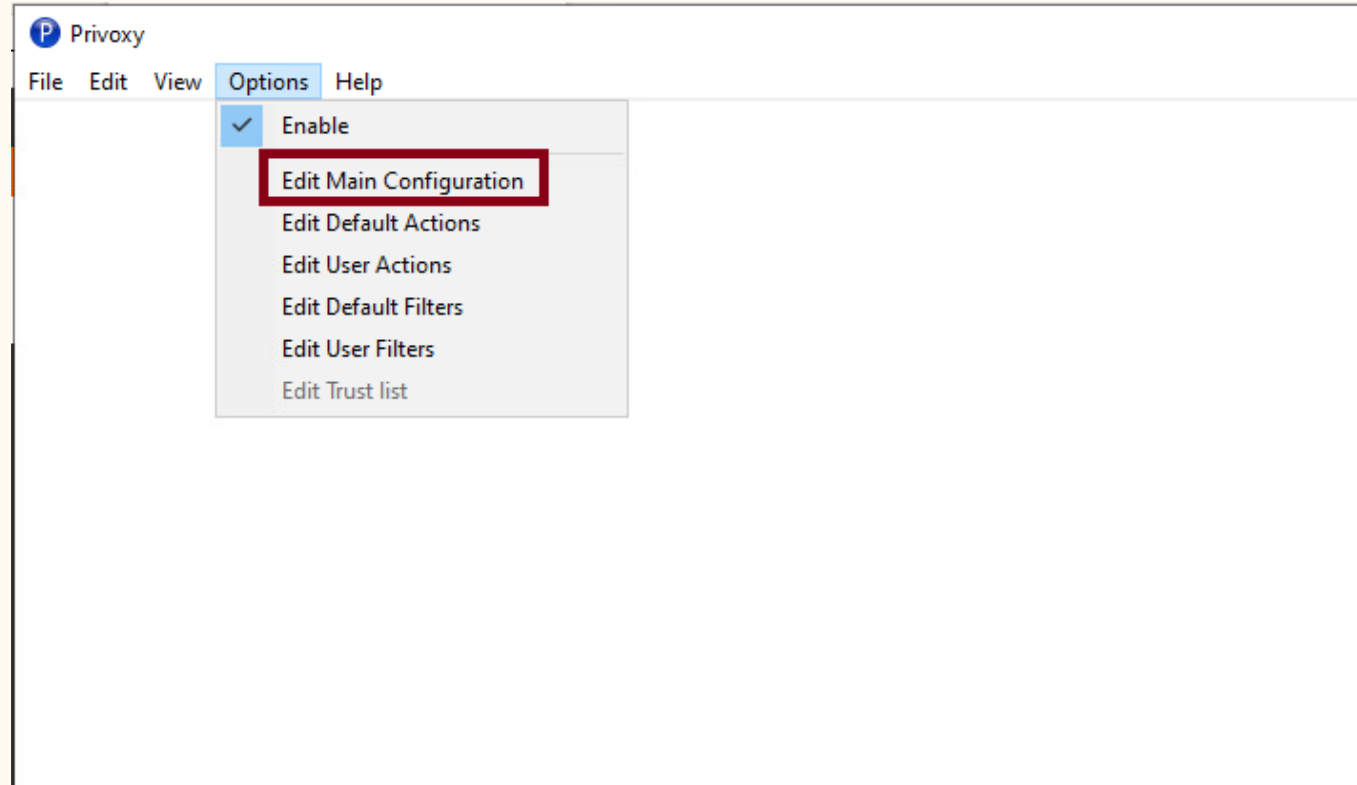
# Privoxy installation in a Windows server.



# Privoxy installation in a Windows server.

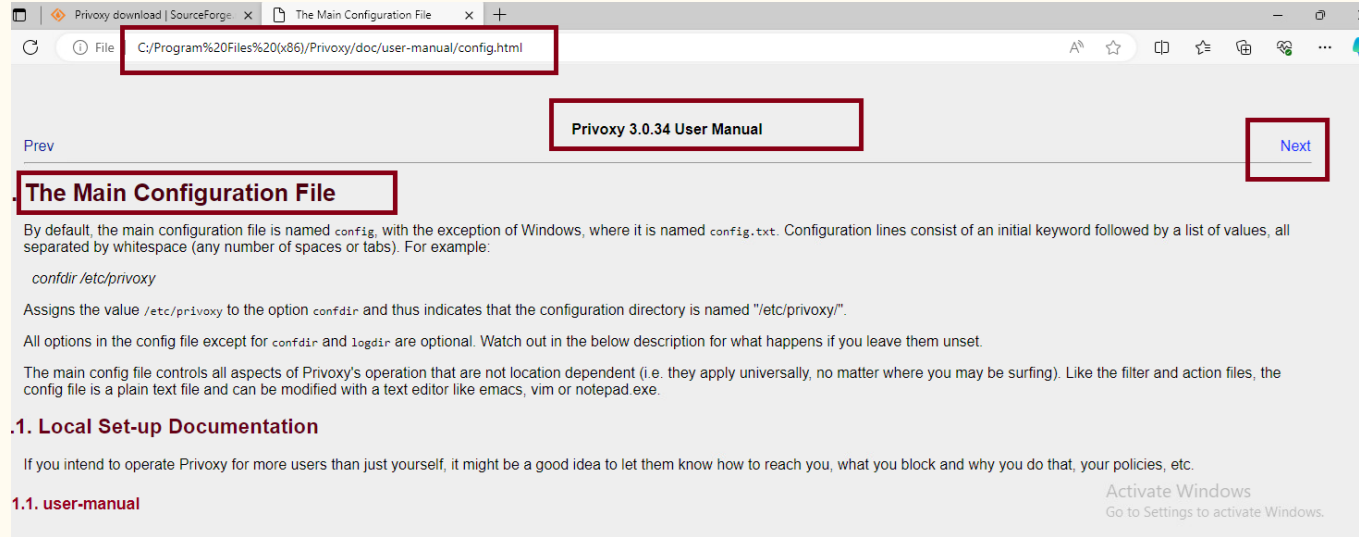


# Privoxy configuration in a Windows server.



# Privoxy configuration in a Windows server.

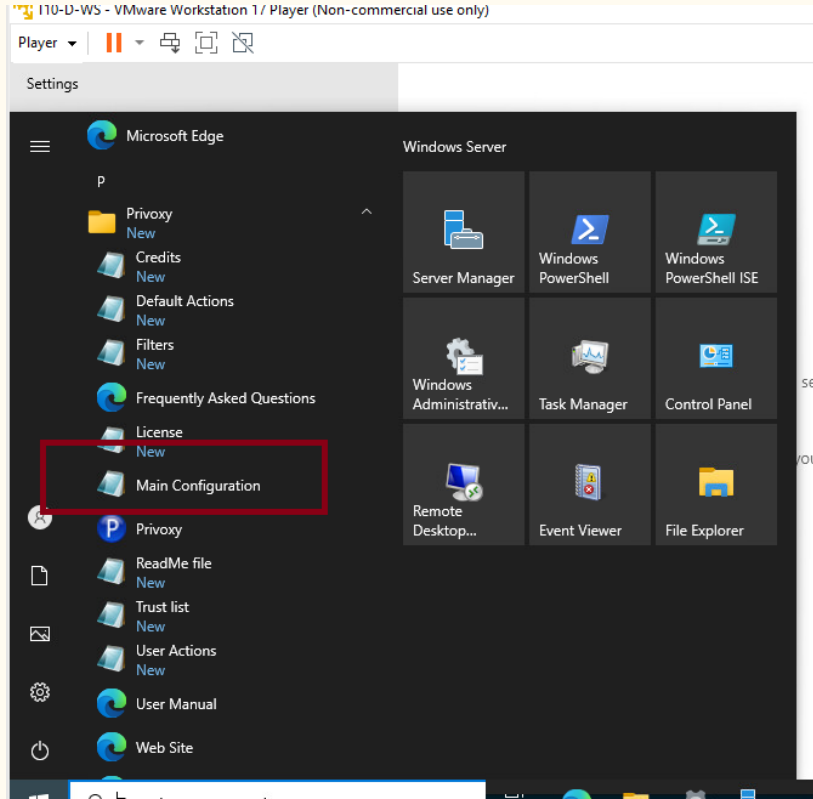
Upon open the app one can look in the web page the configuration options.





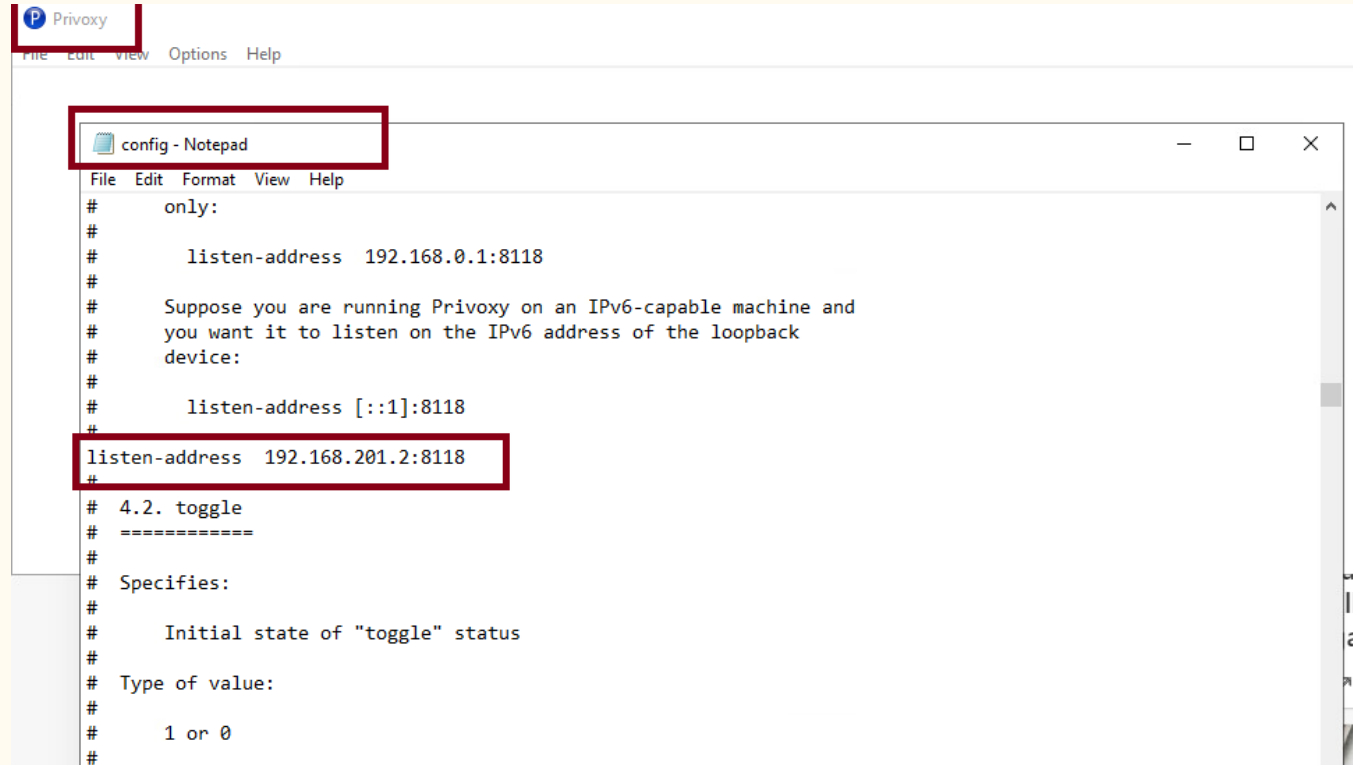
# Privoxy configuration in a Windows server.

A more simple option is to open the main configuration file with administrative privileges, and edit the necessary configurations.



# Privoxy configuration in a Windows server.

This is the only change necessary to provide web services with privoxy. In the uncommented line `listen-address` add the address of the computer where the service runs, and the listening port used for privoxy (8118)

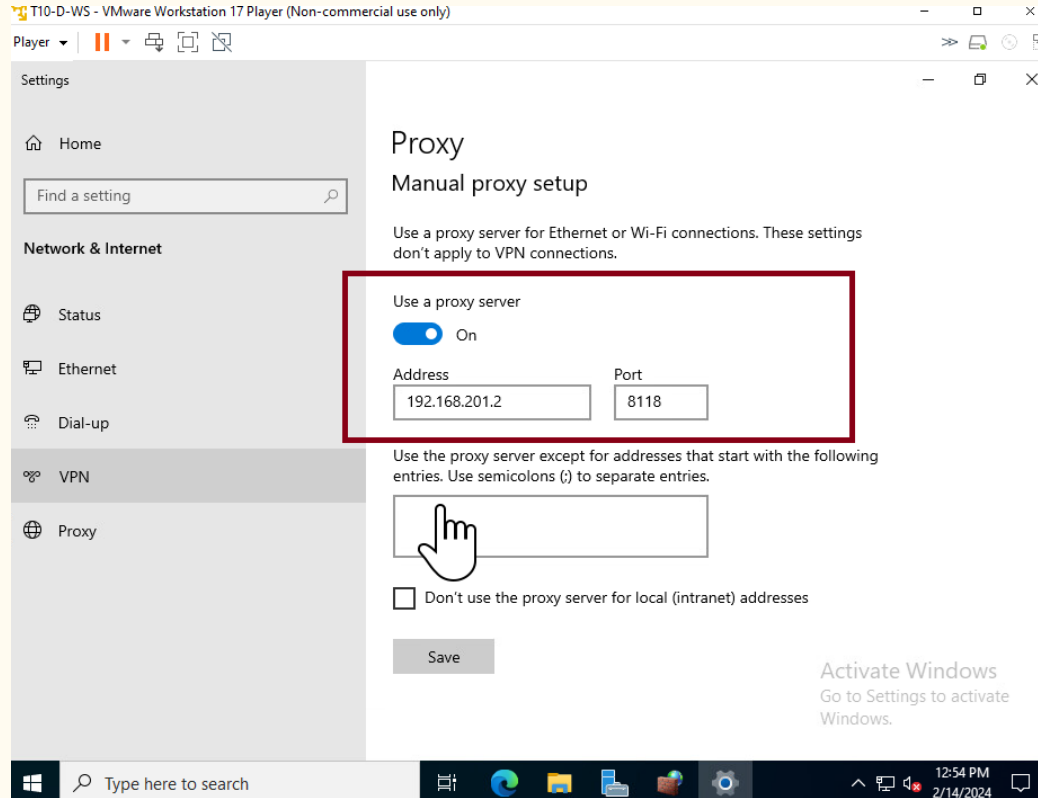


```
Privoxy
File Edit View Options Help

config - Notepad
File Edit Format View Help
# only:
#
#   listen-address 192.168.0.1:8118
#
#   Suppose you are running Privoxy on an IPv6-capable machine and
#   you want it to listen on the IPv6 address of the loopback
#   device:
#
#   listen-address [::1]:8118
#
#   listen-address 192.168.201.2:8118
#
# 4.2. toggle
# =====
# Specifies:
#
#   Initial state of "toggle" status
#
# Type of value:
#
#   1 or 0
#
```

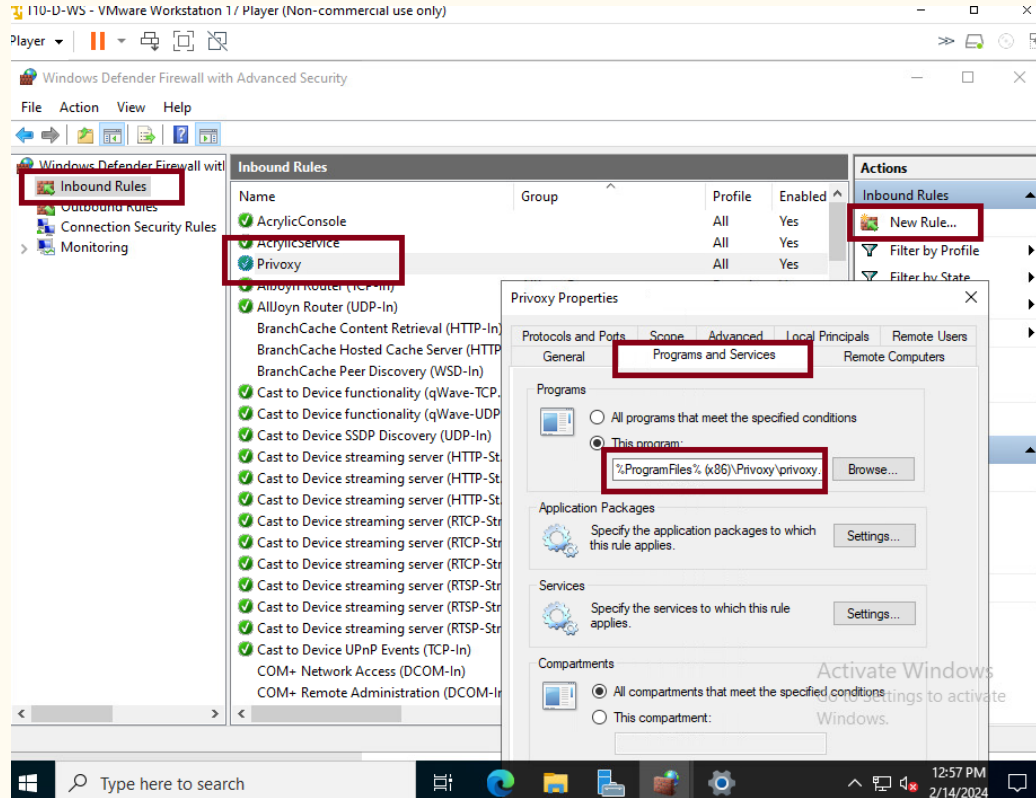
# Privoxy configuration in a Windows computer.

On settings go to proxy and change use a proxy server to on and add the address and listening port.

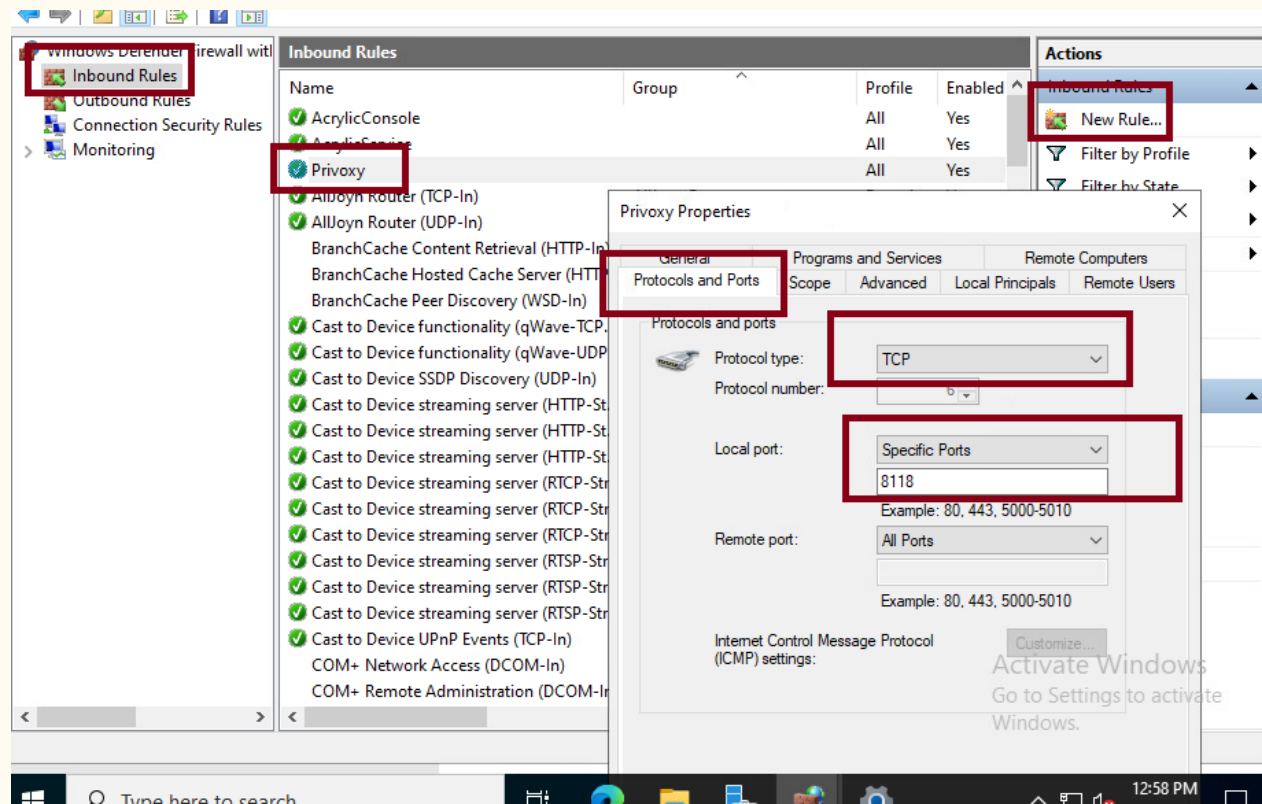


# Privoxy configuration in a Windows server.

You must allow the service to receive request by creating a new rule in windows defender with advance security in windows. Create the rule to give access to privoxy by adding the path to the executable in your computer by browsing to it.

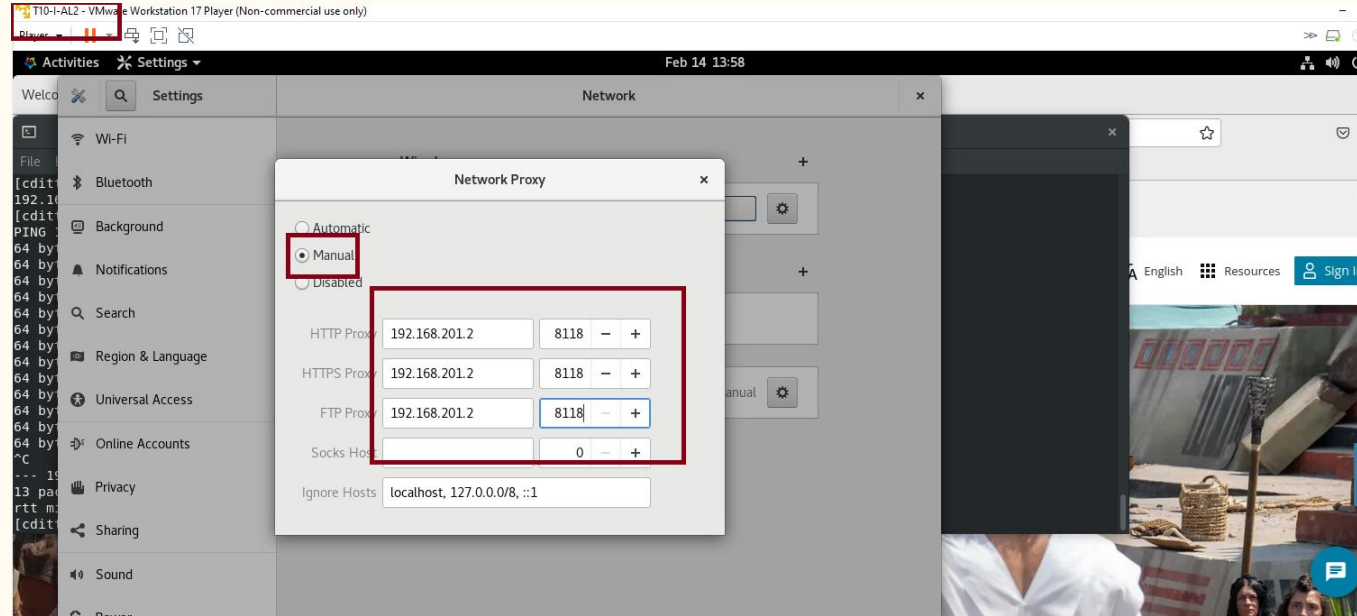


The protocols of the rule must be TCP and the port 8118. If you are not sure of this settings can edit the rule and change the configuration of the rule to match this.



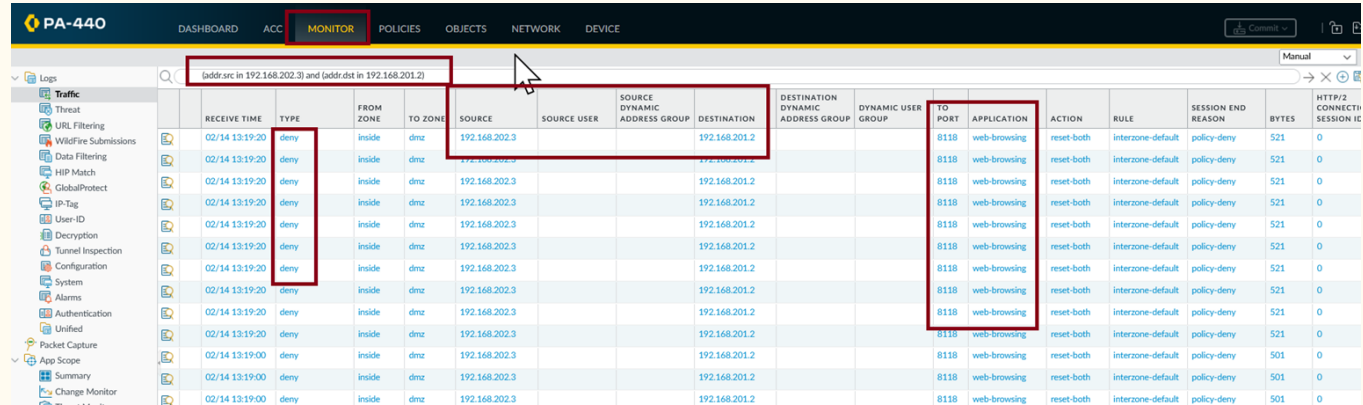
# Privoxy configuration in a Alma Linux server.

Go to settings, and on network proxy change to the address that host privoxy and the listening port. Upon change this stop and start the service network to be sure the changes are updated.



# Testing the service.

The service shows problems between zones. In the Palo Alto monitor we can see many deny request. We must create a rule to allow those request to go through.



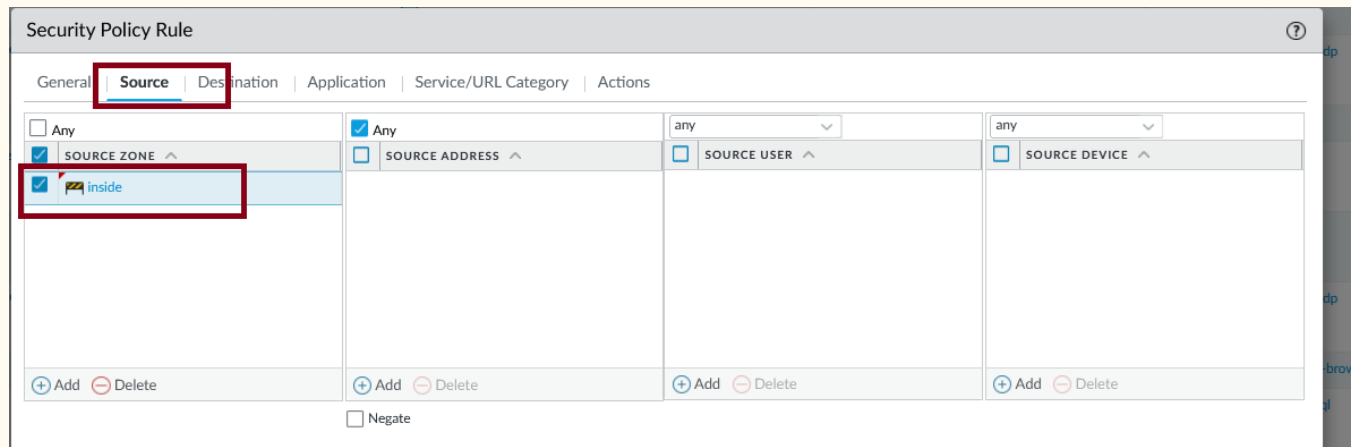
PA-440 DASHBOARD ACC **MONITOR** POLICIES OBJECTS NETWORK DEVICE

Search: (addrsrc in 192.168.202.3) and (addrdst in 192.168.201.2)

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECT
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:20	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	521	0
	02/14 13:19:00	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	501	0
	02/14 13:19:00	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	501	0
	02/14 13:19:00	deny	inside	dmz	192.168.202.3			192.168.201.2			8118	web-browsing	reset-both	interzone-default	policy-deny	501	0

# Creating a rule to allow privoxy on the Palo Alto firewall.

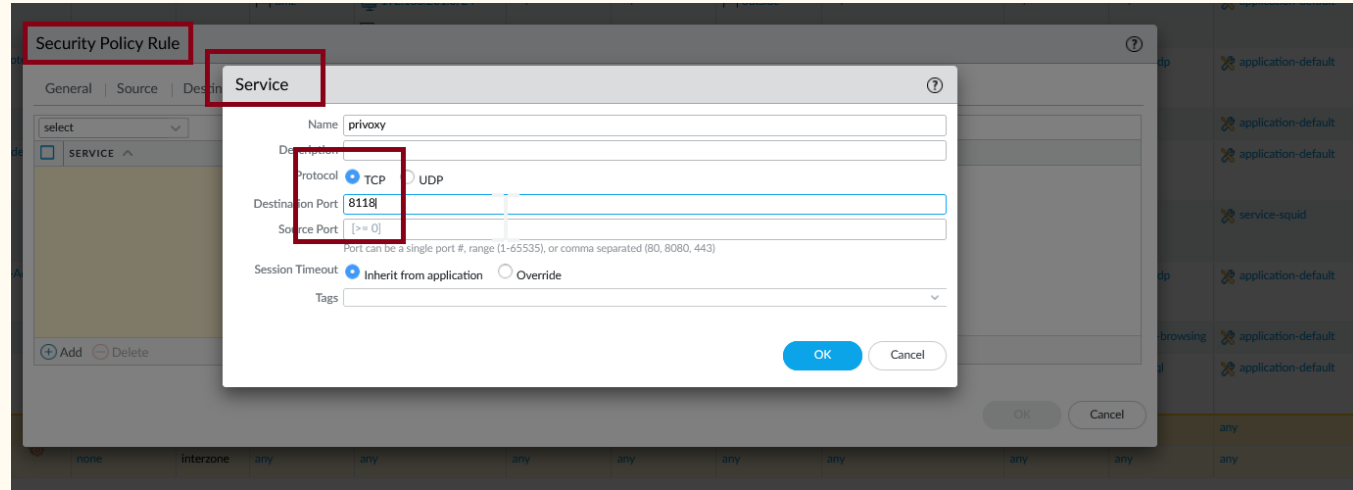
A new rule with source in intern and destination to DMZ will provide access to privoxy. Open on Palo Alto the policy tab and create a new policy.





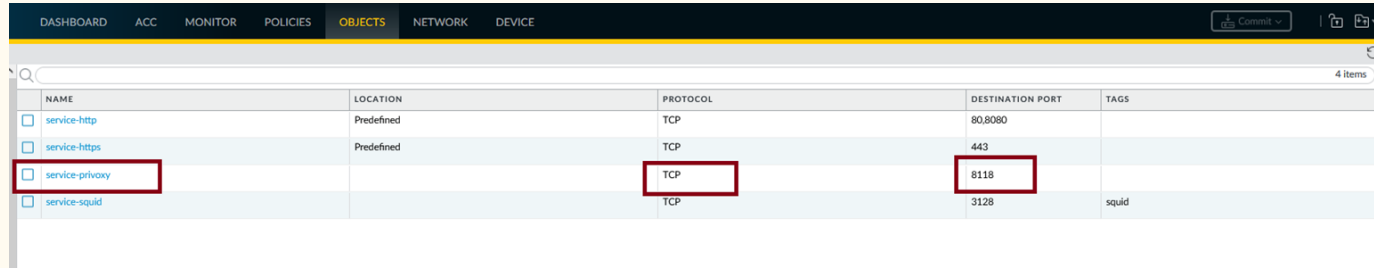
# Creating a rule to allow privoxy on the Palo Alto firewall.

In the service tab create a new service call privoxy, that will use TCP and port 8118.



# Creating a rule to allow privoxy on the Palo Alto firewall.

After the configuration changes if you look into objects you could see the new privoxy service object configuration.



NAME	LOCATION	PROTOCOL	DESTINATION PORT	TAGS
<input type="checkbox"/> service-http	Predefined	TCP	80,8080	
<input type="checkbox"/> service-https	Predefined	TCP	443	
<input type="checkbox"/> service-privoxy		TCP	8118	
<input type="checkbox"/> service-squid		TCP	3128	squid

# Creating a rule to allow privoxy on the Palo Alto firewall.

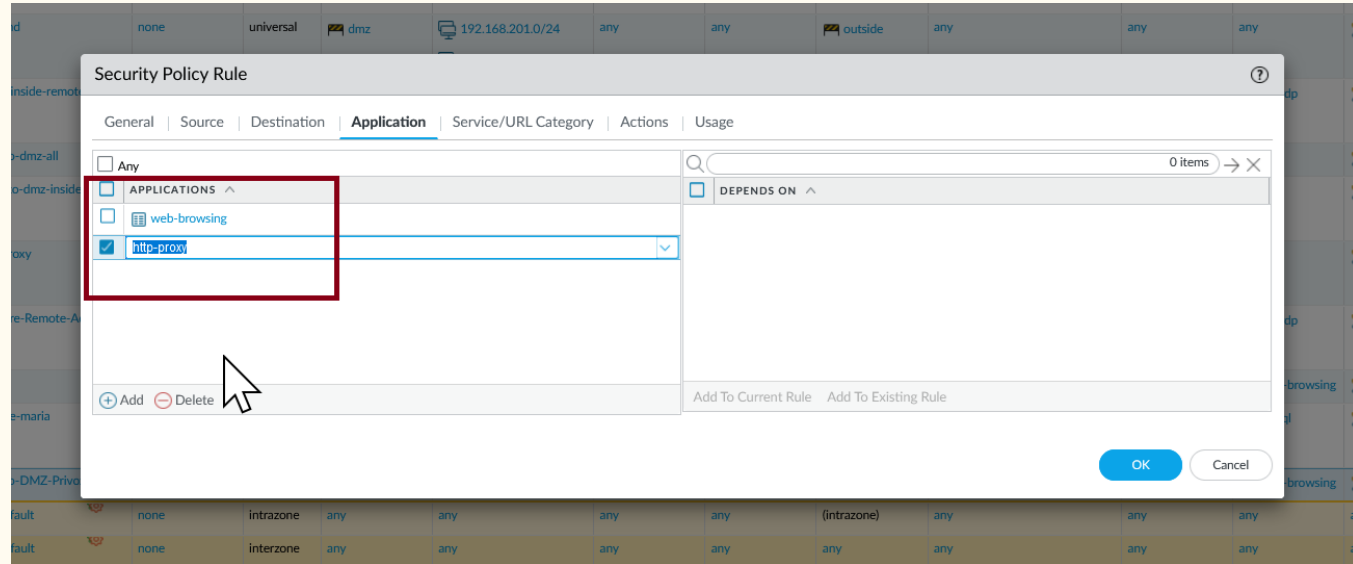
When trying again the web server, communications were deny but because another service is required, http-proxy.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. At the top, there's a navigation bar with tabs like DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. Below this is a search bar containing the IP addresses 192.168.201.2 and 192.168.201.2. The main area displays a table of network events. A red box highlights a specific event row, and two red arrows point to the 'ACTION' and 'POLICY' columns within this row.

	TIME	ACTION	FROM	TO	SOURCE	DYNAMIC	DESTINATION	DYNAMIC USER	TO	ACTION	POLICY	SESSION END REASON	BYTES	HTTP/2 CONN SESSION
	02/14 13:32:20	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	http-proxy	deny	interzone-default policy-deny	503	0
	02/14 13:32:20	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	http-proxy	deny	interzone-default policy-deny	529	0
	02/14 13:32:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	http-proxy	deny	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0
	02/14 13:31:05	deny	inside	dmz	192.168.201.2		192.168.201.2		8118	web-browsing	reset-both	interzone-default policy-deny	521	0

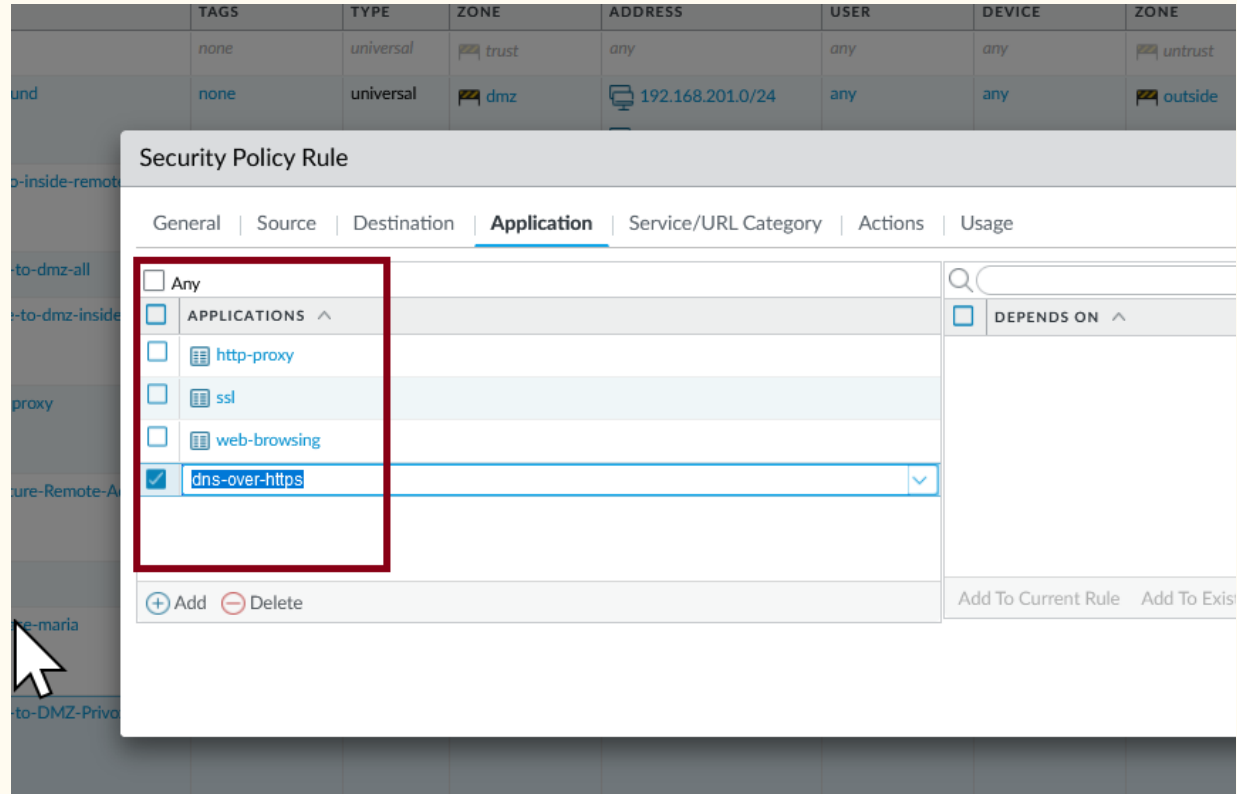
# Creating a rule to allow privoxy on the Palo Alto firewall.

If you allow the service maybe it can allow the privoxy service to work. In the policy rule for privoxy add the service required.



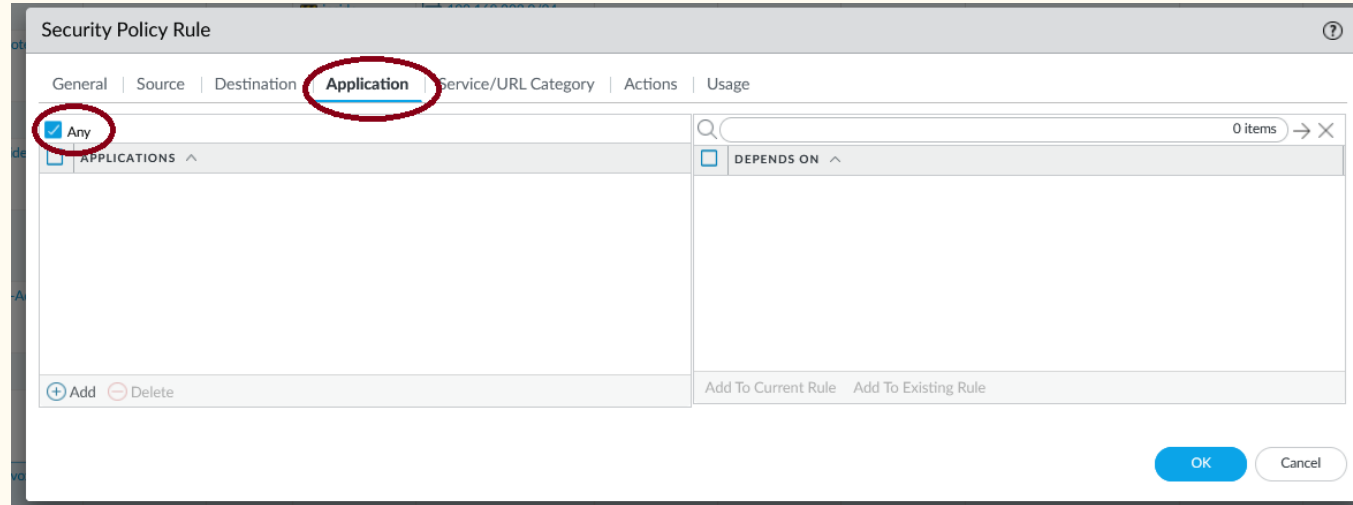
# Creating a rule to allow privoxy on the Palo Alto firewall.

After commit the changes and try again another services were asked until we reached to add 4 services, and still a new one was required.



# Creating a rule to allow privoxy on the Palo Alto firewall.

Don't do what was showing before. Instead is more useful to use the “any” option in the Application tab of the policy rule. That will allow all necessary protocols. That change give access to the web service.



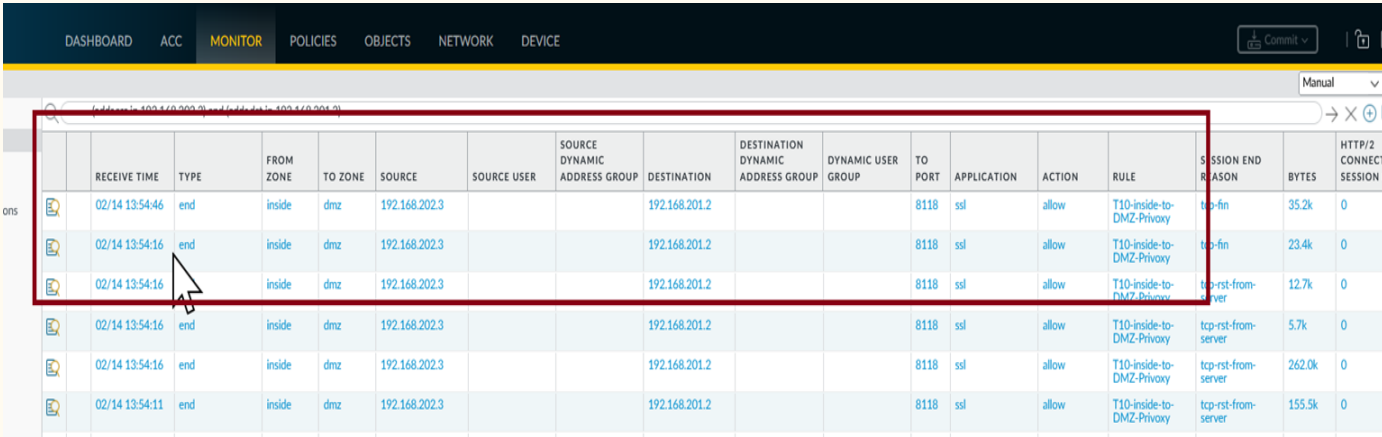
# Creating a rule to allow privoxy on the Palo Alto firewall.

The same problem needs solution for the secure zone. Adding the interconnected zone as a new source to the already working rule for privoxy solved communications between the secure and the dmz zone.

	NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS	DEVICE			
1	rule1	none	universal	trust	any	any	untrust	any	any	any	any	Allow
2	T10-outbound	none	universal	dmz	192.168.201.0/24	any	outside	any	any	any	application-default	Allow
3	T10-dmz-to-inside-remote-access	none	universal	dmz	192.168.201.0/24	any	inside	192.168.202.0/24	any	ms-rdp	application-default	Allow
4	T10-inside-to-dmz-all	none	universal	inside	192.168.202.0/24	any	dmz	192.168.201.0/24	any	ssh	application-default	Allow
5	T10-secure-to-dmz-inside	none	universal	interconnect	192.168.203.0/24	any	dmz	192.168.201.0/24	any	any	application-default	Allow
6	T10-squid-proxy	none	universal	interconnect	192.168.203.0/24	any	dmz	192.168.201.0/24	any	any	service-squid	Allow
7	T10-to-Secure-Remote-Admin	none	universal	dmz	192.168.201.0/24	any	interconnect	192.168.203.0/24	any	ms-rdp	application-default	Allow
8	T10-web	none	universal	outside	any	any	dmz	157.201.22.72	any	web-browsing	application-default	Allow
9	T10-database-maria	none	universal	dmz	192.168.201.7	any	interconnect	192.168.203.3	any	mysql	application-default	Allow
10	T10-inside-to-DMZ-Privoxy	none	universal	inside	any	any	dmz	any	any	any	service-privoxy	Allow

# Creating a rule to allow privoxy on the Palo Alto firewall.

Now traffic to the secure and internal zone is allowed for the privoxy services.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECT SESSION ID
	02/14 13:54:46	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-fin	35.2k	0
	02/14 13:54:16	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-fin	23.4k	0
	02/14 13:54:16	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-rst-from-server	12.7k	0
	02/14 13:54:16	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-rst-from-server	5.7k	0
	02/14 13:54:16	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-rst-from-server	262.0k	0
	02/14 13:54:11	end	inside	dmz	192.168.202.3			192.168.201.2			8118	ssl	allow	T10-inside-to-DMZ-Privoxy	tcp-rst-from-server	155.5k	0



# Working configuration from the intern zone

This is the proxy configuration on the Alma Linux machine in the intern zone, that now have web services provided by privoxy using port 8118 from the DMZ zone.

