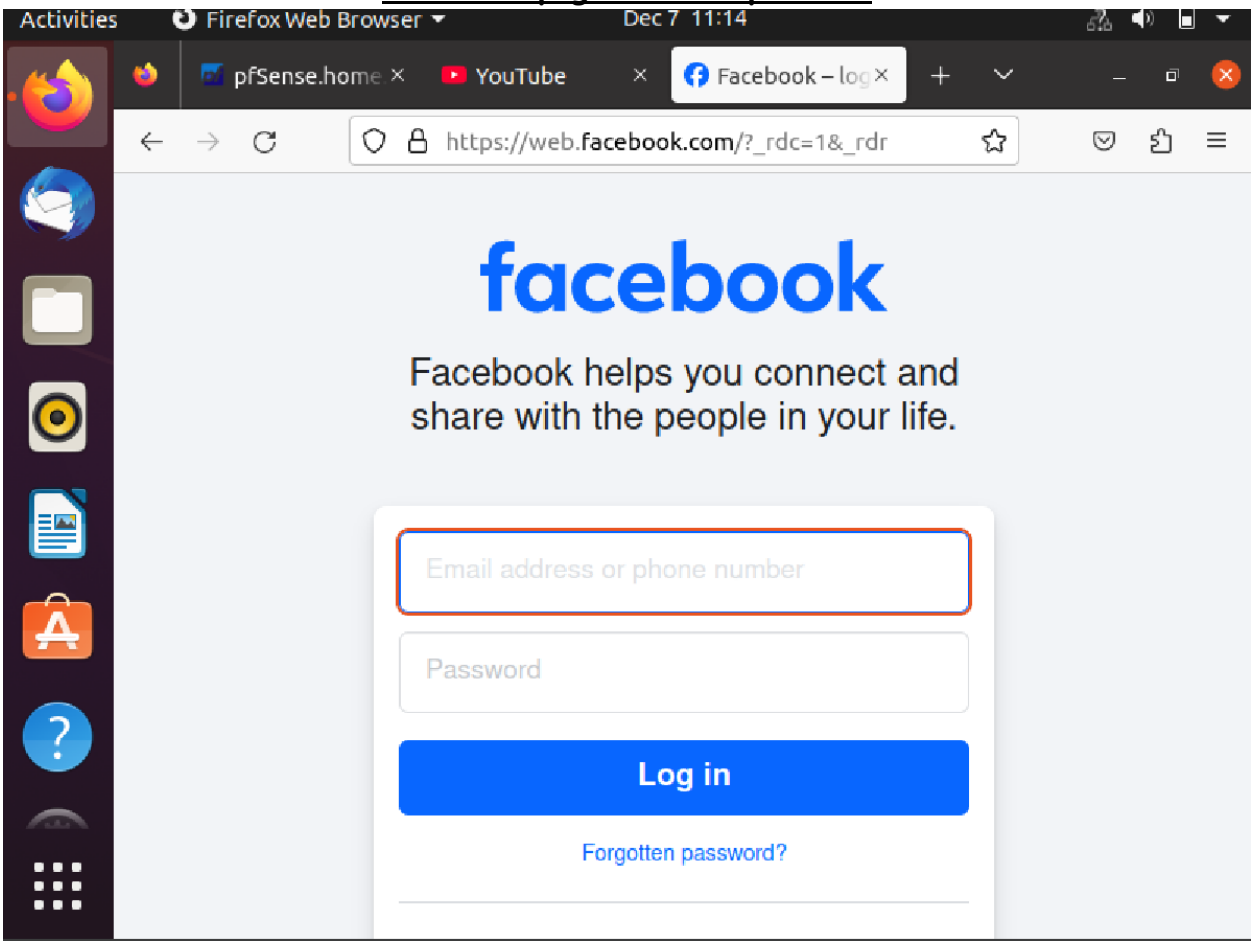
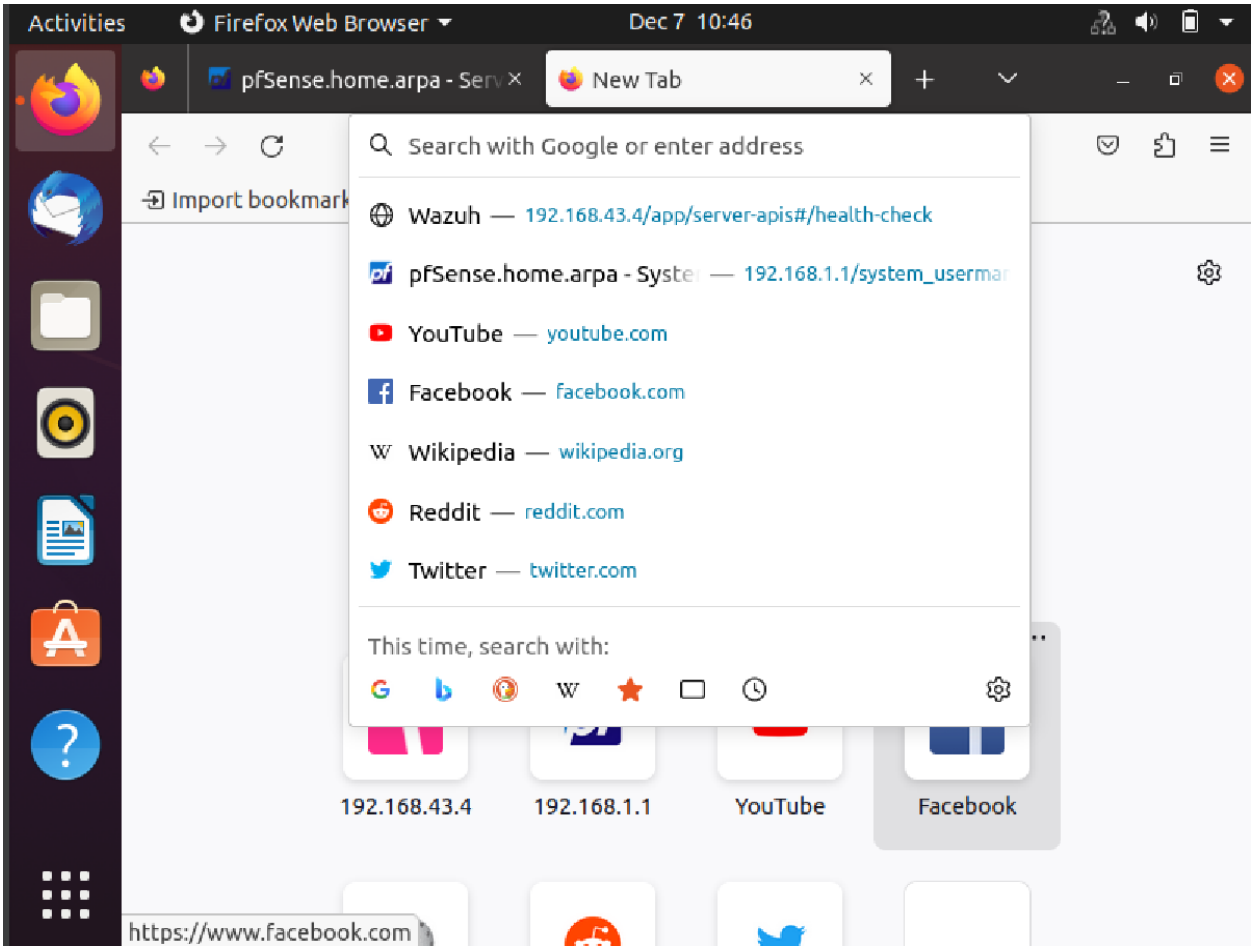
Assignment pfSense

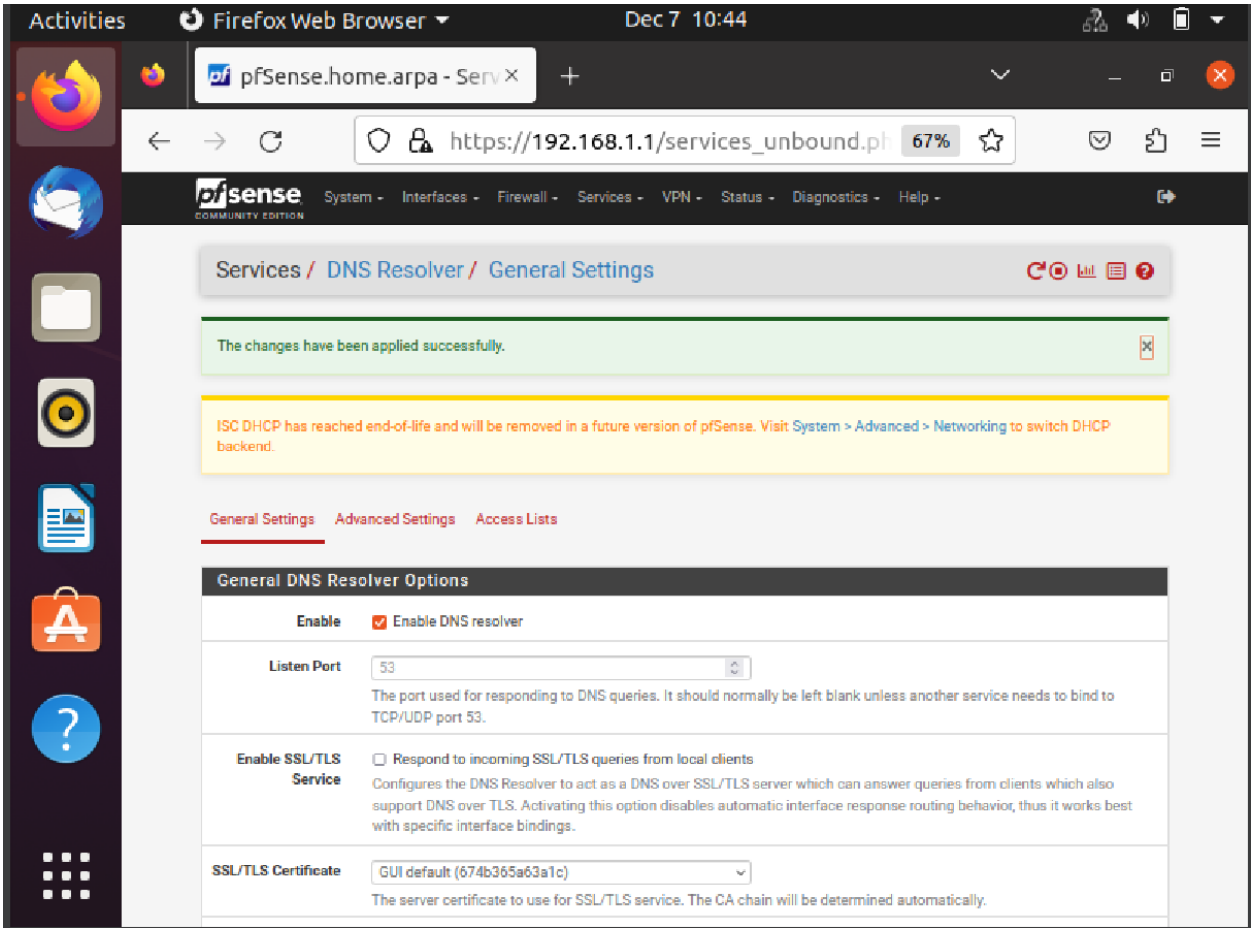
Facebook page without pfSense



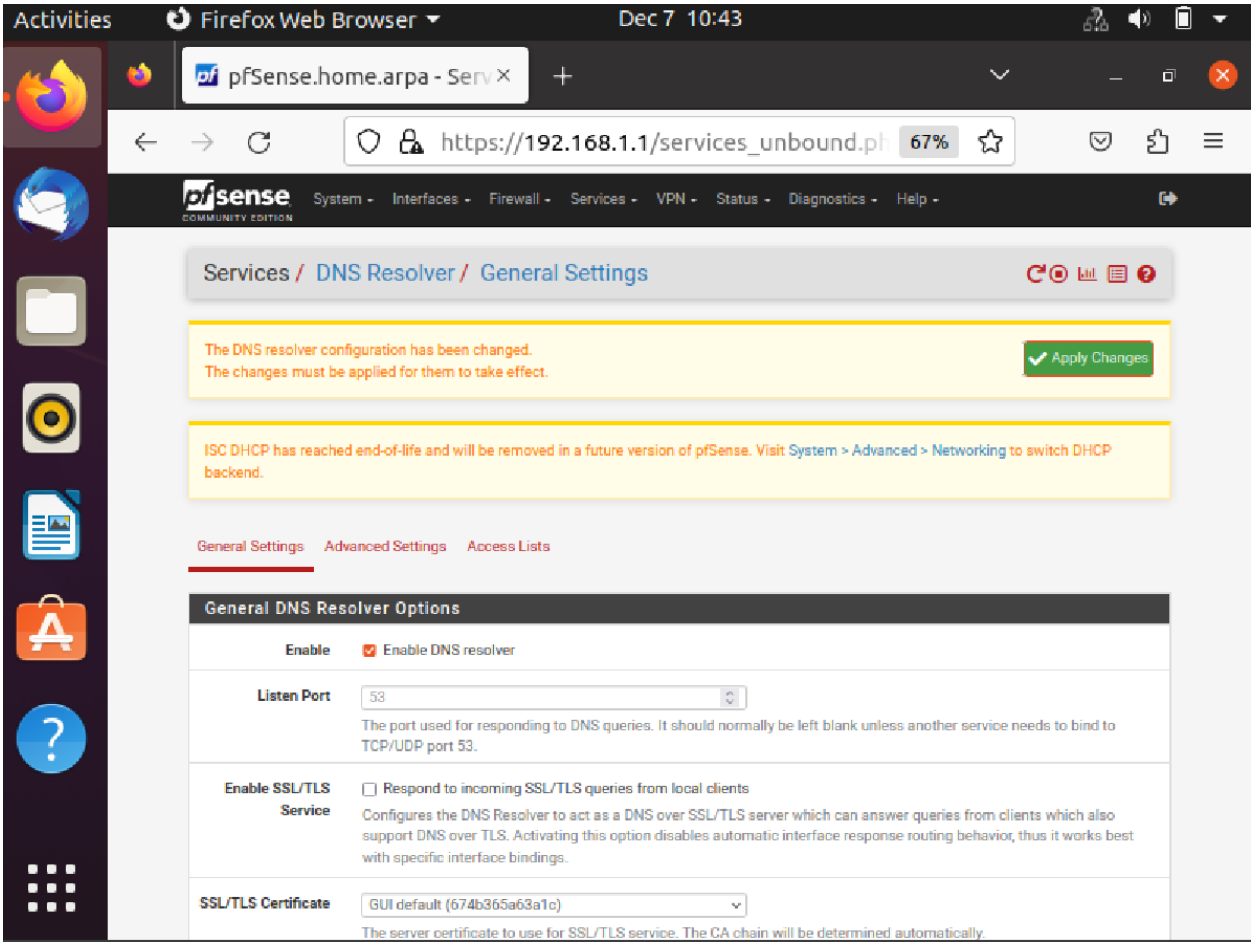
Step 1


Activities
Firefox Web Browser
Dec 7 10:46
pfSense.home.arpa - Serv
New Tab
Search with Google or enter address
Import bookmark
Wazuh — 192.168.43.4/app/server-apis#/health-check
pfSense.home.arpa - Syste — 192.168.1.1/system_usermar
YouTube — youtube.com
Facebook — facebook.com
Wikipedia — wikipedia.org
Reddit — reddit.com
Twitter — twitter.com
This time, search with:
192.168.43.4
192.168.1.1
YouTube
Facebook
https://www.facebook.com

Step2

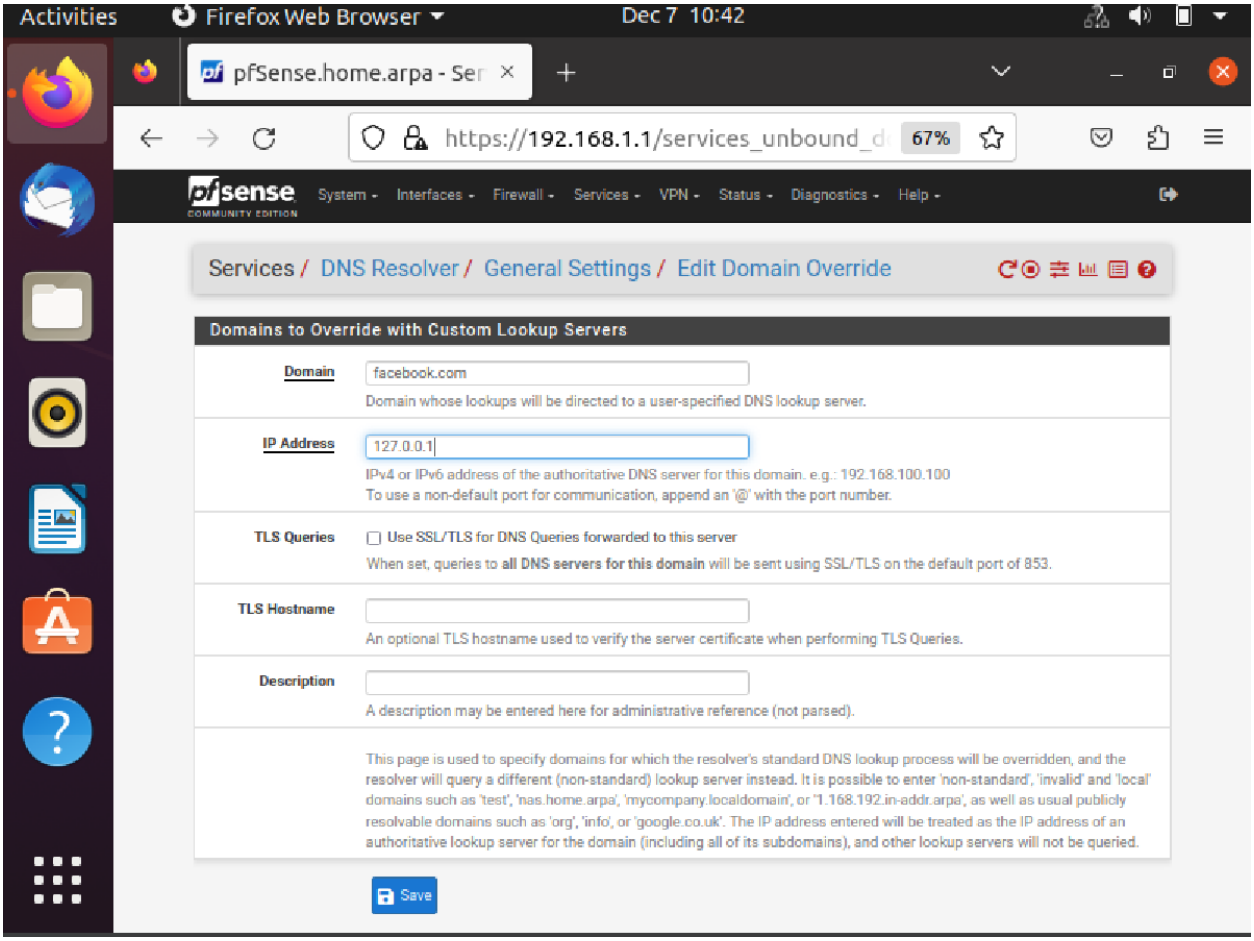

Activities
Firefox Web Browser
Dec 7 10:44
pfSense.home.arpa - Serv
https://192.168.1.1/services_unbound.pl
67%
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DNS Resolver / General Settings
The changes have been applied successfully.
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate
GUI default (674b365a63a1c)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

Step3

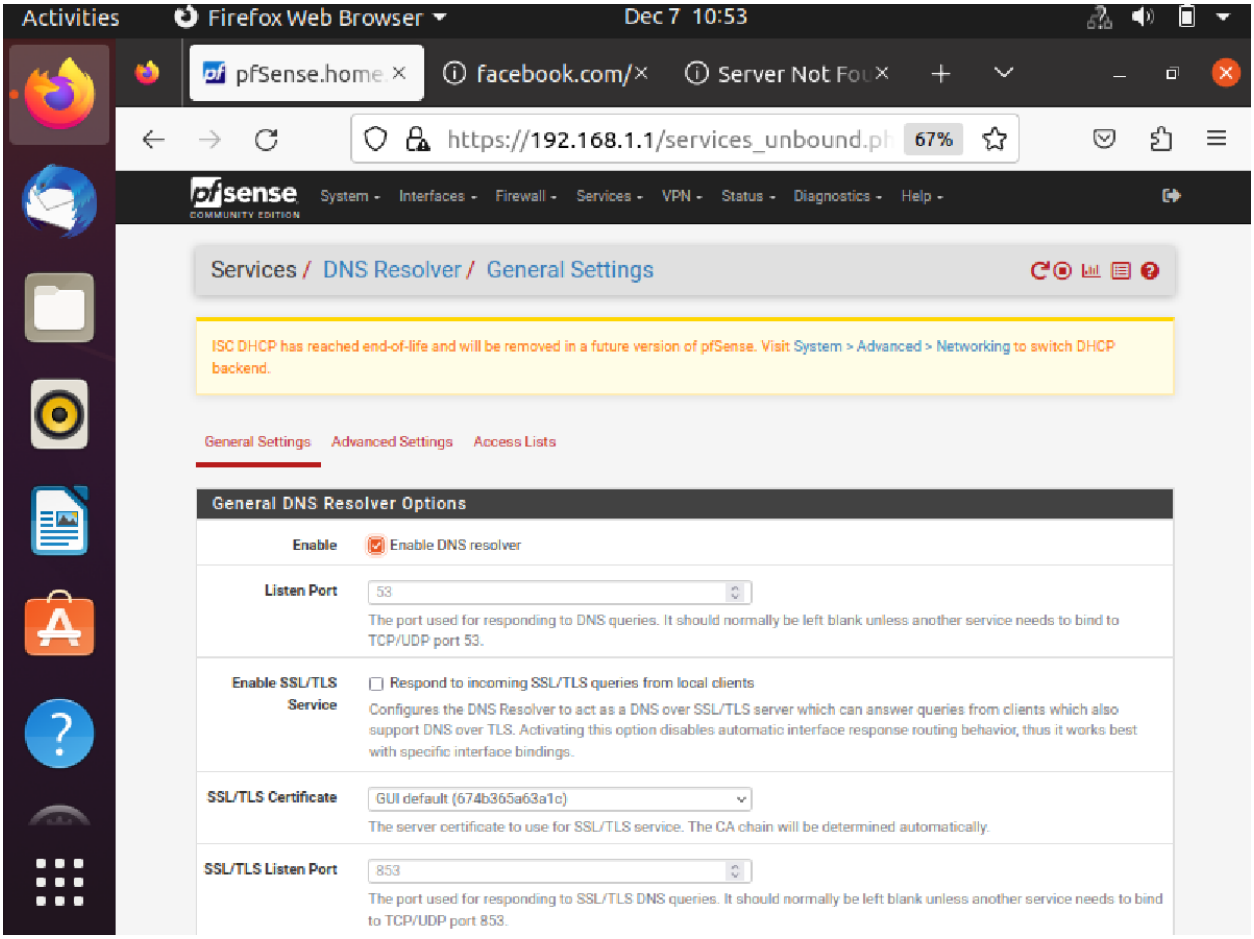

Activities
Firefox Web Browser
Dec 7 10:43
pfSense.home.arpa - Serv
https://192.168.1.1/services_unbound.pl
67%
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DNS Resolver / General Settings
The DNS resolver configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate
GUI default (674b365a63a1c)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

Step 4

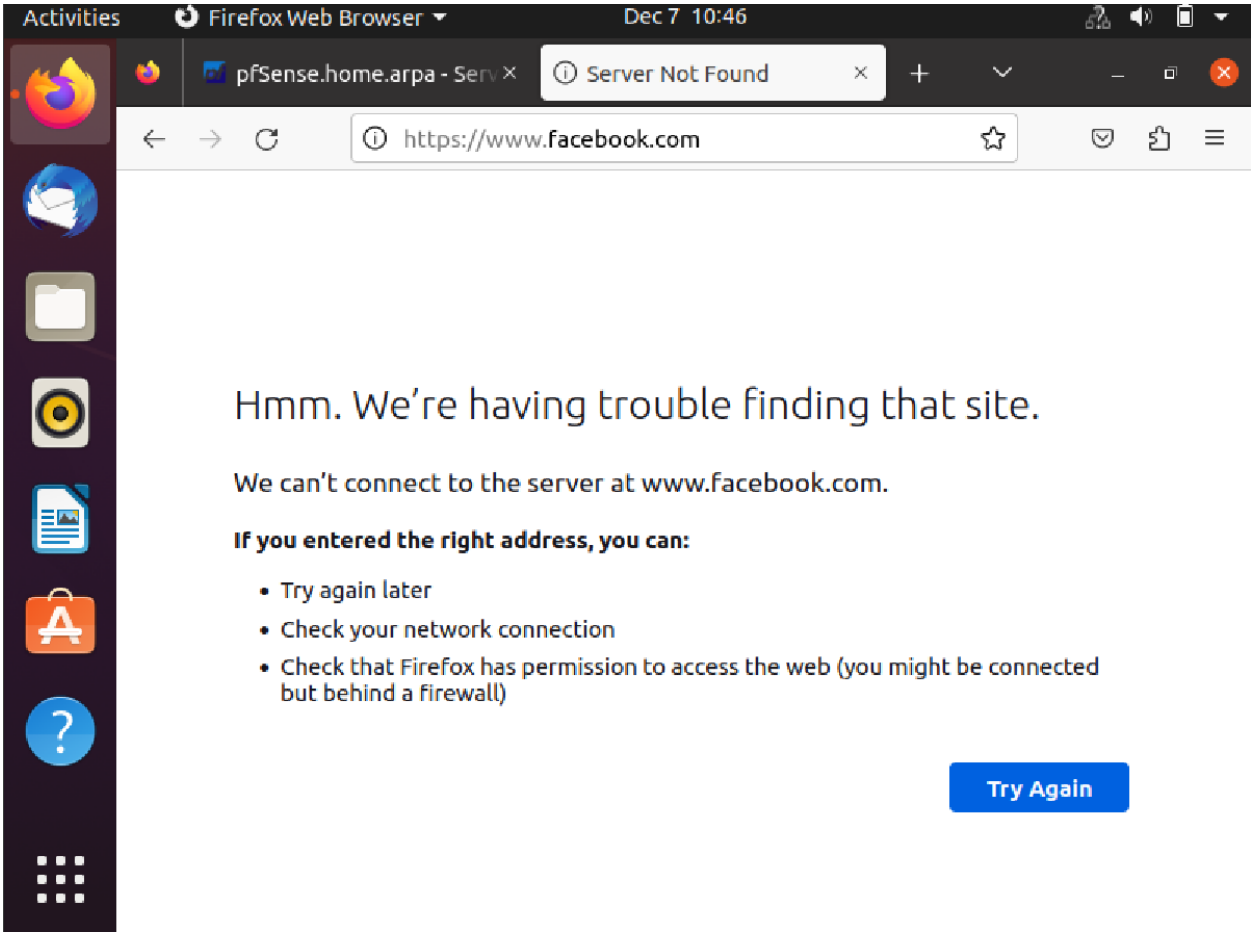
Step 5


Activities
Firefox Web Browser
Dec 7 10:42
pfSense.home.arpa - Ser
https://192.168.1.1/services_unbound_d
67%
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DNS Resolver / General Settings / Edit Domain Override
Domains to Override with Custom Lookup Servers
Domain
facebook.com
Domain whose lookups will be directed to a user-specified DNS lookup server.
IP Address
127.0.0.1
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100
To use a non-default port for communication, append an '@' with the port number.
TLS Queries
Use SSL/TLS for DNS Queries forwarded to this server
When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
TLS Hostname
An optional TLS hostname used to verify the server certificate when performing TLS Queries.
Description
A description may be entered here for administrative reference (not parsed).
This page is used to specify domains for which the resolver's standard DNS lookup process will be overridden, and the resolver will query a different (non-standard) lookup server instead. It is possible to enter 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable domains such as 'org', 'info', or 'google.co.uk'. The IP address entered will be treated as the IP address of an authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.
Save

Step 6


Activities
Firefox Web Browser
Dec 7 10:53
pfSense.home
facebook.com/
Server Not Fou
https://192.168.1.1/services_unbound.ph
67%
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DNS Resolver / General Settings
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate
GUI default (674b365a63a1c)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.
SSL/TLS Listen Port
853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

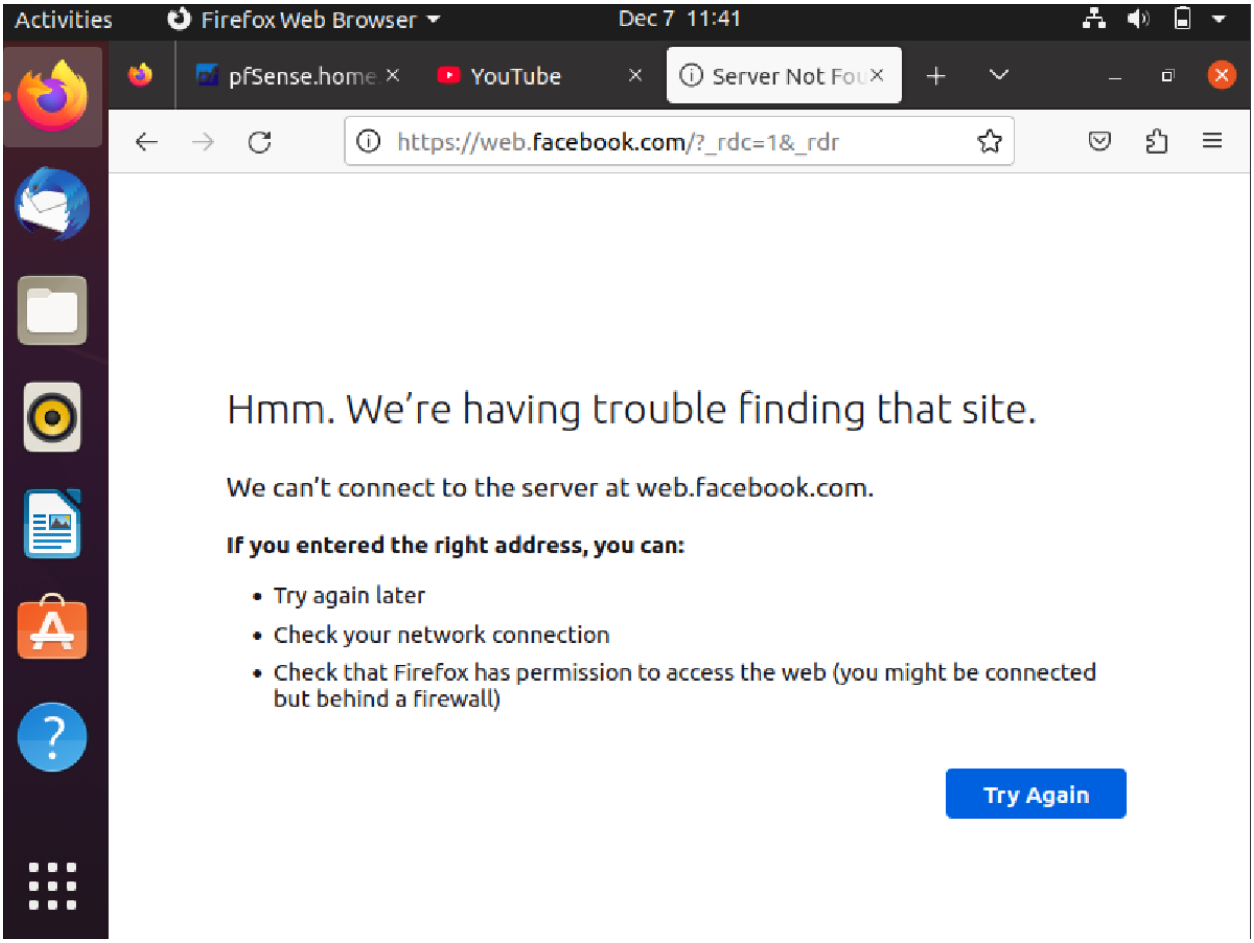
Step 7: Testing.

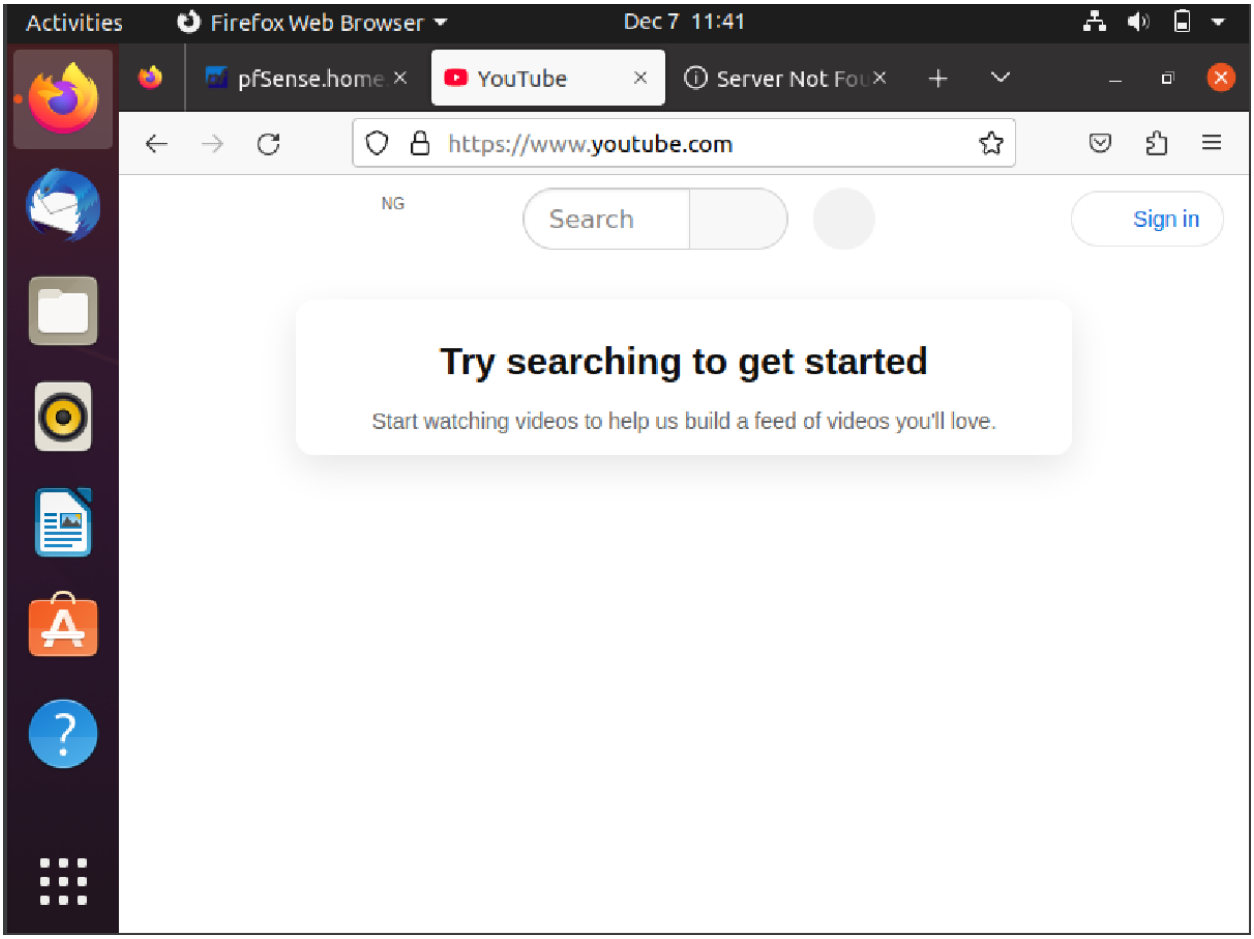


Observations:

1. The facebook website was accessible without pfSense on Ubuntu
2. The website was inaccessible when connected to pfsense with NAT as we as with bridge network
3. However unresolved is the issue where other websites were also not accessible from behind pfSense firewall
4. I will continue to try resolving this issue.
5. Update: Internet connection worked for other websites with pfSense→Bridge-Adapter and Ubuntu→Internal→LAN. Otherwise it blocks all. Only the blocked domain name is inaccessible now

After changing to bridge on pfSense and blocking facebook.com Blocking




Activities
Firefox Web Browser
Dec 7 11:41
pfSense.home
YouTube
Server Not Fou
https://www.youtube.com
NG
Search
Sign in
Try searching to get started
Start watching videos to help us build a feed of videos you'll love.