securly://

best practices to secure your Securly DNS deployment

tech brief – March2016 – v1.0

Contents

Overview

This document outlines several Best Practices that Securly recommends for a successful web-filtering deployment.

Onboarding

Static IP address

One of the key components of a successful deployment as well as to utilize an in school and take home policy is the requirement for a static public IP address(s). If it very critical that any IPs in which traffic will leave your network be registered with Securly.

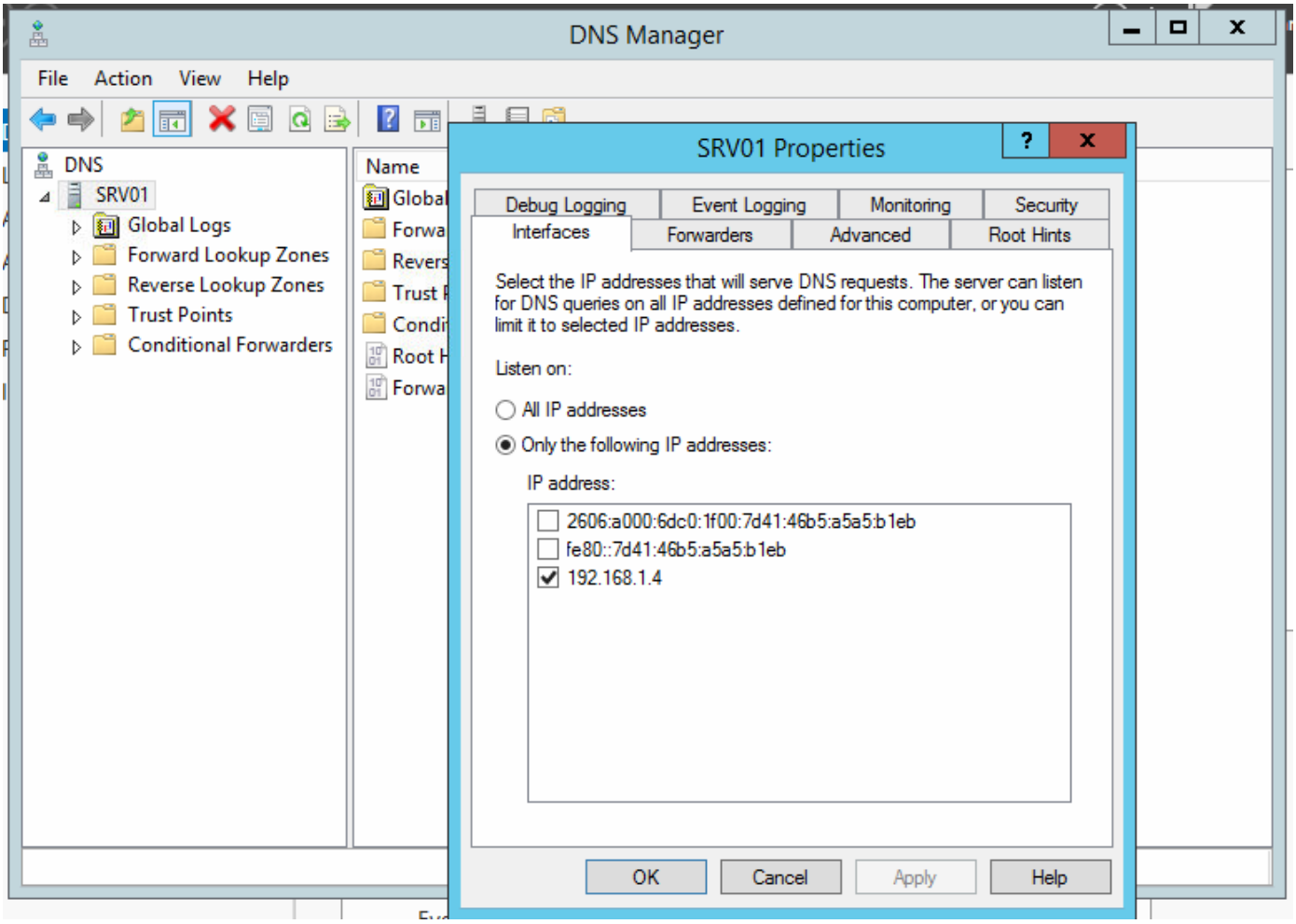
Configuration

IPv6

At this time it is a requirement to completely disable IPv6 as we currently only support IPv4. To disable IPv6. The following pages describe how to disable IPv6 on various platforms.

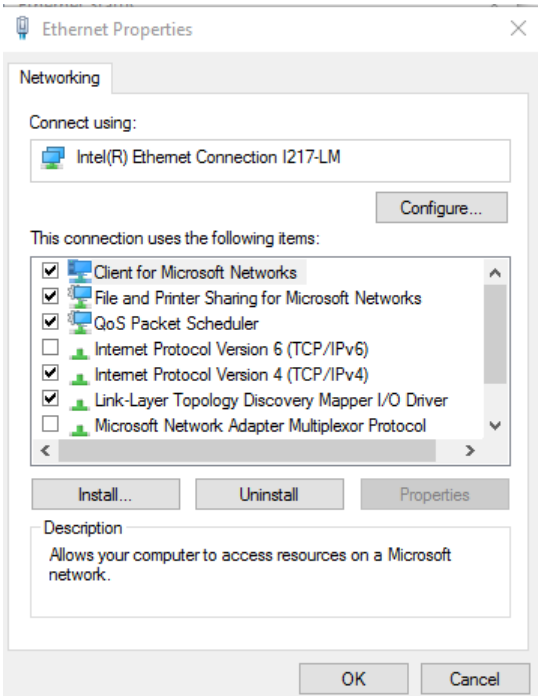
Windows Server DNS

- Start> DNS Manager
- Expand out the DNS options
- Right click the DNS server name and select properties
- Select the radio box under Interfaces for “Listen On:” “Only the following IP addresses:” and uncheck any IPv6 address that is listed.



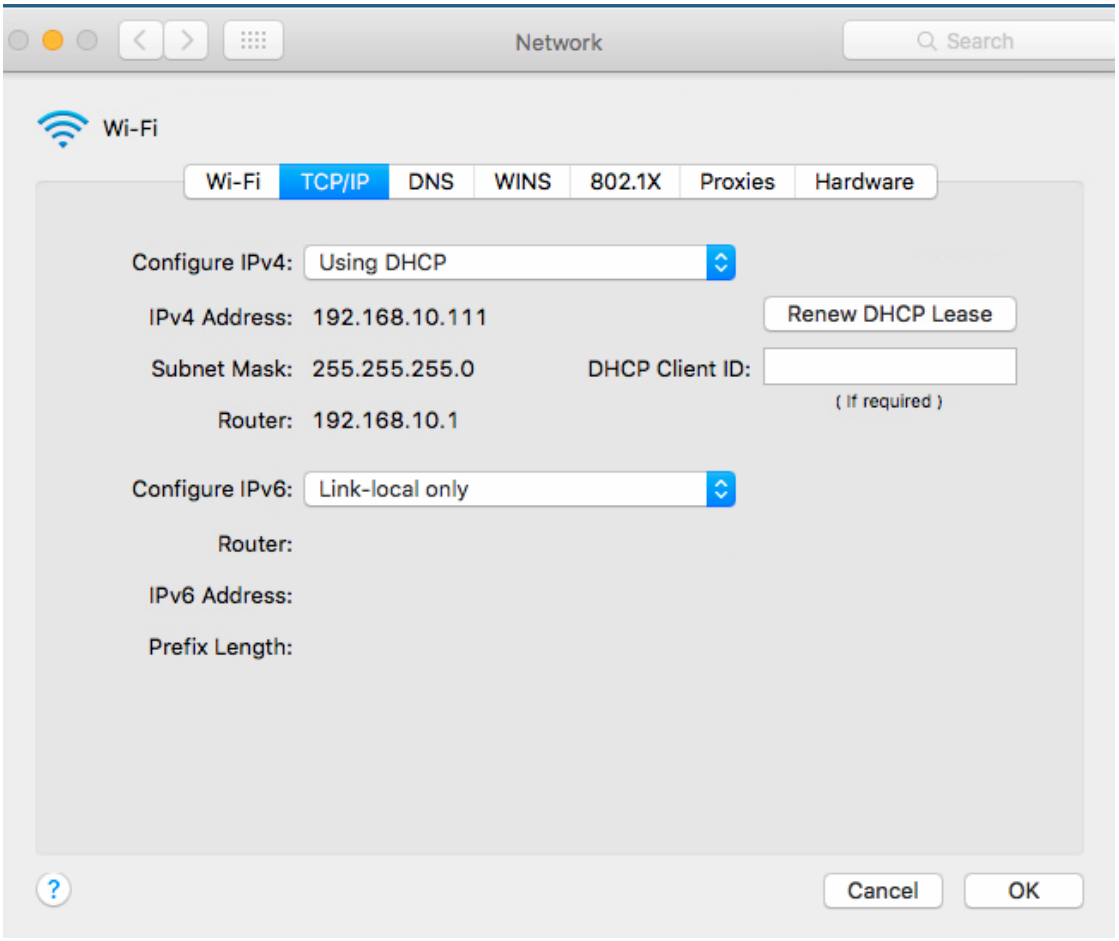
Windows Standalone DNS

- Start > type in “view network connections” and open the control panel item
- Double click on one of the network connections
- Go to Properties
- Uncheck “Internet Protocol Version 6 (TCP/IPv6)
  Note: This step needs to be done for all network adapters on the machine



OSX DNS

- Click the magnifying the glass at the top right corner
- Type in “network” and select the network preferences
- Select the current connection on the left
- At the bottom click on “Advanced”
- Click on “TCP/IP”
- Under “Configure IPv6” please change this from “Automatically” to “link-local only”



SSL deployment

SSL Standalone deployment

If you are using standalone PC/MAC the SSL certificate will have to be manually installed.

Windows Server Deployment

- Open Administrative Tools, and then click Group Policy Management.
- In the console tree, under the top level of the domain, right click and create a new policy and title it Securly SSL.

- Double-click Group Policy Objects in the domain containing the Securly SSL Group Policy object (GPO) that you want to edit.
- In the Group Policy Management Console (GPMC), go to "Computer Configuration > Windows Settings > Security Settings > Public Key Policies".
- Right-click the Trusted Root Certification Authorities store.

Click Import and follow the steps in the Certificate Import Wizard to import the certificates.

Windows SSL Standalone

- Please click on start->type in “certmgr.msc”
- Click on “Trusted Root Certificate Authorities”
- Expand out Certificates
- Right click on Certificates Select All Tasks>Import
- Please select the downloaded Securly certificate and leave all other options as their defaults.

OSX SSL Standalone

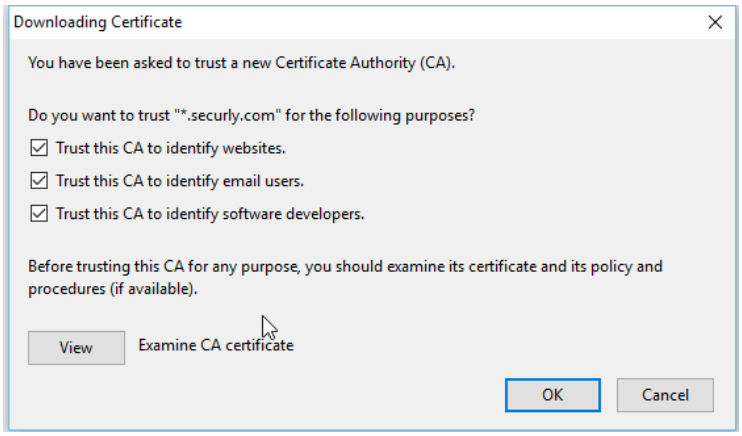
- Right hand corner of the screen>Magnifying Glass>Keychain Access.
- From Keychain Access>System.
- Click on the pad lock to unlock these settings.
- Please drop the downloaded Securly certificate to this window.
- Double click on “*.securly.com”.
- Expand out “trusts”.
- For “when using this certificate” please change this from “System Defaults” to “Always Trust”.

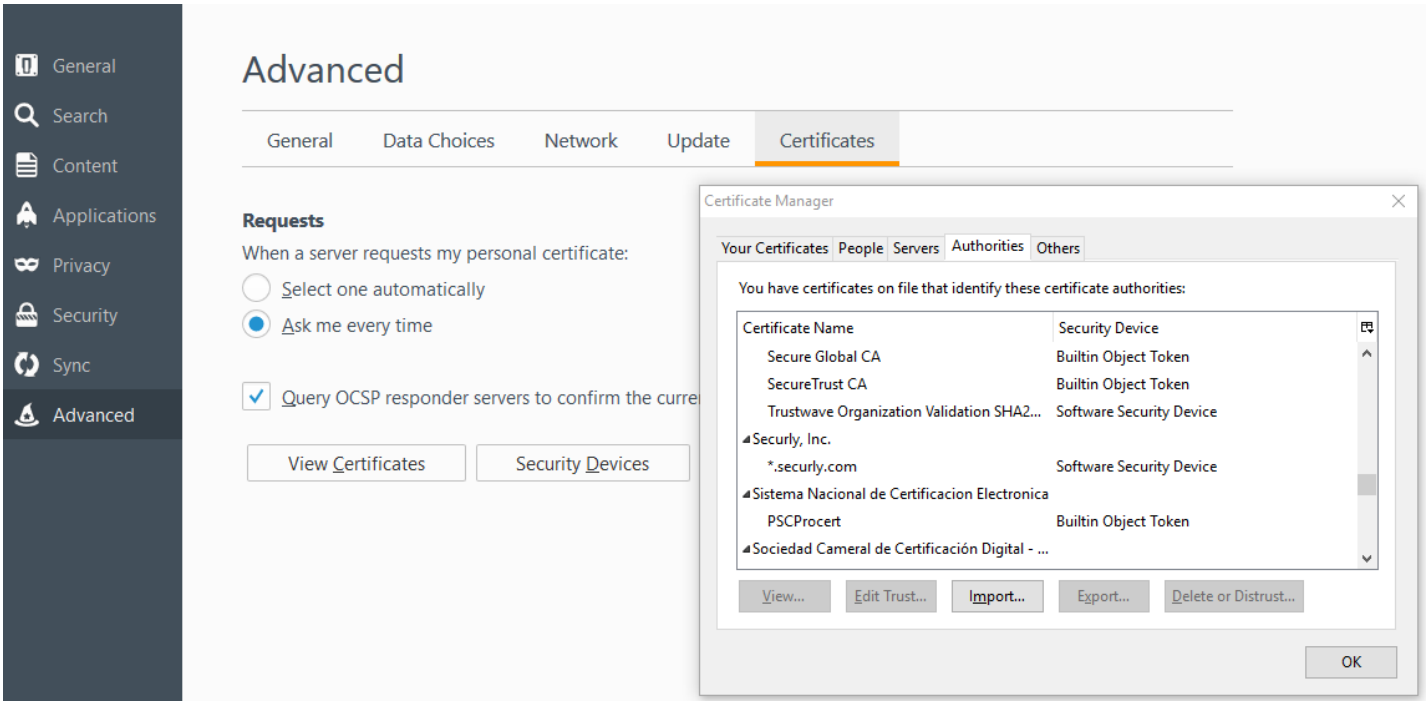
Firefox SSL deployment

Firefox on every OS does not use the centralized certificate store so it will have to be manually installed to the browser itself.

Windows Firefox SSL

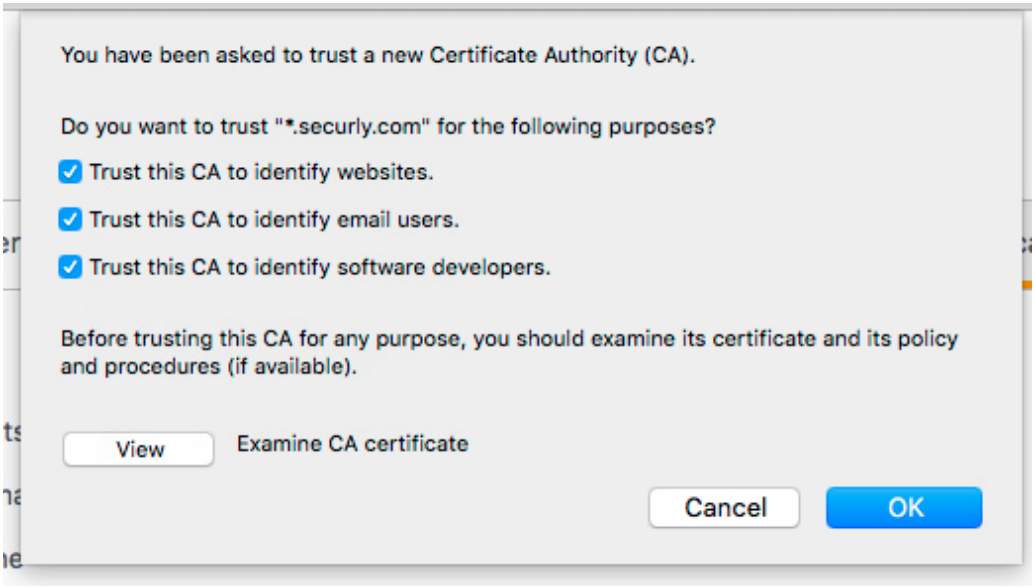
- In the Firefox window press the "alt" key on your keyboard.
- At the top of the screen select Tools > options.
- From the General Menu on the left click on Advanced>Certificate>View Certificates.
- Click the Authorities tab.
- Click Import and select the downloaded certificate.
- Please be sure to allow the certificate to be trusted for all 3 items offered.

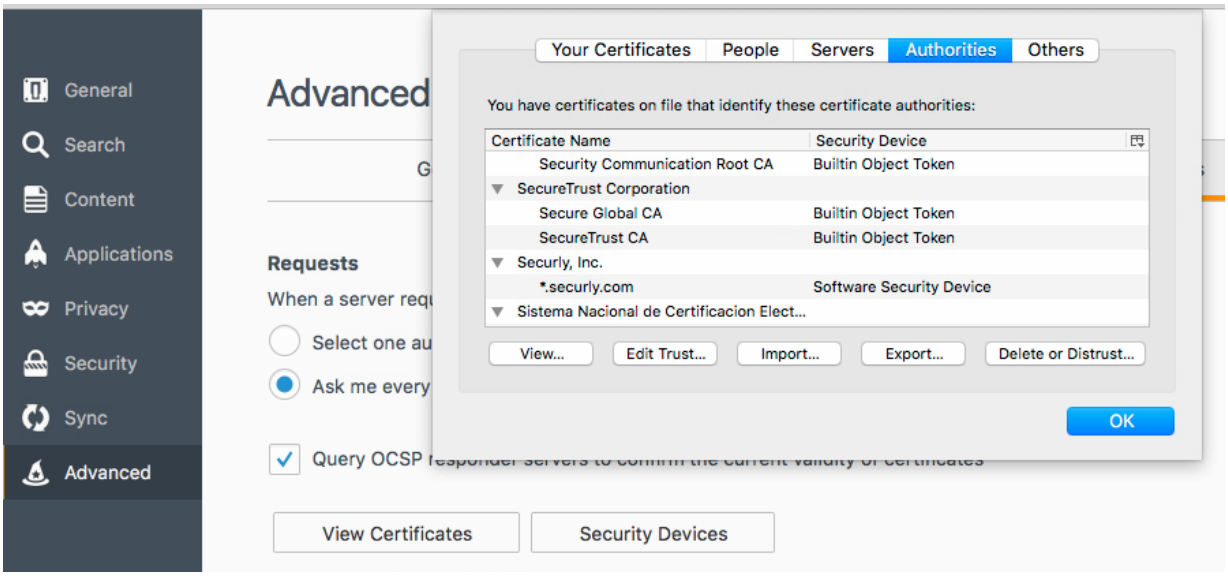

Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "*.securly.com" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
OK
Cancel


General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Advanced
General
Data Choices
Network
Update
Certificates
Requests
When a server requests my personal certificate:
Select one automatically
Ask me every time
Query OCSP responder servers to confirm the curre
View Certificates
Security Devices
Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
Secure Global CA
Builtin Object Token
SecureTrust CA
Builtin Object Token
Trustwave Organization Validation SHA2...
Software Security Device
Securly, Inc.
*.securly.com
Software Security Device
Sistema Nacional de Certificacion Electronica
PSCProcert
Builtin Object Token
Sociedad Cameral de Certificación Digital - ...
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK

OSX Firefox SSL

- In the Menu window, click on Firefox and select Preferences from the drop down menu.
- Click on Advanced>Certificates>View Certificates.
- From the Firefox View Certificates menu.
- Click the Authorities tab.
- Click Import and select the downloaded certificate.
- Please be sure to allow the certificate to be trusted for all 3 items offered.

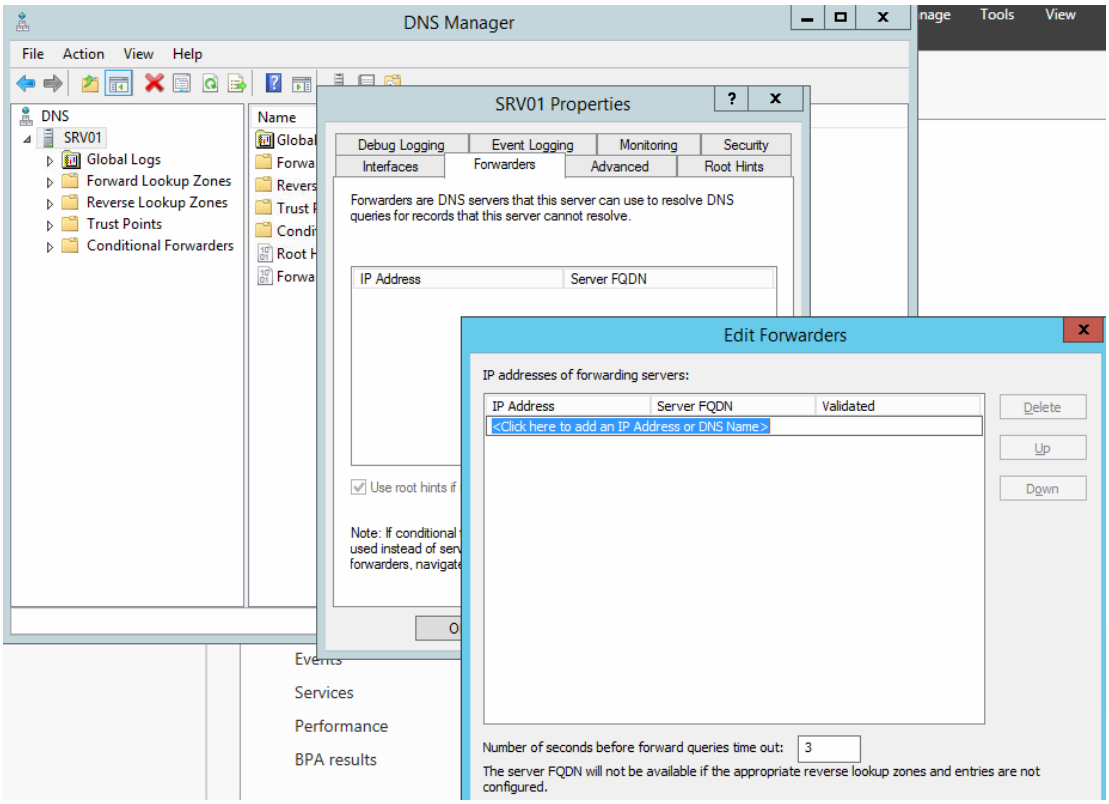




DNS Deployment

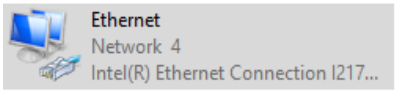
Windows Server

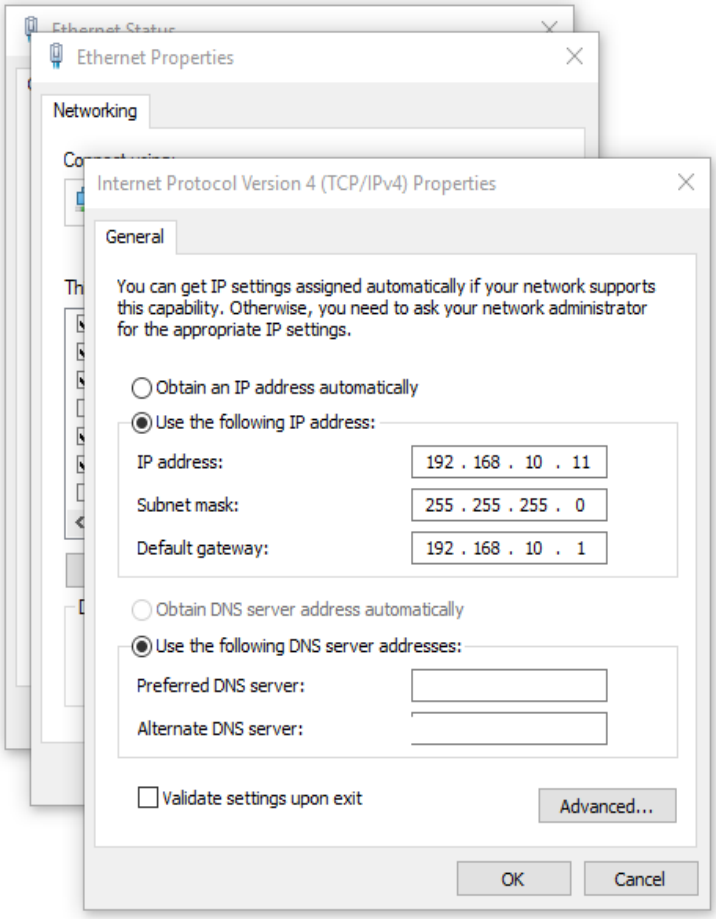
- Start> DNS Manager.
- Expand out the DNS options.
- Right click the DNS server name and select properties.
- Select Forwarders.
- Select “Edit”.
- For the 2 DNS servers please enter your applicable DNS server provided to you by your Sales Engineer.



Standalone Windows

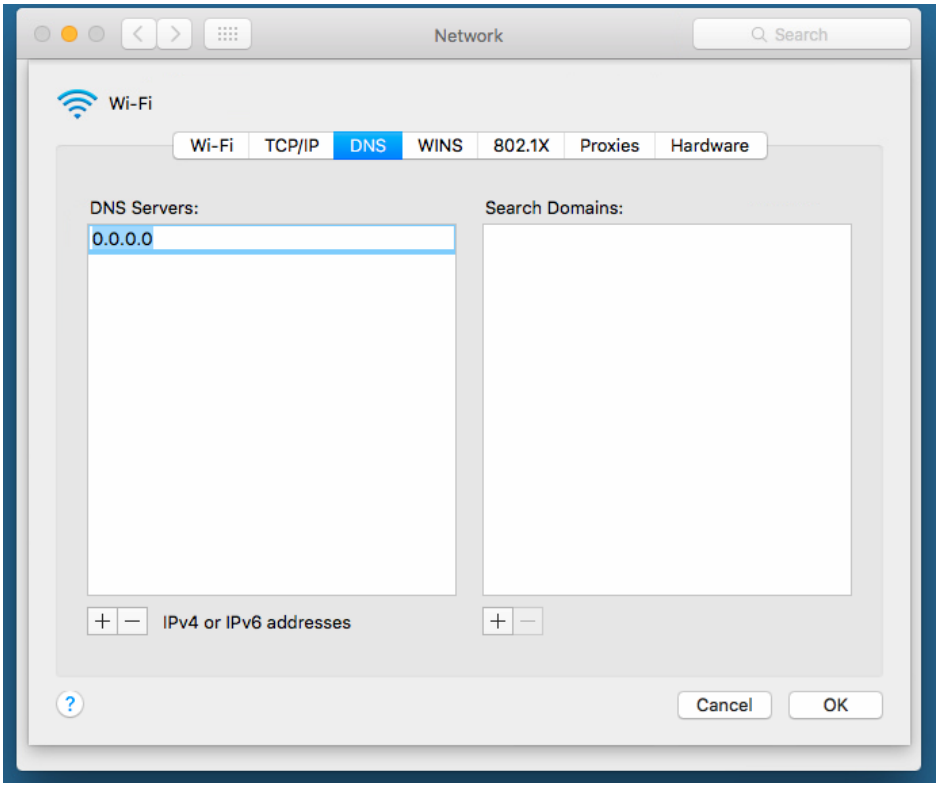
- Start > View Network Connections.
- Double click your current applicable Network adapter.
- Click on properties.
- Double click on “Internet Protocol Version 4 (TCP/IPv4)”.
- Where it state “obtain DNS servers automatically” please change this to “Use the following DNS server addresses”.
- **Note:** These steps are to be done on all DNS servers for your school.
- For the 2 DNS servers please enter your applicable DNS server provided to you by your Sales Engineer.





Standalone OSX

- Click the magnifying the glass at the top right corner.
- Type in “network” and select the network preferences.
- Select the current connection on the left.
- At the bottom click on “Advanced”.
- Then select DNS and then click the “+” at the bottom for “IPv4 or IPv6 address”.
- For the 2 DNS servers please enter your applicable DNS server provided to you by your Sales Engineer.



Standalone router

As each and every routers user interface and such are drastically different it would be almost impossible to detail instructions for how to do this portion. However the steps remain the same as the above, you would want to set the DNS to point only to Securly’s DNS servers provided to you by your sales engineer.