Securly's

DNS deployment best practices

A guide for schools

October 2019

Table of contents

Overview

This document will walk you through some important things to remember while deploying Securly DNS. Configuring Securly DNS filtering can be done in two different ways. It can be done at the device level where you change the device DNS to point directly to Securly's IPs. The second way is to modify your DNS servers' forwarders to point to Securly's IPs. Irrespective of which process you follow, the best practices mentioned in this document will help you ensure a successful web-filtering experience with Securly.

Deploying Securly DNS is a simple five-minute process that a Securly sales engineer can walk you through. You can also check out the steps for deploying Securly DNS here. You can also learn about the fundamentals of Securly's DNS architecture here.

Tip 1: Register your IP addresses with Securly

It is very important that Securly know what Public IP Addresses should be associated with your account to ensure that your users receive the filtering policy you customize for them. If you own more than one Public IP Address and did not go through a formal evaluation with a Sales Engineer, or if any of your IPs change it is highly recommended that you email support@securly.com with a list of what IP Addresses should be associated with your account.

If you do not register one or more of your Public IP Addresses with Securly and in-school internet traffic comes from one of them, your students will get either the Default policy of the Take-Home policy. The Take-Home policy is a type of customized policy that you can create to be applied specifically when students carry their school-owned devices home.

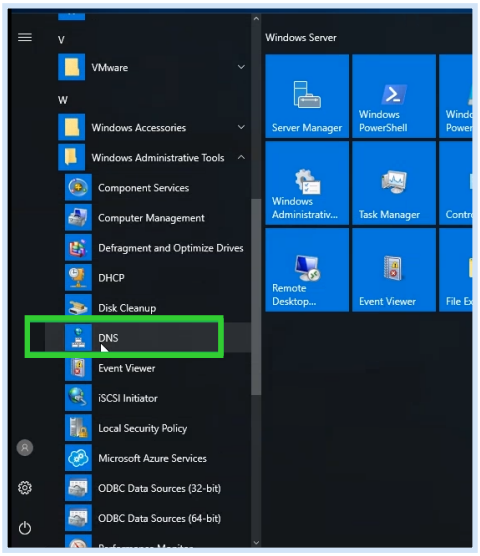
Additionally, if you have multiple internal DNS servers and one has traffic coming out of a registered IP and the other an unregistered IP, then you will experience split DNS. It is very likely that end-users will experience SSL Certificate errors on sites they shouldn't.

Tip 2: Disable IPv6

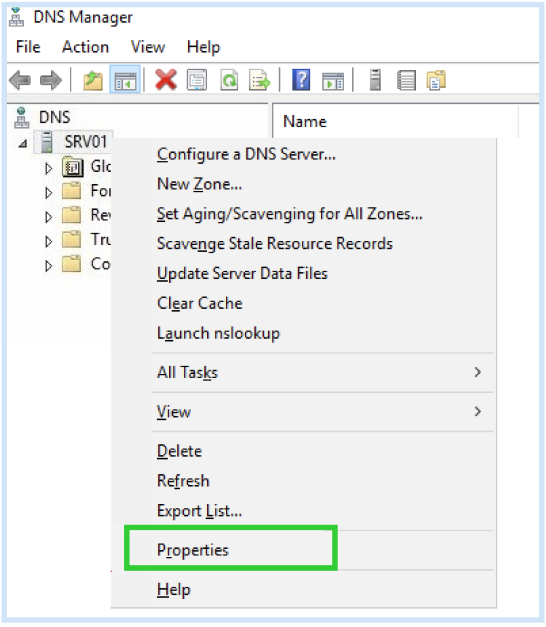
Securly currently does not support IPv6 and it is therefore recommended that you disable it. To learn what it means as a Securly user, click here.

To disable IPv6 for Windows server DNS follow the steps below:

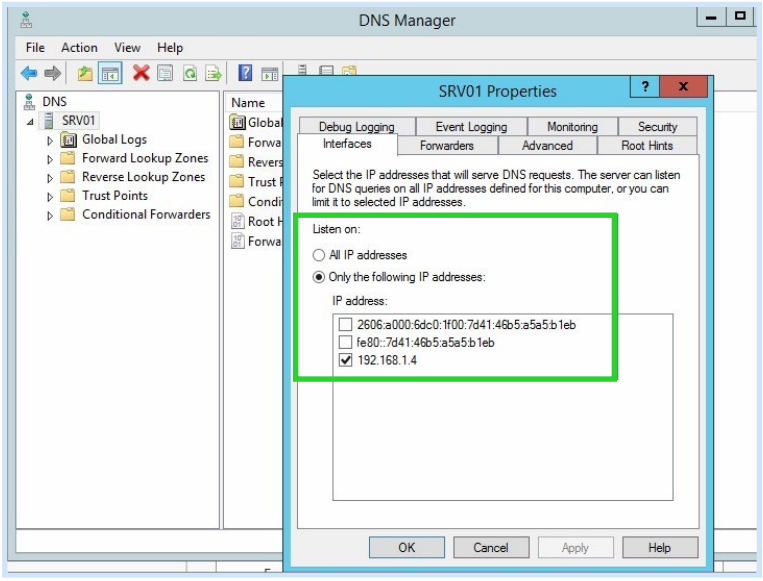
1. Navigate to Start > DNS Manager.



2. Expand out the DNS options.
3. Right-click the DNS server name and select properties.



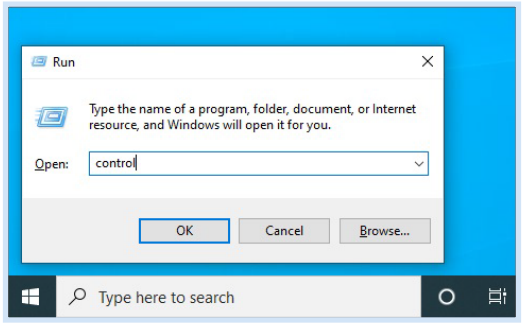
4. Under the "Listen On" field select the "Only the following IP addresses" radio button and uncheck any IPv6 address that is listed under it.



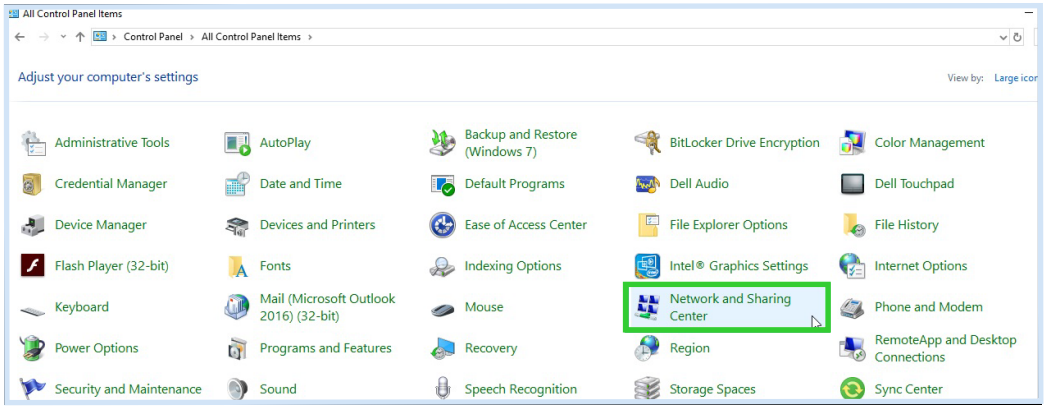
5. Click "Ok" to complete the process.

To disable IPv6 for Windows standalone DNS follow these steps:

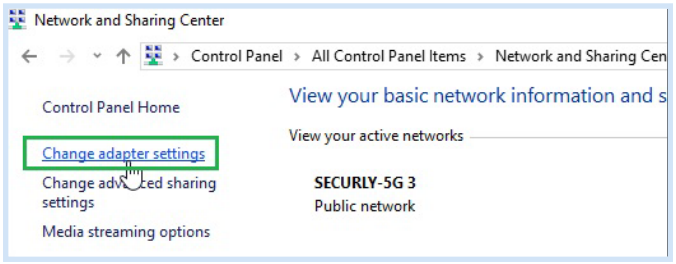
1. Right-click “Start” and select “Run” and type in “control.”



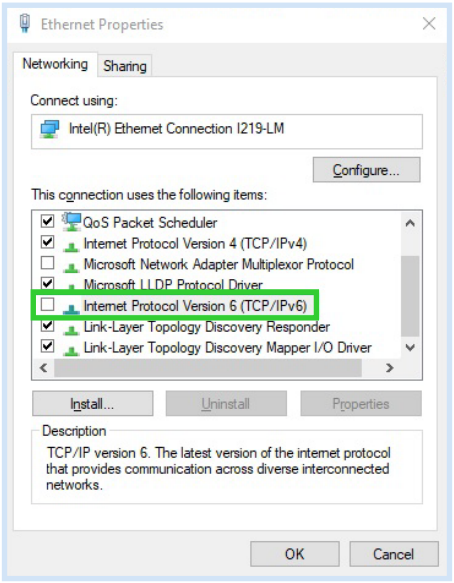
2. Open the control panel item "Network and Sharing Center."



3. Click “Change adapter settings.”



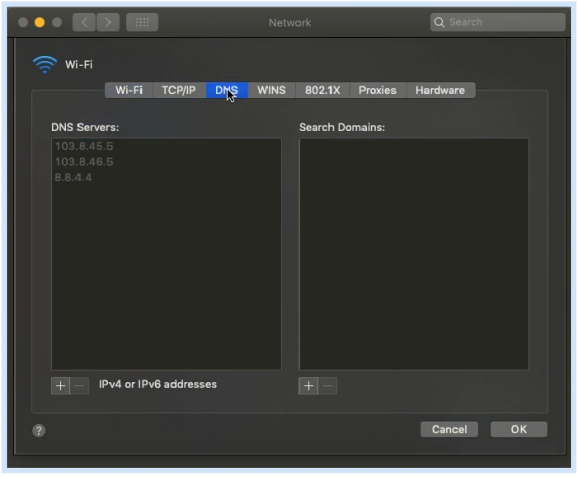
4. Double click on the network connections and go to “Properties.”



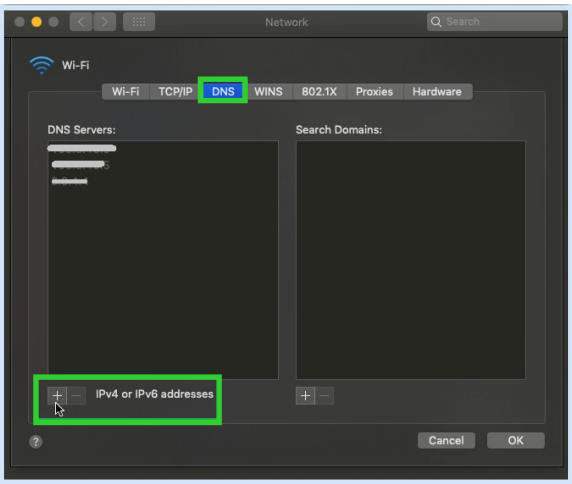
5. Uncheck the “Internet Protocol Version 6 (TCP/IPv6)” field.
6. Click “Ok” to complete the process.

To disable IPv6 for OSx DNS follow the steps below:

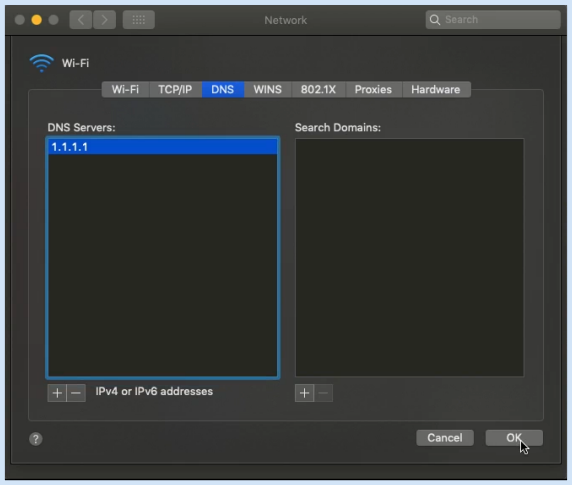
1. Click the magnifying the glass at the top right corner.



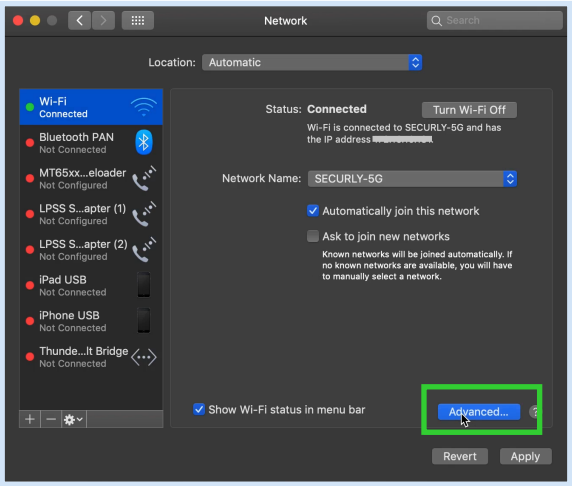
2. Type in “network” and select the network preferences.



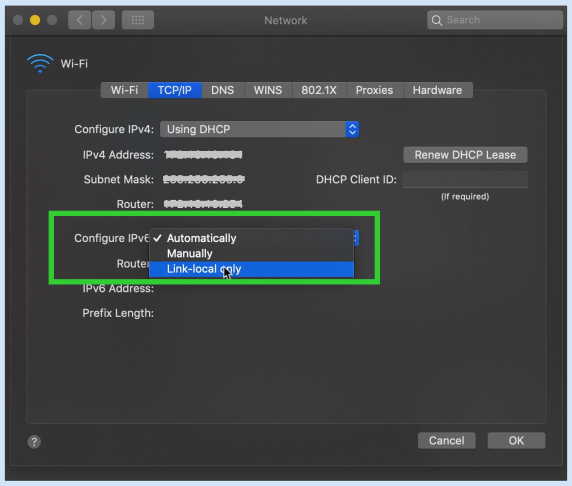
3. Select the current connection on the left.



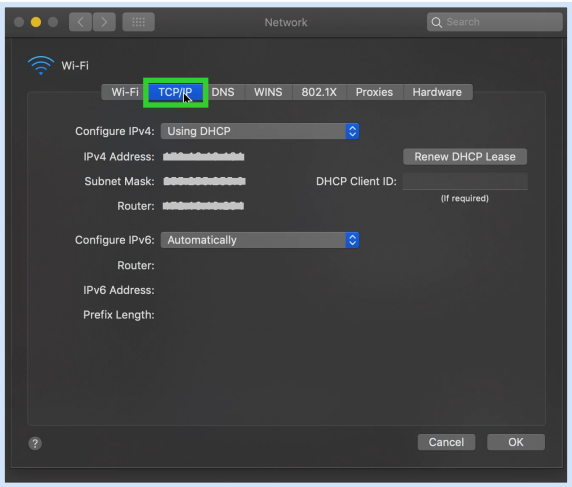
4. At the bottom click on "Advanced."



5. Click "TCP/IP."



6. Under "Configure IPv6" select "link-local only" in place of "Automatically."



7. Click "Ok" to complete the process.

Tip 3: Install Securly SSL certificates

The Securly SSL certificates help you ensure that your users get a seamless browsing experience and allow Securly to filter HTTPs sites properly. It is recommended that you install the certificate on all your devices. Visit this page to download the latest certificate. For detailed instructions about installing SSL certificates on different browsers and using specific MDMs, please refer to this page.

Tip 4: Lock firewall settings

Securly DNS can be configured by modifying your DNS servers' forwarders to point to Securly's IPs. By forwarding your DNS servers to Securly, device DNS settings can be changed by the end-user (especially on BYOD where users likely have admin privileges). This poses a problem as it would allow users to bypass filtering. It is therefore recommended that you implement certain firewall rules to prevent this easily discovered circumvention technique.

Firewall rules may change depending on the model and version of your Firewall. But here are some guidelines for the basic allow and deny rules for your Firewall to get you started.

	ACTION	SOURCE IP	SOURCE PORT	ORIGINAL DESTINATION IP	PROTOCOL	ORIGINAL DESTINATION PORT	TRANSLATED DESTINATION IP	TRANSLATED DESTINATION PORT	NOTES
RULE 01	Allow	Any	Any	Securly DNS Server IP Address	UDP	53	-	-	Allow Securly DNS Servers for all devices
RULE 02	Allow	Allow Any DNS Group	Any	Any	UDP	53	-	-	Internal DNS servers and Bypass devices
RULE 03	Allow	Any	Any	Any	UDP	53	Internal DNS or Securly DNS	53	Optional redirect DNS instead of deny
RULE 04	Deny	Any	Any	Any	UDP	80,443,5353	-	-	Optional Block Quic and DNS Crypt
RULE 05	Deny	Any	Any	Any	UDP+TCP	53	-	-	Block all other DNS

Understanding the Rules

Rule #1: This will allow any device on the network to use Securly DNS server. Each cluster has different DNS servers. Please check your deployment documentation or consult support@securly.com for more details.

Rule #2: This rule will allow some devices to access any DNS server. This is a good rule to have in place while planning on switching to Securly. Internal DNS server can be set to non-Securly DNS to "turn off" filtering.

Rule #3: This an optional rule. Some firewalls support the ability to change outbound requests to different DNS servers. It can be changed to force users to use Securly DNS IP. Another option is to force users to loop back and use the internal DNS server. This will help users that have their DNS setting statically set to other servers.

Rule #4: This an optional rule. This rule will help block Quic Protocol. DNScrypt is a new DNS service that runs on non-standard DNS ports. Blocking the additional ports is recommended.

Rule #5: It is important to block all other DNS requests to only allow the above rules. This is blocking both TCP and UDP traffic on port 53.

(Note that the Allow rules are only for UDP Port 53.)

Tip 5: Block browser settings

It is recommended that you lock down your browser settings so that users are unable to bypass filtering by making unauthorized changes to browser settings.