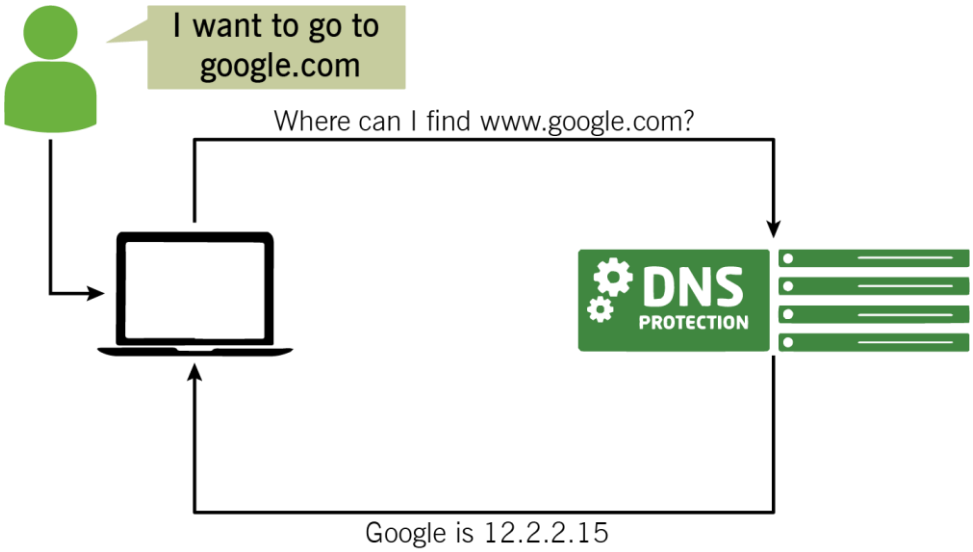
WEBROOT®

SecureAnywhere®
DNS Protection
Admin Guide

Table of Contents

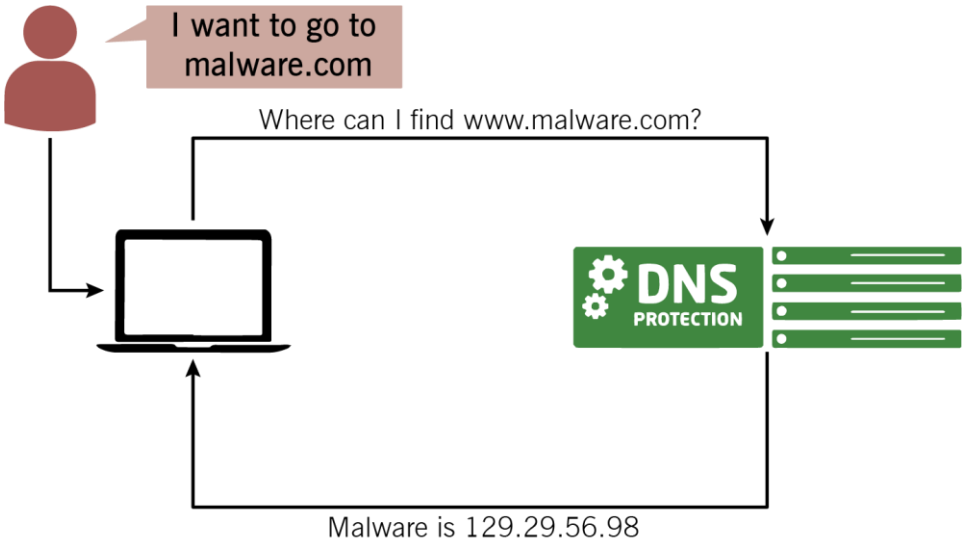
What Is DNS?

Domain Name System (DNS) is the Internet's equivalent of a phone book. It holds domain names, such as google.com, and when queried, provides information that includes a corresponding IP address. This allows your computer to find the desired site.



Why Is DNS-Based Web Security Needed?

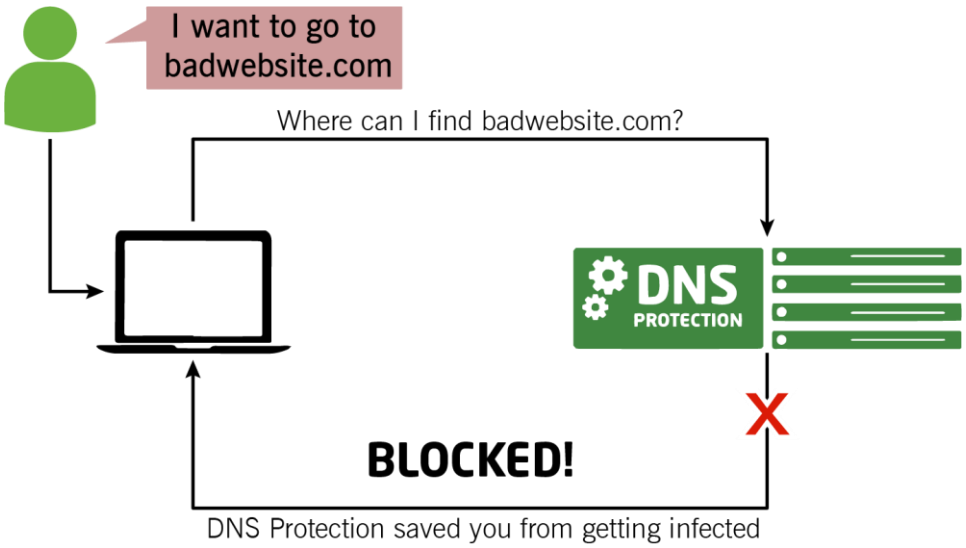
Generic DNS servers simply answer DNS requests, but have no way to differentiate between good and bad websites.



What Is Webroot SecureAnywhere DNS Protection?

Webroot SecureAnywhere DNS Protection is a cloud based security solution that proactively prevents communication between your network and web-based threats.

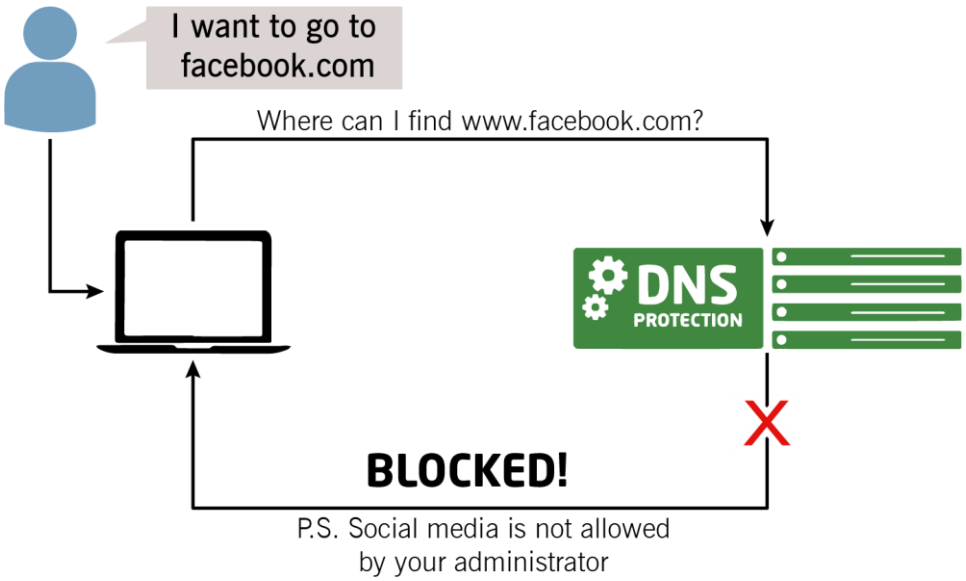
Customers who direct their DNS traffic to Webroot SecureAnywhere DNS Protection servers integrated with Webroot BrightCloud Threat Intelligence can monitor all DNS requests from clients to block responses for sites associated with Malware, Phishing, and Botnets, while allowing requests for safe sites to proceed. When a request for malicious site is made, the response is blocked.



Can I Use This For Content Filtering?

In addition to protecting against dangerous and fraud-based websites, SecureAnywhere DNS Protection service can also be used for policy management using web filtering categories such as Adult, Dating. Customers have the option to manage 80 plus categories using Webroot recommended templated policies or by creating custom policies to suit an organization's needs.

SecureAnywhere DNS Protection also maintains granular reporting on DNS requests along with category and blocking information for 90 days.



Webroot's Differentiators

SecureAnywhere DNS Protection Is Powered by BrightCloud Threat Intelligence

- Network level protection at the DNS layer.
- Trusted by leading Network and Security Vendors such as F5, Cisco, HP, and their customers.
- Largest and most accurate in terms of coverage and efficacy.

Single Management Console for Endpoint and SecureAnywhere DNS Protection

- Simplicity and ease of use.
- Single view of their deployments across multiple sites.
- Easy to use template based reporting.
- Manage both WSA-B and Webroot SecureAnywhere DNS Protection all from one GSM Portal—Single Pane of Glass!

FAQs

Is this part of WSA Business?

SecureAnywhere DNS Protection is planned to be sold as an add-on to WSAB, as well as a stand-alone.

What is the primary purpose of SecureAnywhere DNS Protection?

SecureAnywhere DNS Protection protects networks from malicious domains and inappropriate websites by filtering DNS requests, helping users be secure in a connected world.

What reporting capabilities are available?

A full audit trail of all DNS requests from each site is available for up to 90 days. This includes reporting on the different policy categories as well as what has been blocked and allowed.

Setting Up Webroot SecureAnywhere DNS Protection

The following describes how to set up Webroot SecureAnywhere DNS Protection.

Determining the External IP Address

- On the networks that will be using DNS Protection, identify the public IPv4 address used for internet access (WAN IP). An internet search of My IP generally reveals the appropriate IP address.
- These addresses will need to be entered in order for DNS Protection to answer DNS requests, and for logging and filtering to be provided.
- If the network is using a dynamically provided address, the IP address may change if you reboot your router or if your ISP, such as Comcast, Century Link, etc., makes changes. If this happens, you must look up the newly assigned address and update the entry.
- IPv6 is not yet supported.

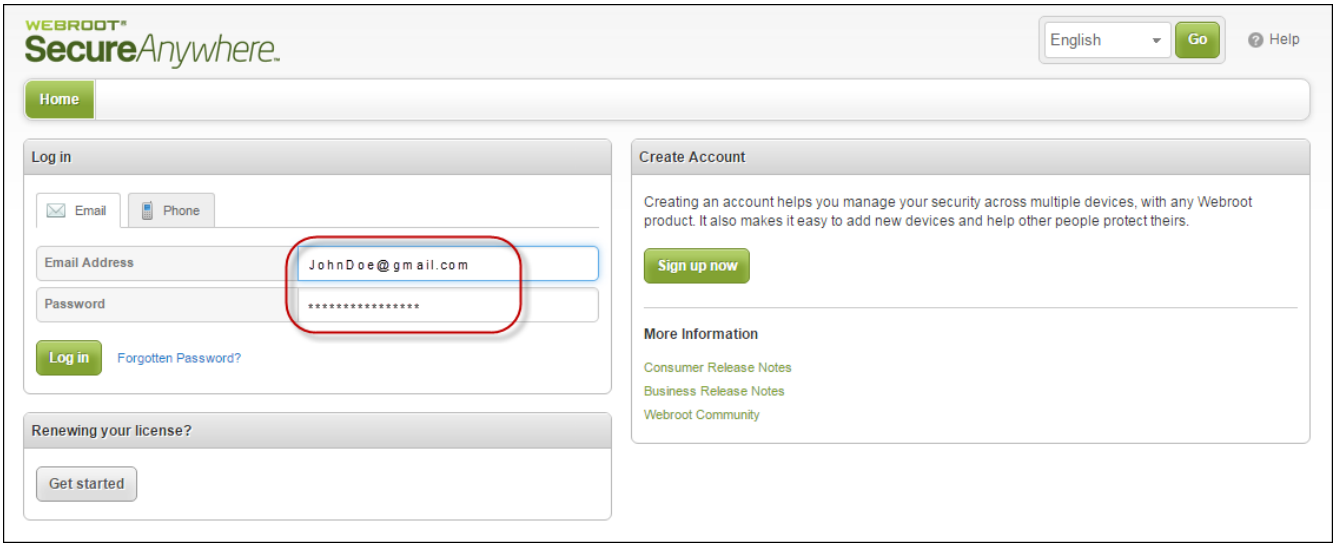
Setup Information

To set up SecureAnywhere DNS Protection:

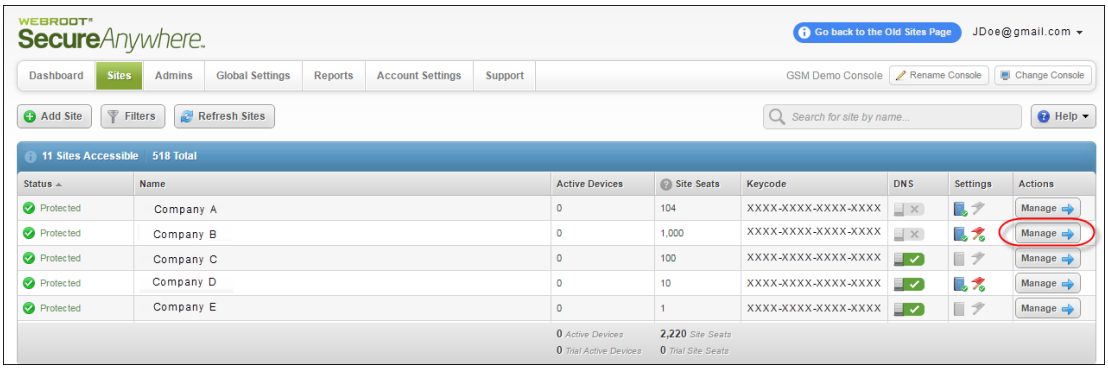
1. Go to the GSM console:

   https://my.webrootanywhere.com/

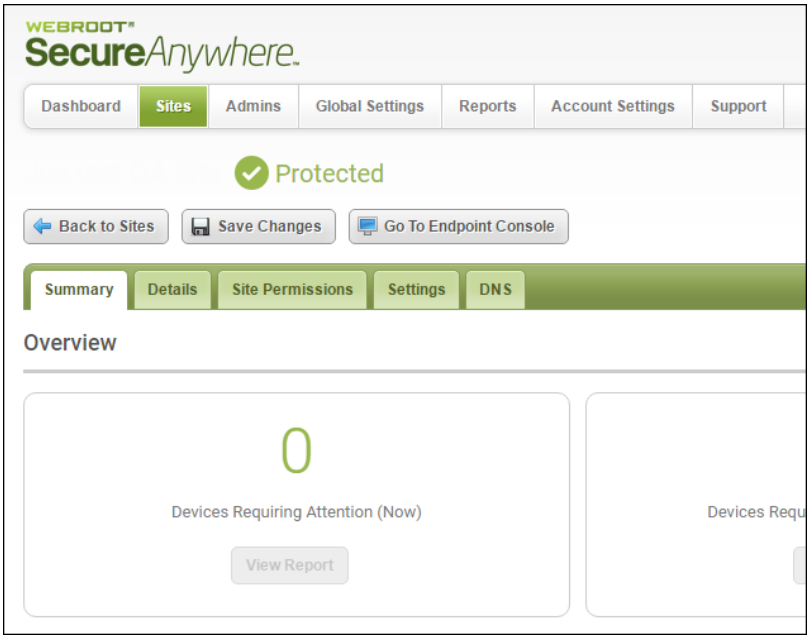
2. Log in, using the credentials provided.



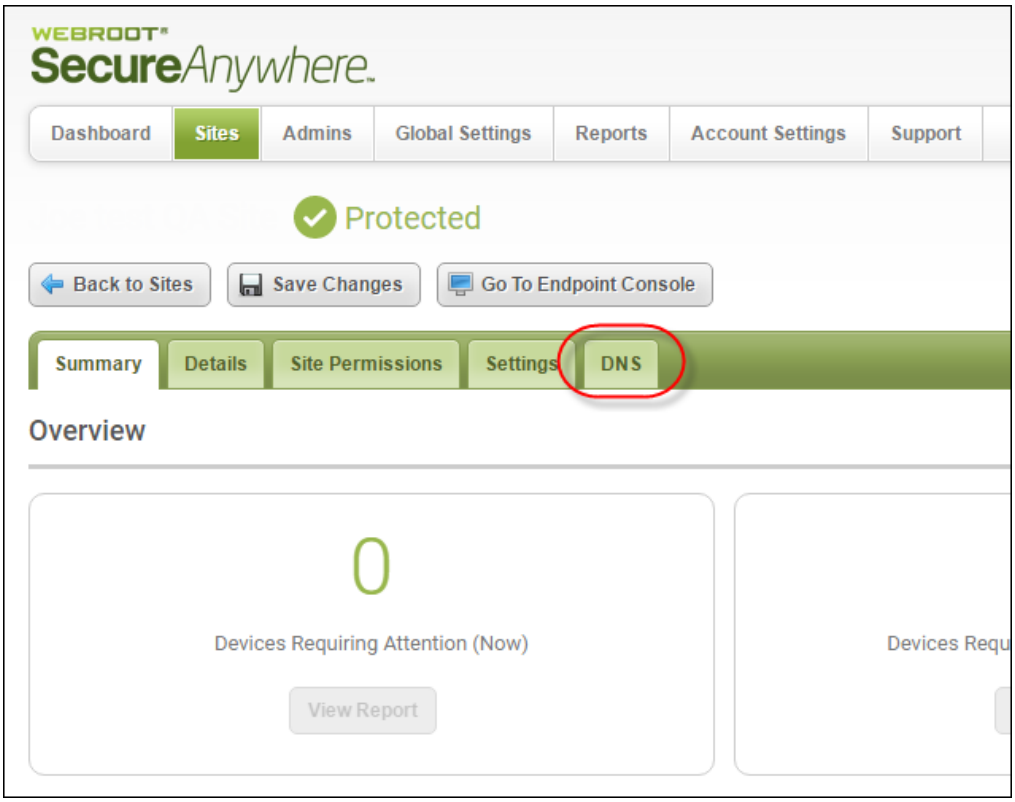
3. Webroot SecureAnywhere DNS Protection can be enabled on a per site basis by clicking the **Manage** button on the far right of the Sites tab.



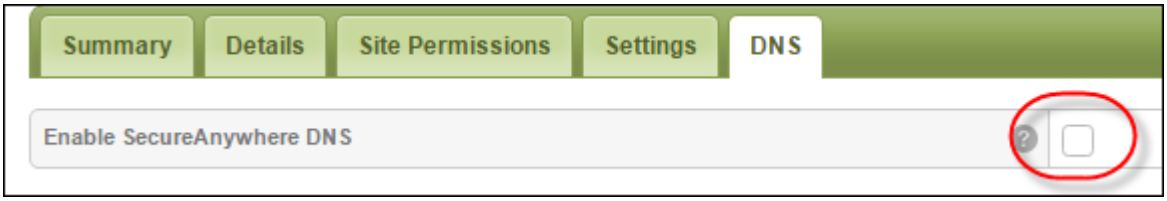
The Summary panel displays.



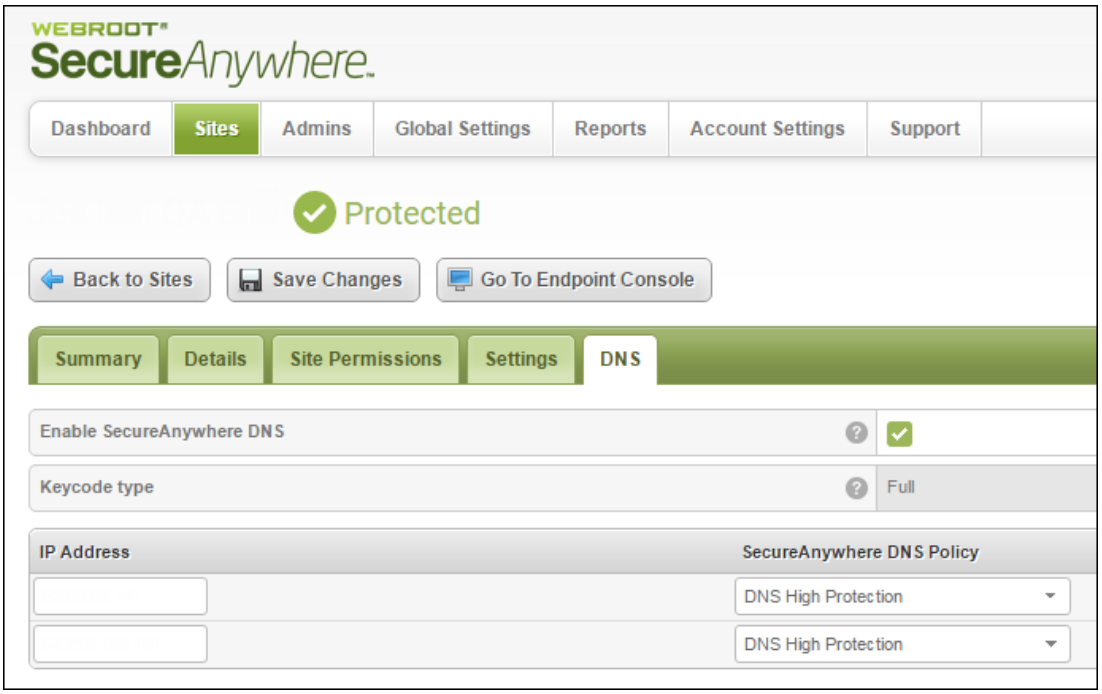
4. Select the **DNS** tab.



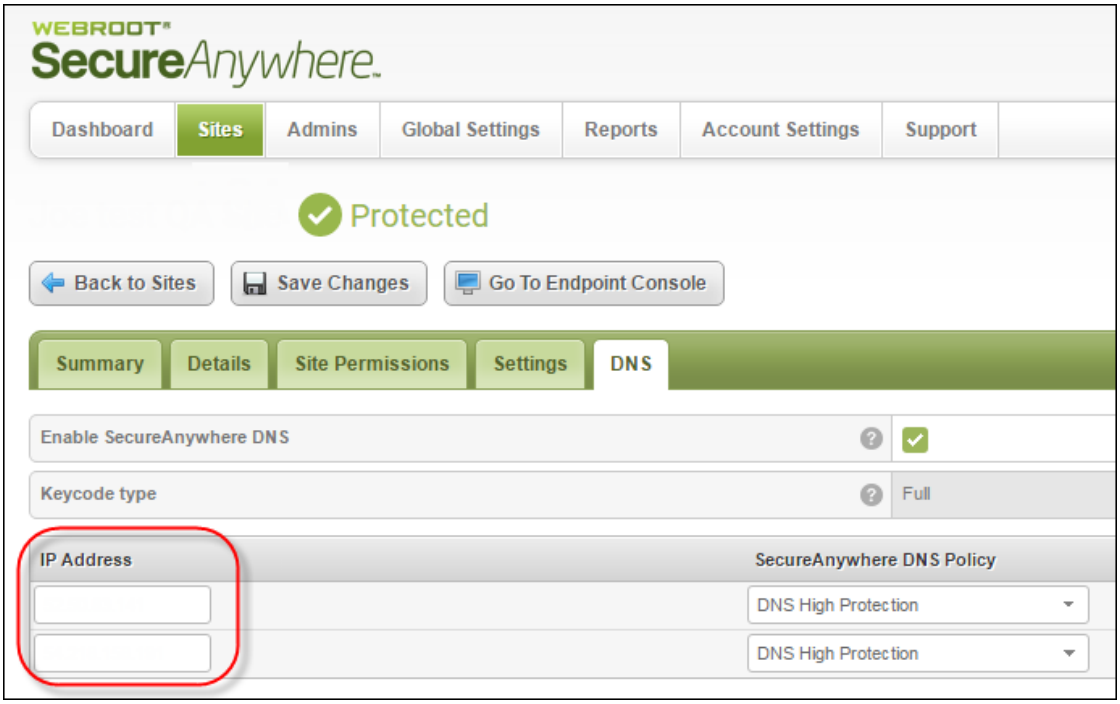
5. Enable/disable Webroot SecureAnywhere DNS Protection by selecting the **Enable SecureAnywhere DNS** checkbox.



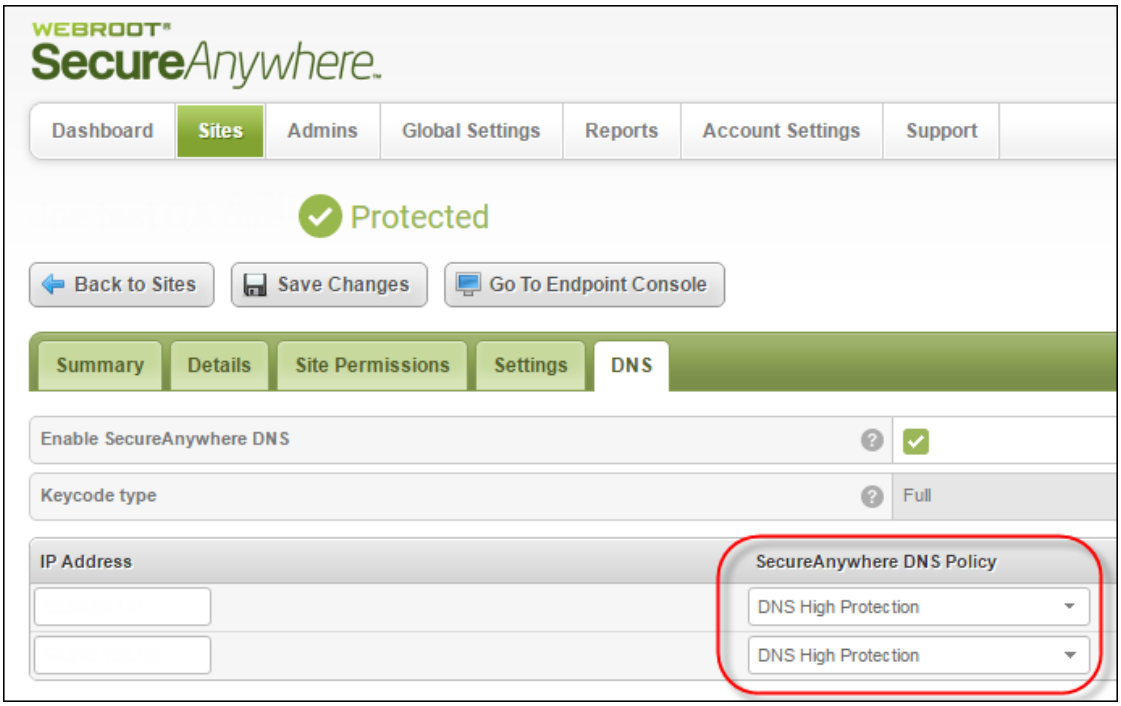
The DNS tab expands.



6. In the IP Address column, add or remove IP addresses, as needed.



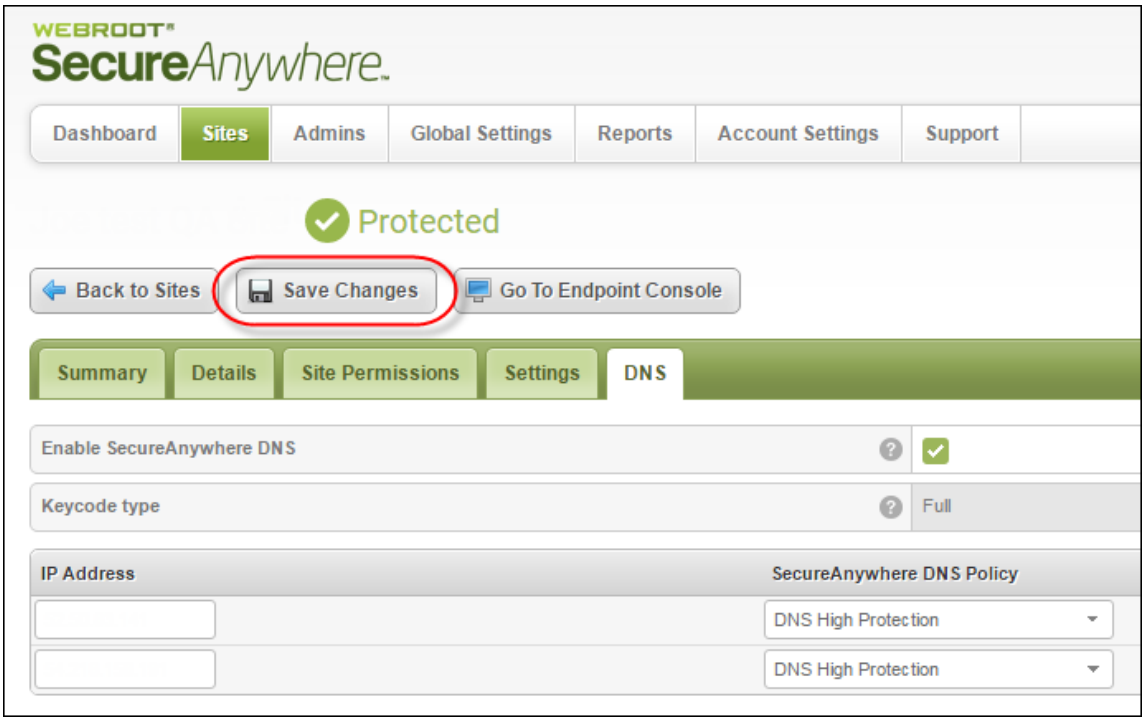
7. From the SecureAnywhere DNS Policy drop-down menu, select a policy for that particular IP address.



A default policy is automatically applied to the IP when created. You will also have the ability to choose a separate policy, if the default is not desired. The service is pre-loaded with two template policies:

- **SecureAnywhere DNS High Protection** – The High Protection policy builds on Medium Policy, but also adds additional filters, blocking categories such as gambling and hacking. Access to Security, Parental Controls and Questionable (Cheating, Cult, etc.) sites is restricted.
- **SecureAnywhere DNS Medium Protection** – The Medium Protection Policy includes all Security Risks and adds filtering for categories that may not be appropriate for the workplace. Access to Security and Parental Controls (Adult, Nude, Porn, etc.) sites is restricted.

8. When you're done, click the **Save Changes** button to apply the policy.



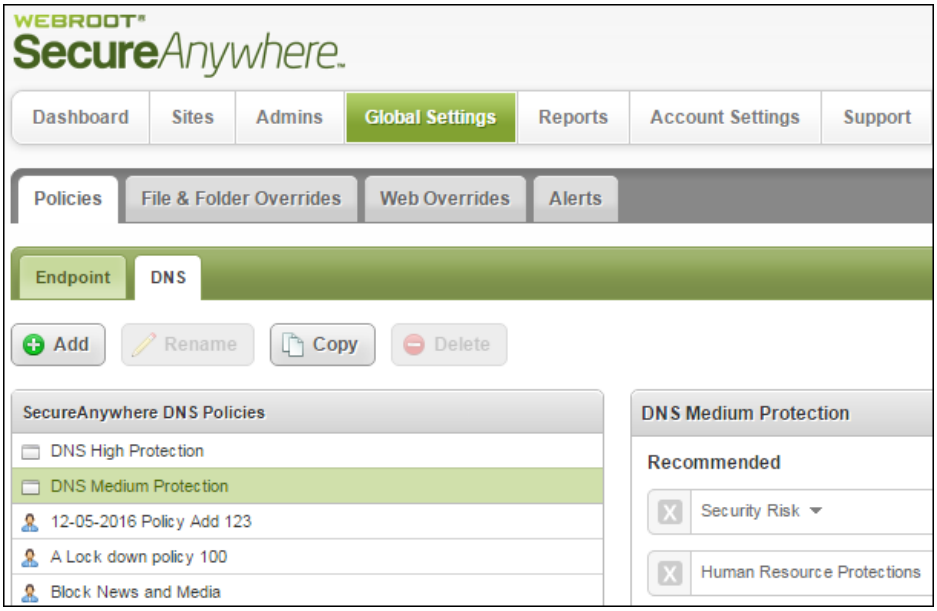
Defining Policies

Policies for DNS Protection are managed under the Global Settings tab of the GSM console. Here you will find that policies are broken out into two tabs:

- Endpoint
- DNS

As with Endpoint policies, functional static policies are provided.

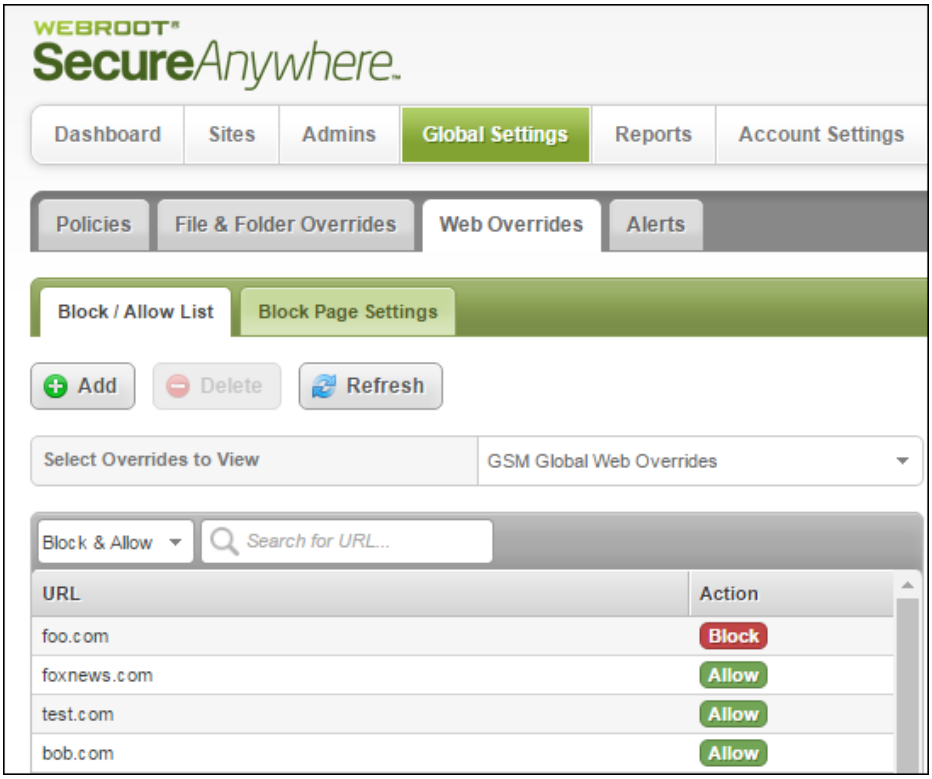
- The Medium Protection Policy includes all Security Risks and adds filtering for categories that may not be appropriate for the workplace.
- The High Protection policy builds on Medium Policy, but also adds additional filters, blocking categories such as gambling and hacking.
- To create custom polices, click the **Add** button, and create a new policy, or click the **Copy** button to create a new policy from an existing one.



Web Overrides

Web Overrides and the Block Page configuration are managed under the Web Overrides tab. These are broken out into two sub tabs.

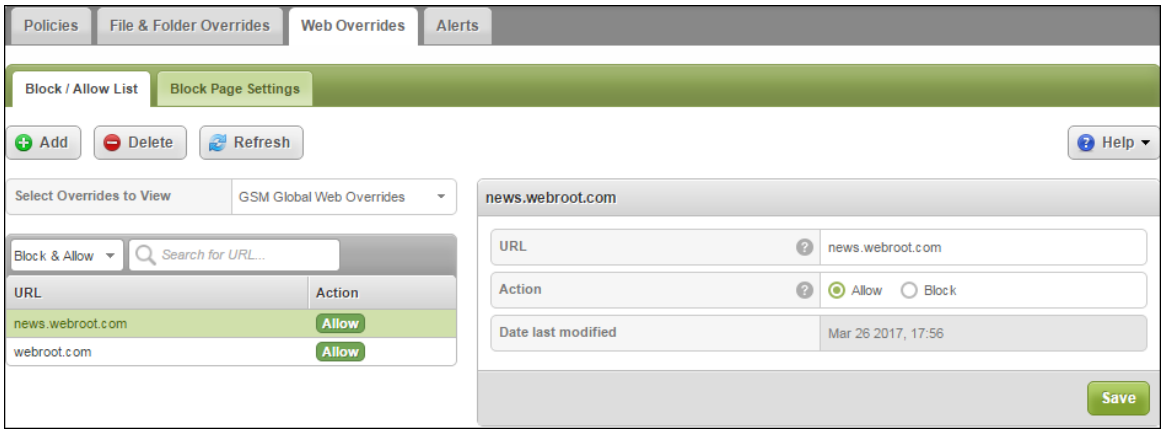
- Block / Allow List
- Block Page Settings



Block / Allow List

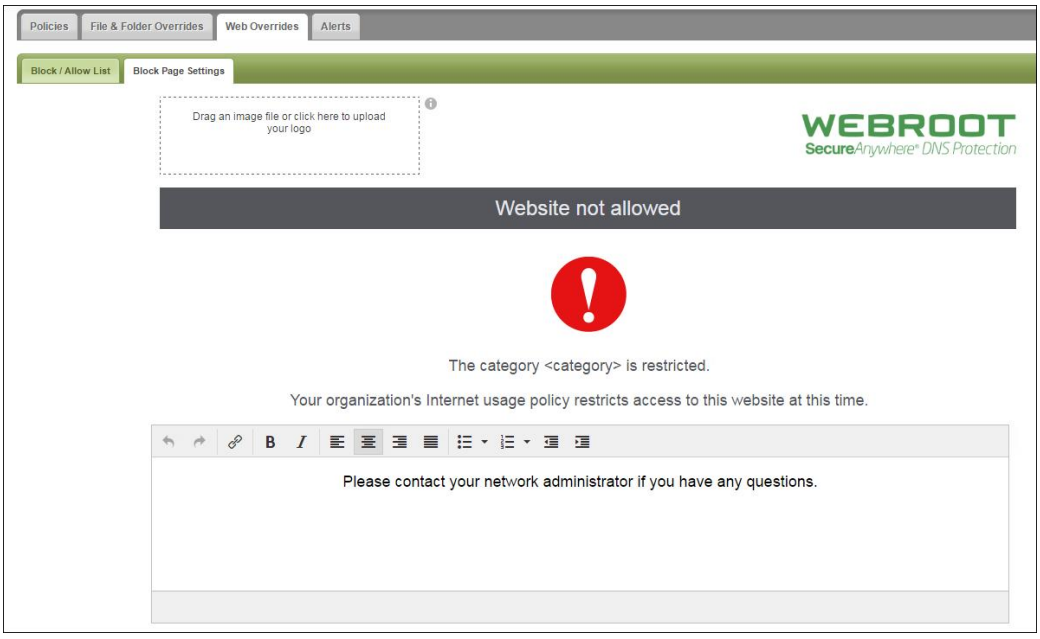
Under the Block / Allow List tab, custom entries can be added to augment the DNS Protection policies. This is done by adding the specific domain or subdomain, assigning an action, and then associating it with a specific site or to all sites by using the GSM Global Overrides selection.

Note that this entry is specific to the domain or subdomain entered. For example, allowing webroot.com does not cover news.webroot.com. In order to control access to news.webroot.com, a separate entry is required.



Block Page Settings

- The Block Page can be customized for each GSM console; allowing the user to be provided with more information alongside the standard Webroot messaging to include a logo as well as custom text.
- The image size is restricted to 1 MB.
- The Content field can be used for custom text such as telephone numbers, websites, and links. For example, you could enter information such as *Please contact your network administrator if you have any questions,* and then include the contact method of your choice.



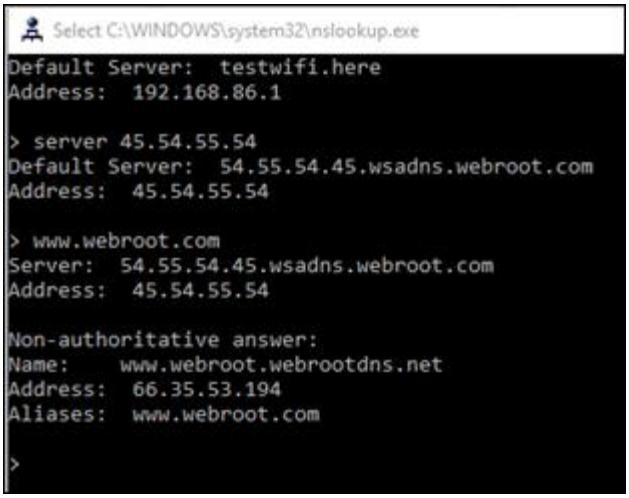
Testing DNS Functionality

Once the IP addresses and the policies have been configured, it needs to be confirmed that the servers are responding with appropriate information. This can be done from an endpoint on the network to be protected.

To test DNS functionality:

1. Open a command prompt.
2. Run NSLookup.
3. Set the server to 45.54.55.54.
4. Check several sites to confirm valid responses.

   A successful test looks like the following:



Installing Certificates

Certificates need to be installed to avoid browser errors when https websites are blocked. Although skipping this step will not stop filtering, it does avoid certificate errors when an https site is redirected. Certificates can be downloaded from behind a registered IP address: http://45.54.55.55/download

The certificate needs to be installed to Trusted Root Certification Authorities. This can be done on individual systems or, depending on your environment, pushed out automatically.

To install a certificate:

1. Click **Start**, click **Start Search**.
2. In the Search field, type **mmc**, and then press **Enter**.
3. From the File menu, select **Add/Remove Snap-in**.
4. Under Available snap-ins, click **Certificates**, and then click **Add**.
5. Under This snap-in will always manage certificates for, click **Computer account**, and then click **Next**.
6. Click **Local computer**, then click **Finish** then **OK.**
7. In the console tree, double-click **Certificates**.
8. Right-click **Trusted Root Certification Authorities**.
9. Click **Import to import the certificates** and follow the steps in the Certificate Import Wizard to add the P7B certificate.

Configuring the Network

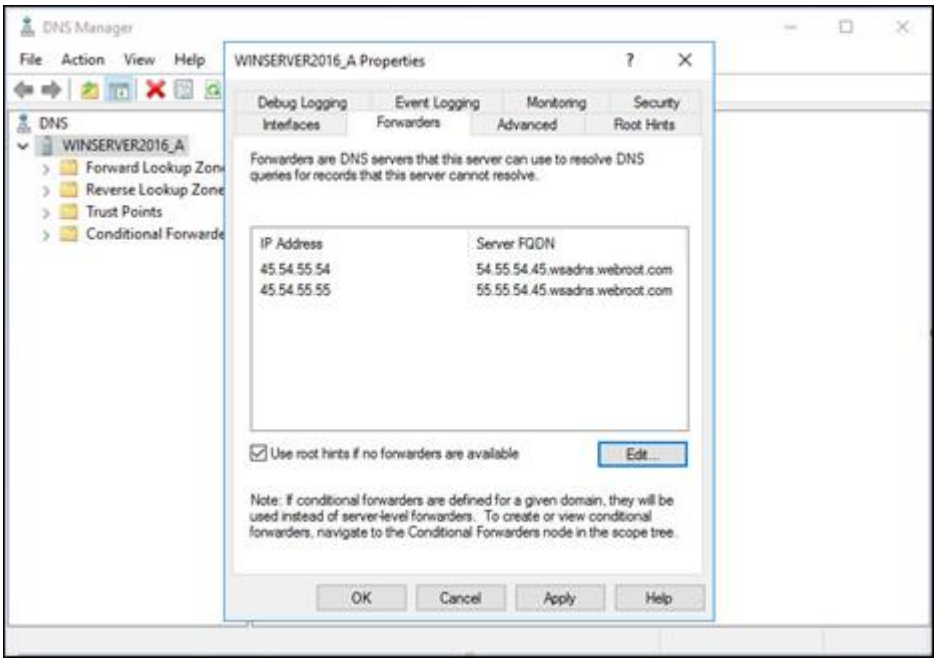
Set the DNS forwarders, in the case of AD, or appropriate router to forward DNS requests to the Webroot SecureAnywhere DNS Protections servers.

To configure a DNS server to use forwarders using the Windows interface:

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server.
3. On the Action menu, click Properties.
4. On the Forwarders tab, under DNS domain, select a domain name.
5. Under Selected domain's forwarder IP address list, type the IP address of a forwarder, and then click **Add**.

   For more information, you can view the full article here.

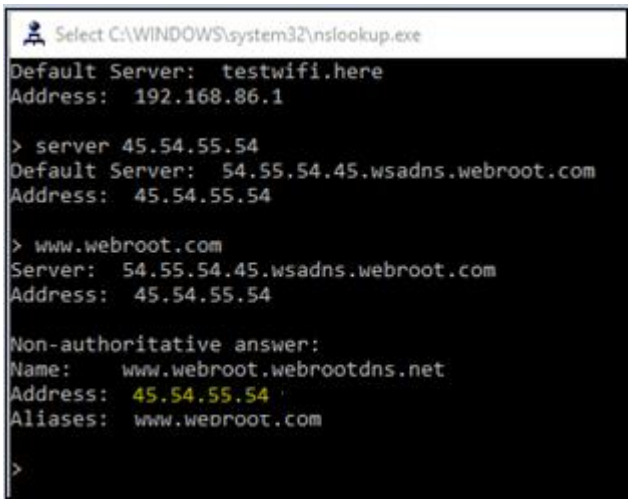
   - DNS1: 45.54.55.54
   - DNS2: 45.54.55.55



Testing DNS Filtering

Testing can be done via NSlookup from a system behind a protected IP address. By asking the server to lookup a known blocked page, instead of receiving the actual IP address, the block page IP will be provided. Alternately, the cache can be flushed from both the server and the workstation, and then the blocked website can be loaded in a browser.

Block Page Returned

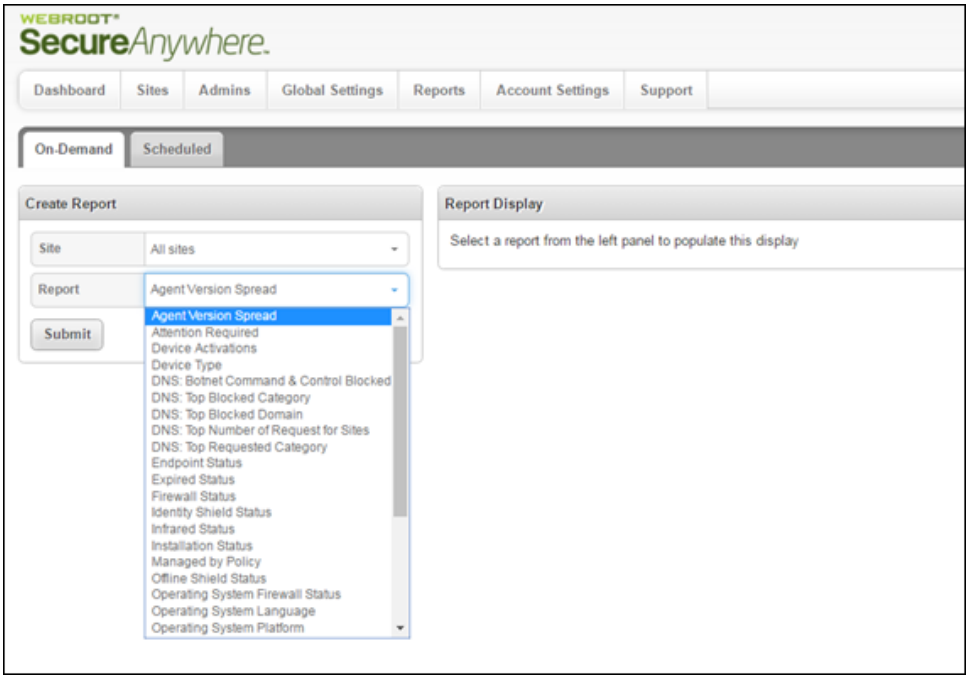


Browser Test

- Flush existing DNS cache – command prompt: ipconfig /flushdns.
- Using a web browser, confirm the internet is available by browsing to an unfiltered site.
- Test the filtering by opening a blocked https site such as https://www.webroot.com when running a policy with the Business / Government / Services selected.

  In this instance, your custom Block Page should display without certificate errors. If you see a certificate error, review the Installing Certificates section of this document.

- SecureAnywhere DNS Protection provides Dashboard, On-Demand, and Scheduled Reporting. This can be accessed by navigating to **Reports Tab**. For more information, see *Generating On-Demand Reports*.



Appendix

Setting Up Your Router to Use Webroot SecureAnywhere DNS Protection

Changing the DNS server settings on your router isn't that difficult, but every manufacturer uses their own custom interface, meaning the process can be very different depending on the router you own.

Linksys

1. Sign in to your Linksys router's web-based administration, usually http://192.168.1.1.
2. From the top menu, tap or click **Setup**.
3. From the Setup submenu, tap or click **Basic Setup**.
4. In the Static DNS 1, enter the primary DNS server you'd like to use.
5. In the Static DNS 2 field, enter the secondary DNS server you'd like to use.
6. The Static DNS 3 field can be left blank, or you can add a primary DNS server from another provider.
7. At the bottom of the screen, tap or click the **Save Settings** button.
8. On the next screen, tap or click the **Continue** button.

NETGEAR

1. Sign in to your NETGEAR router manager page, most often via http://192.168.1.1 or http://192.168.0.1.
2. NETGEAR has two major interfaces with different ways of performing the next step:
   - If you have a Basic and Advanced tab along the top, select the **Basic** tab followed by selecting the **Internet** option on the left.
   - If you don't have those two tabs along the top, select **Basic Settings**.
3. Under the Domain Name Server (DNS) Address section, select **Use These DNS Servers**.
4. In the Primary DNS field, enter the primary DNS server you'd like to use.
5. In the Secondary DNS field, use the secondary DNS server you'd like to use.
6. If your NETGEAR router gives you a Third DNS field, you can leave it blank or choose a primary DNS server from another provider.
7. Tap or click **Apply** to save the DNS server changes you just entered.
8. Follow any additional prompts about restarting your router. If you don't get any additional prompts, your changes should be now be live.

D-Link

1. Sign in to your D-Link router using http://192.168.1.1.
2. On the left side of the page, select the Internet option.
3. From the top of the page, select the **Setup** menu.
4. Find the Dynamic IP (DHCP) Internet Connection Type section, and in the Primary DNS Address field, enter the primary DNS server you want to use.
5. In the Secondary DNS Address field, enter the secondary DNS server you want to use.
6. At the top of the page, click the **Save Settings** button.
7. The DNS server settings should have changed instantly, but you may be told to reboot the router to complete the changes.

Asus

1. Sign in to your ASUS router's admin page with this address: http://192.168.1.1.
2. From the menu to the left, click or tap **WAN**.
3. At the top of the page, to the right, click the **Internet Connection** tab.
4. In the DNS Server1 field, under the WAN DNS Setting section, enter the primary DNS server you want to use.
5. In the DNS Server2 field, enter the secondary DNS server you want to use
6. Click the **Apply** button at the bottom of the page to save the changes.

TP-Link

1. Sign in to your TP-LINK router's configuration page, usually via the http://192.168.1.1 address, but sometimes via http//192.168.0.1.
2. From the menu on the left, select the **DHCP** option.
3. Tap or click the DHCP submenu option called **DHCP Settings**.
4. In the Primary DNS field, enter the primary DNS server you'd like to use.
5. In the Secondary DNS field, enter the secondary DNS server you'd like to use.
6. Click the **Save** button at the bottom of the page to save the changes.

Cisco

1. Sign in to your Cisco router from either http://192.168.1.1 or http://192.168.1.254, depending on your router model.
2. Click or tap the **Setup** option from the menu at the very top of the page.
3. Click the **LAN Setup** tab from the menu that's just below the Setup option.
4. In the LAN 1 Static DNS 1 field, enter the primary DNS server you'd like to use.
5. In the LAN 1 Static DNS 2 field, select the secondary DNS server you'd like to use.
6. Some Cisco routers may have a LAN 1 Static DNS 3 field, which you can leave blank, or enter yet another DNS server.
7. Save the changes clicking the **Save Settings** button at the bottom of page.

Belkin

1. Sign in to your Belkin router through the address http://192.168.2.1.
2. Select **DNS** under the Internet WAN section from the menu on the left.
3. In the DNS Address field, enter the primary DNS server you'd like to use.
4. In the Secondary DNS Address field, use the secondary DNS server you'd like to use.
5. Click or tap the **Apply Changes** button to save the changes.
6. You may be told to restart your router for the changes to take effect. If told to do so, simply follow the on-screen prompts.