DNS Protection Guest WiFi
Getting Started Guide

Copyright

DNS Protection Guest WiFi Getting Started Guide

Table of Contents

Chapter 1: DNS Protection Guest WiFi Getting Started Guide

To use the DNS Protection Guest WiFi Getting Started Guide, see the following topics:

DNS Protection Guest WiFi Overview

This document is designed as a guide for deploying and using Webroot SecureAnywhere DNS Protection for Guest Wi-Fi. It is intended as a technical resource for network administrators and those who will be configuring or managing DNS Protection.

DNS Protection for Guest Wi-Fi can be quickly configured and managed through the Webroot console. It allows for easy deployment and scalability, whether configuring a single Access Point or deploying a standard configuration to thousands of networks.

The configuration process includes five steps:

- *Defining a Filtering Policy on page 3*
- *Enabling DNS Protection on page 4*
- *Registering the WAN IP Address*
- *Configuring the Guest WiFi Network on page 5*
- *Reporting on page 7*

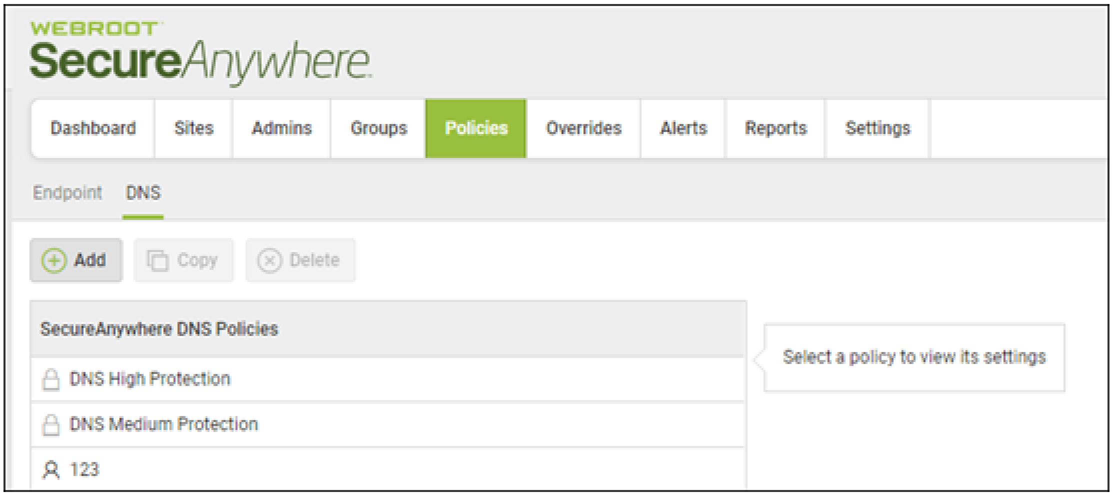
Defining a Filtering Policy

There are 80 categories that can be selected in a filtering policy. These categories range from Security Risks, which includes categories that should always be filtered, such as Malware and Phishing Sites, to categories that may need to be filtered based on appropriate content for the network, such as Peer to Peer or Streaming. One policy can be used for every site or a separate policy can be used for each network or circuit.

The DNS Policies are configured under **Policies** > **DNS**.

To create custom polices:

1. Do either of the following:
   - Click the **Add** button and create a new policy.
   - Click the **Copy** button to create a new policy from an existing one.
2. Select the categories you want to have filtered.
3. When you're done, click **Save**.



SecureAnywhere DNS Policies

DNS High Protection

DNS Medium Protection

123

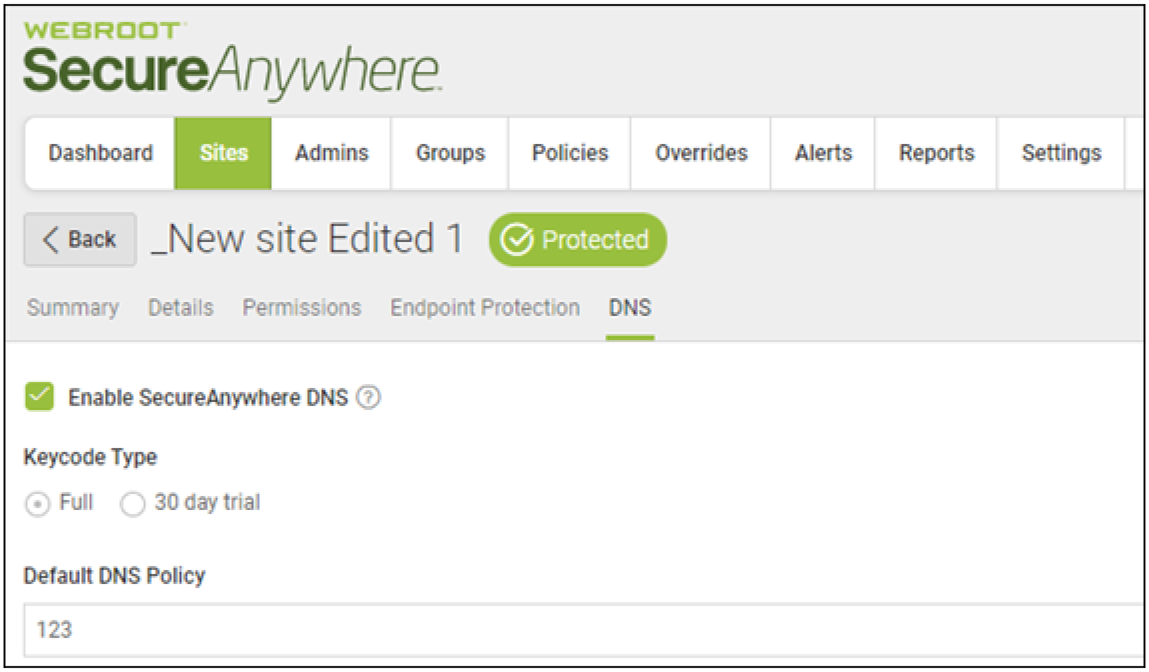
Select a policy to view its settings

Enabling DNS Protection

To manage DNS Protection, there must be a site for the Guest Wi-Fi network. This can be an existing site or, if a new network, a site can be created specifically for the Wi-Fi network. DNS Protection for the Site is then configured by clicking the **Manage** button next to the site and navigating to the DNS tab.

Once the **Enable SecureAnywhere DNS** checkbox is selected, there is an option to select whether to initiate a 30 day trial or whether the site is immediately fully licensed.

Note that once the trial expires, DNS Protection will stop working for the Site until set to Full – this does not happen automatically upon the expiration of the trial.



☑ Enable SecureAnywhere DNS

Keycode Type

● Full ○ 30 day trial

Default DNS Policy

123

Configuring the Guest WiFi Network

Once a policy has been defined and a WAN IP registered, the Guest Wi-Fi network can be configured to use DNS Protection.

There are two steps to complete the configuration:

- Test DNS Resolution
- Configure DNS

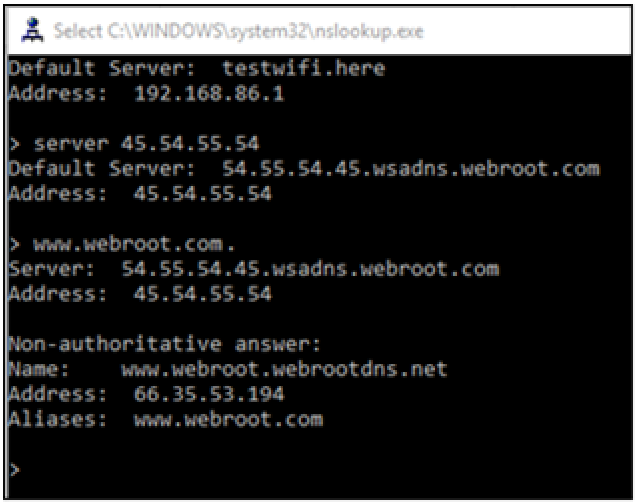
Testing DNS Resolution

It is important to test before forwarding DNS requests to the DNS Protection servers. This verifies that the WAN IP address entered is correct, while also confirming the service is performing as expected.

To test DNS resolution:

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:



```
Default Server:  testwifi.here
Address:  192.168.86.1

> server 45.54.55.54
Default Server:  54.55.54.45.wsadns.webroot.com
Address:  45.54.55.54

> www.webroot.com.
Server:  54.55.54.45.wsadns.webroot.com
Address:  45.54.55.54

Non-authoritative answer:
Name:    www.webroot.webrootdns.net
Address:  66.35.53.194
Aliases:  www.webroot.com

>
```

If the NSLookup times out, check that you have registered the correct WAN IP address. For more information regarding WAN IP Addresses, see the DNS Protection Admin Guide.

Configuring DNS

Once DNS has been successfully tested, all DNS requests for the Guest Wi-Fi network can be forwarded to the DNS Protection servers. The DNS Protection Servers for Wi-Fi are:

- 45.54.55.54
- 45.54.55.55

The DNS settings for the Router or Access Point should look as follows:

- DNS1: 45.54.55.54
- DNS2: 45.54.55.55
- DNS3: Failover DNS Server (Provided by ISP)

In the case of a DNS server, the DNS Protection Servers should be configured as Forwarders. Alternately, DHCP can be used to pass the DNS settings directly to each connected device.

Note that the only time the third DNS server should answer is if both the Primary and Secondary fail to do so. This setting is optional.

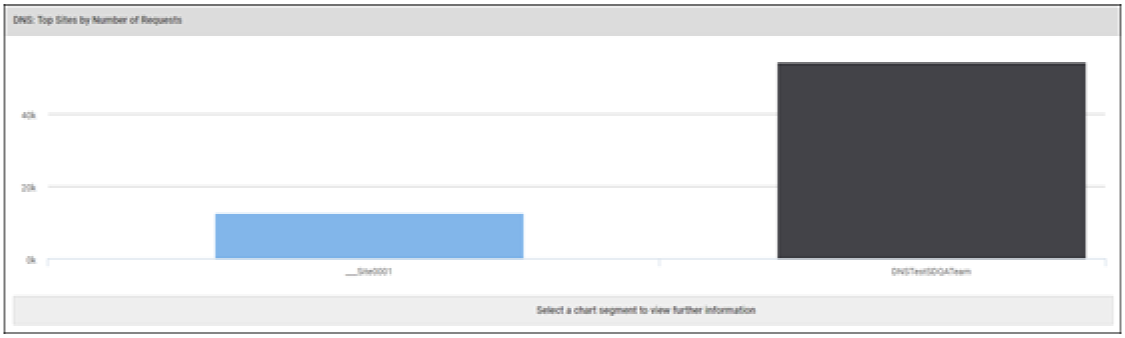
To test DNS Protection is working correctly, simply connect a device to the Guest Wi-Fi network. The internet should function as per normal. If, however, a prohibited site is requested, the Webroot Block page should appear. Note that communication on this Block Page can be customized under Global Settings, Web Overrides, and Block Page Settings.

Reporting

Once everything is set up, the DNS requests on the Guest Wi-Fi networks can be reviewed. If there are no active DNS requests being made, it is possible that all DNS requests are falling through to the failover DNS server or DNS is not configured correctly.

Additionally, through the reports, it is possible to see how a circuit is being used. There are six on-demand and scheduled reports available under the Reports tab to help identify the different characteristics of the internet traffic. The number of DNS requests by day can be found under the DNS: Top Sites by Number of Requests report.

For more information on reporting, see the DNS Protection Admin Guide.


DNS: Top Sites by Number of Requests
40k
20k
0k
__Site0001
DNSTestSDQATeam
Select a chart segment to view further information

Chapter 2: DNS Protection Guest WiFi Support

For information about support, see the following topic:

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledgebase.
- Look for the answer in our online documentation.
- Enter a help ticket .
- Connect to the Webroot Online Business Forum.

Index