SonicOS 7.1

DNS Security

Administration Guide

Contents

1

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on how to configure the DNS settings, Dynamic DNS, and DNS Proxy settings on the SonicWall security appliances.

Topics:

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTPPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

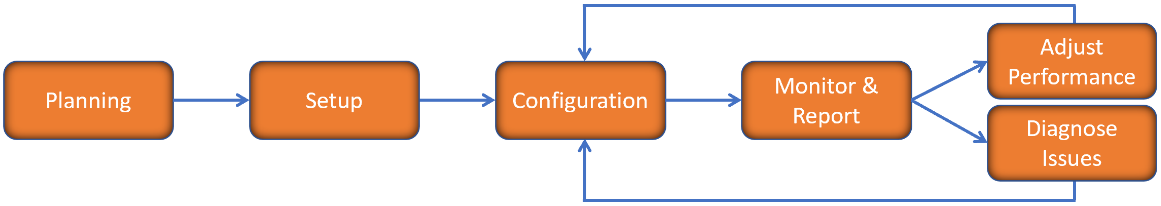
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide

- *SonicOS Command Line Interface Reference Guide*

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

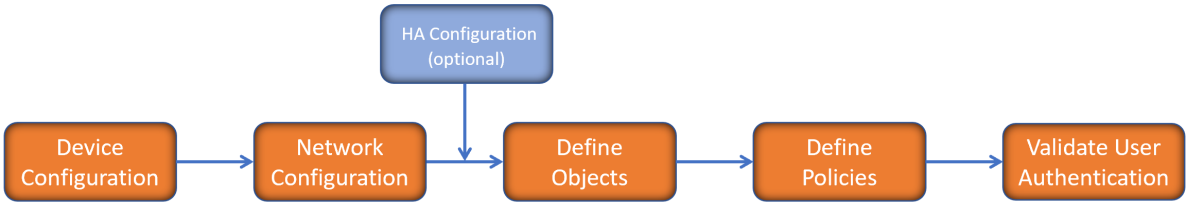


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

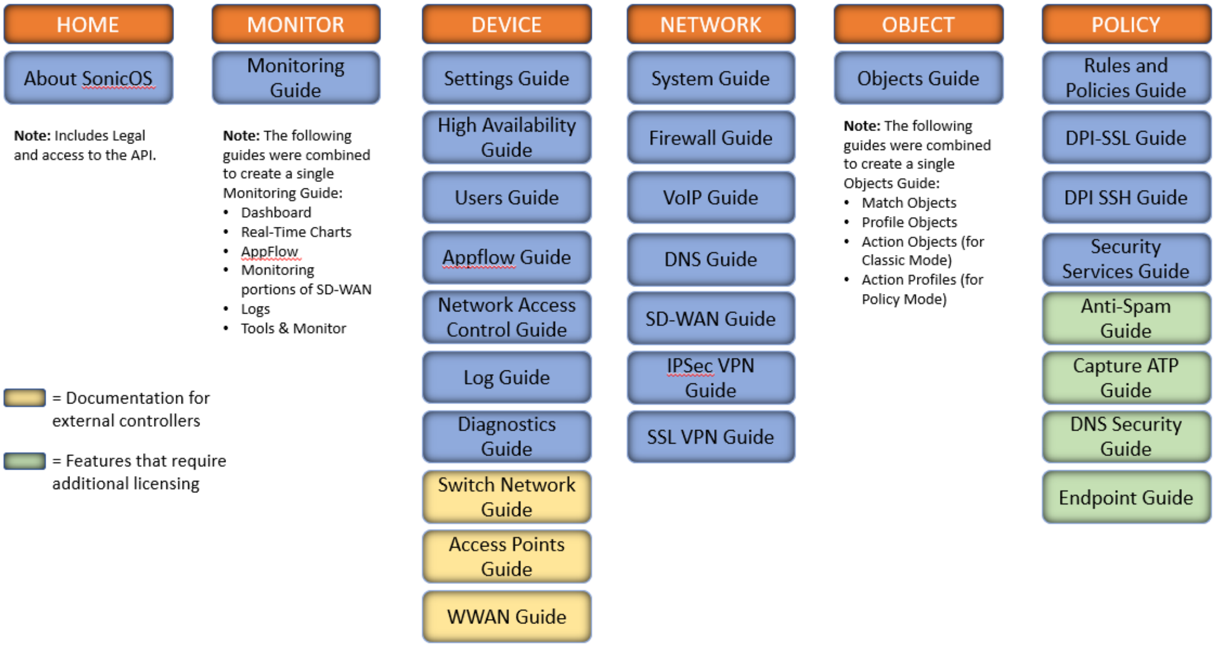


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



Note: Includes Legal and access to the API.

Note: The following guides were combined to create a single Monitoring Guide:

- Dashboard
- Real-Time Charts
- AppFlow
- Monitoring portions of SD-WAN
- Logs
- Tools & Monitor

Note: The following guides were combined to create a single Objects Guide:

- Match Objects
- Profile Objects
- Action Objects (for Classic Mode)
- Action Profiles (for Policy Mode)

🟨 = Documentation for external controllers

🟩 = Features that require additional licensing

The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the https://www.sonicwall.com/support/technical-documentation/.

Guide Conventions

These text conventions are used in this guide:

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

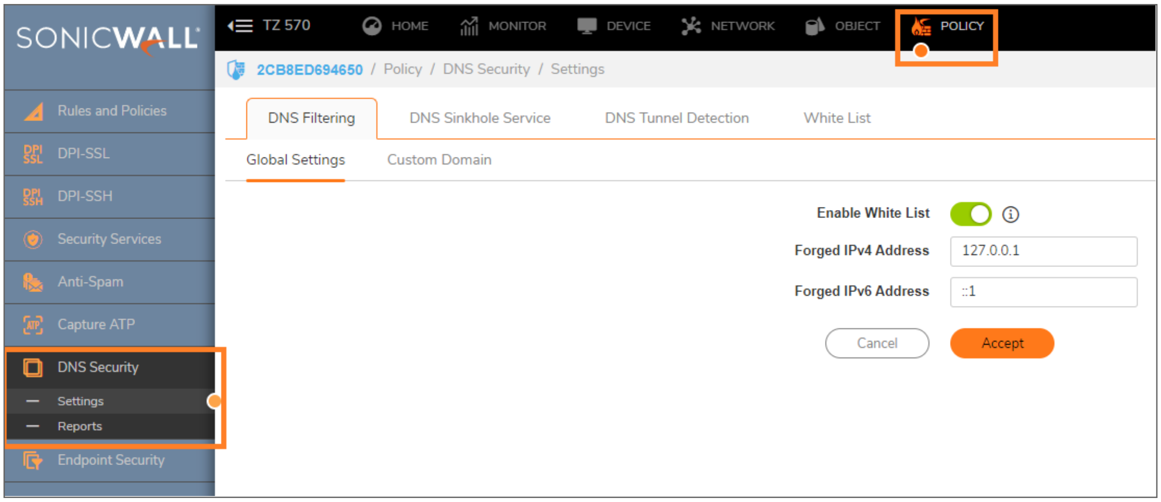
⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=**<*your serial number*>, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

2

About Policy

SonicOS comes equipped with several features to configure policy. The other policy configuration tools are group under the **POLICY** option as follows.



2CB8ED694650 / Policy / DNS Security / Settings

Enable White List ●

Forged IPv4 Address 127.0.0.1

Forged IPv6 Address ::1

- **Rules and Policies** - To configure the setting rules and policies.
- **DPI-SSL** - DPI-SSL is a separate, licensed feature that provides inspection of encrypted HTTPS traffic and other SSL-based IPv4 and IPv6 traffic.
- **DPI-SSH** - To configure the decryption DPI-SSH.
- **Security Services** - Security Services settings allow a choice of operating for maximum security, or accepting less than the highest security level but with higher network performance levels.
- **Anti-Spam** - Anti-Spam is a separate, licensed feature that provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.
- **Capture ATP** - Capture Advanced Threat Protection (ATP) helps a firewall identify whether a file is malicious by transmitting the file to the cloud where the SonicWall Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements.
- **DNS Security** - The Domain Name System (DNS) Security is a domain categorization service by integrating with public DNS Server Neustar.

- **Endpoint Security** - Manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus/Anti Spyware/Capture ATP.

Topics:

- DNS Security Introduction
- DNS Filtering Dashboard

DNS Security Introduction

The Domain Name System (DNS) Security is a domain categorization service by integrating with public DNS Server Neustar. The following are the features of DNS Security:

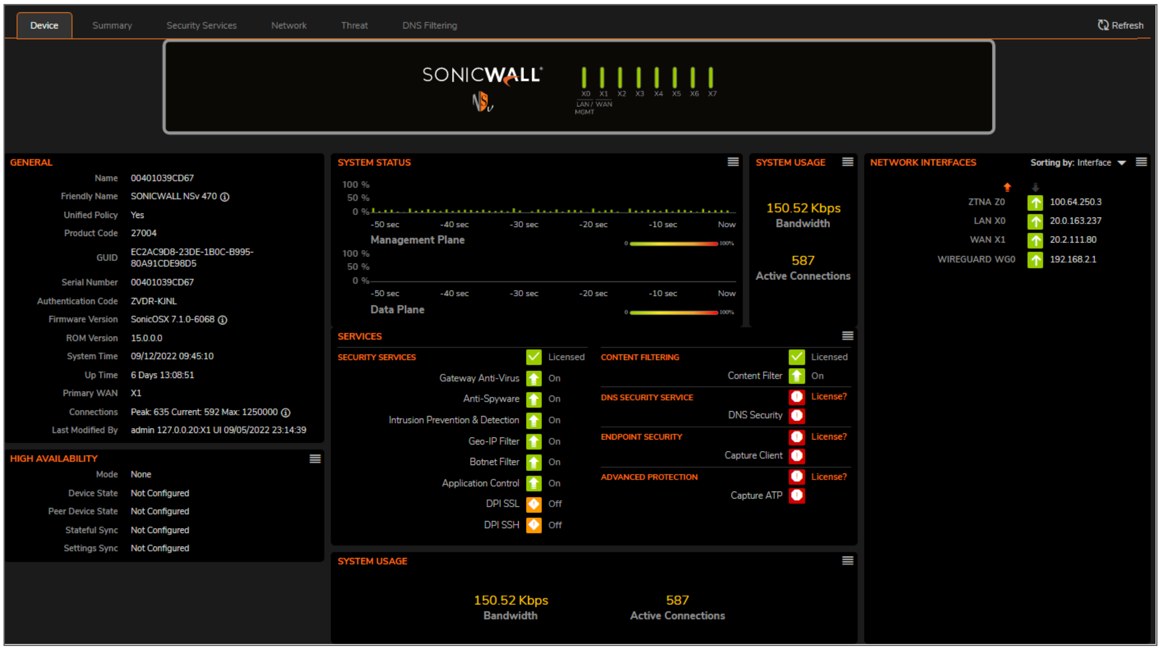
- Provide central DNS management by leveraging SonicOS DNS proxy
- Support DNS Filtering enforcement in both UPE and Global mode
- Support EDNS packet process and DNS category processing report
- Inspect and deny domains associated with malicious activity over 19 pre-defined categories
- Early Malware detection with out decryption

The DNS tools are group under the **POLICY | DNS Security** options allows you to configure DNS Security.

- Configuring DNS Security Settings
- Reports

DNS Filtering Dashboard

The Dashboard is the default view when you log in to SonicOS for the first time. The navigation path is **HOME > Dashboard > System**.



GENERAL

Name	00401039CD67
Friendly Name	SONICWALL NSv 470 ⓘ
Unified Policy	Yes
Product Code	27004
GUID	EC2AC9D8-23DE-1B0C-B995-80A91CDE98D5
Serial Number	00401039CD67
Authentication Code	ZVDR-KJNL
Firmware Version	SonicOSX 7.1.0-6068 ⓘ
ROM Version	15.0.0.0
System Time	09/12/2022 09:45:10
Up Time	6 Days 13:08:51
Primary WAN	X1
Connections	Peak: 635 Current: 592 Max: 1250000 ⓘ
Last Modified By	admin 127.0.0.20:X1 UI 09/05/2022 23:14:39

HIGH AVAILABILITY

Mode	None
Device State	Not Configured
Peer Device State	Not Configured
Stateful Sync	Not Configured
Settings Sync	Not Configured

SYSTEM STATUS

SYSTEM USAGE

150.52 Kbps
Bandwidth

587
Active Connections

NETWORK INTERFACES

Sorting by: Interface

ZTNA Z0	↑	100.64.250.3
LAN X0	↑	20.0.163.237
WAN X1	↑	20.2.111.80
WIREGUARD WG0	↑	192.168.2.1

SERVICES

SECURITY SERVICES	✓	Licensed
Gateway Anti-Virus	↑	On
Anti-Spyware	↑	On
Intrusion Prevention & Detection	↑	On
Geo-IP Filter	↑	On
Botnet Filter	↑	On
Application Control	↑	On
DPI SSL	!	Off
DPI SSH	!	Off

CONTENT FILTERING	✓	Licensed
Content Filter	↑	On
DNS SECURITY SERVICE	!	License?
DNS Security	!	
ENDPOINT SECURITY	!	License?
Capture Client	!	
ADVANCED PROTECTION	!	License?
Capture ATP	!	

SYSTEM USAGE

150.52 Kbps
Bandwidth

587
Active Connections

It provides several sections and tabs for viewing the status of your SonicOS firewall and shows a graphical representation of key firewall features and performance. The Dashboard can be your starting place for monitoring performance. Symbols and colors are used to indicate whether things are operational, need attention, or if a problem needs to be resolved.

Click the DNS Filtering tab in **HOME > Dashboard > System** to view the DNS Filtering status.

3

Configuring DNS Security Settings

The **POLICY | DNS Security** page allows you to manually configure your DNS security settings at the unit and group levels.

Topics:

- About DNS Filtering
- Configuring DNS Sinkhole Service
- Configuring DNS Tunnel Detection
- White List

About DNS Filtering

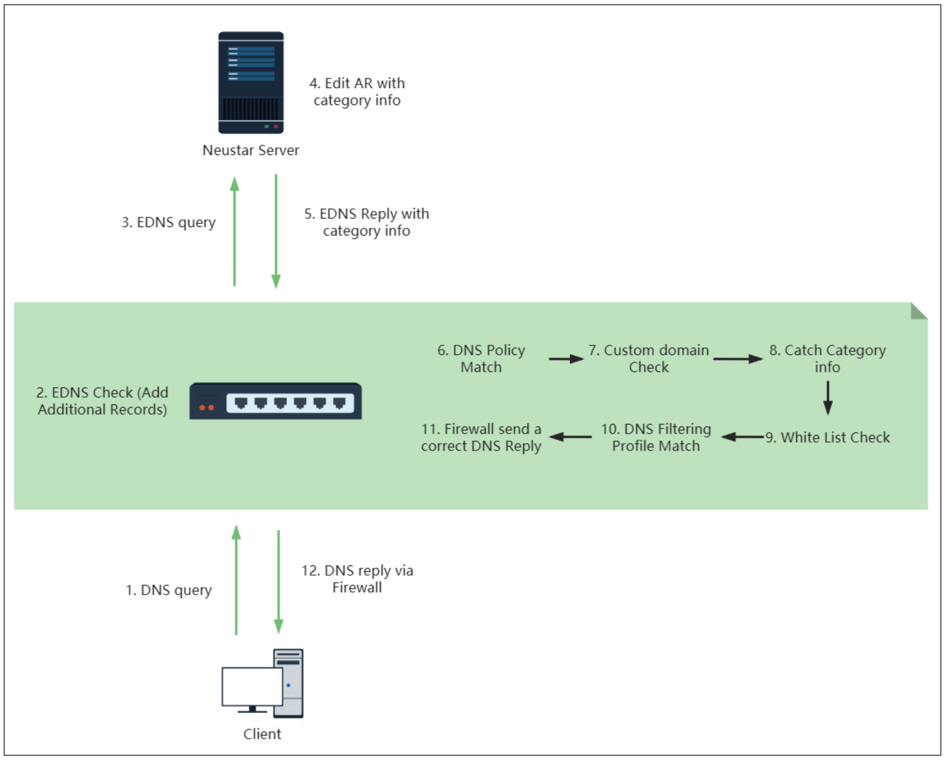
Before SonicOS 7.x, SonicOS doesn’t have the domain categorization service

SonicOS 7.1 onwards, SonicOS has central DNS management by leveraging DNS proxy, and DNS security features like DNS Filtering, DNS Sinkhole service ,and DNS Tunnel Detection.

The following are the configuration change reference.

Before 7.x	After 7.x
Global Enable DNS Proxy	No longer needed
Enable DNS Proxy per interface	In each DNS Policy, configure the source interface
DNS Proxy Mode	Configured in each DNS Policy
Enforce DNS Proxy For All DNS Requests	As origin
Enable DNS Proxy Cache	As origin

Neustar is a public DNS Server which has intelligence of domain name categorization. By integrating Neustar DNS service with SonicWall firewall, we obtain domain categorization service along with DNS for SonicWall customers.SonicWall support profiles to take different actions on different categories, then the DNS Packet will process according to the action. Neustar support 19 pre-defined categories and SonicWall support 4 actions.


4. Edit AR with category info
Neustar Server
3. EDNS query
5. EDNS Reply with category info
2. EDNS Check (Add Additional Records)
6. DNS Policy Match
7. Custom domain Check
8. Catch Category info
9. White List Check
10. DNS Filtering Profile Match
11. Firewall send a correct DNS Reply
1. DNS query
12. DNS reply via Firewall
Client

Topics:

- Configuring DNS Filtering

Configuring DNS Filtering

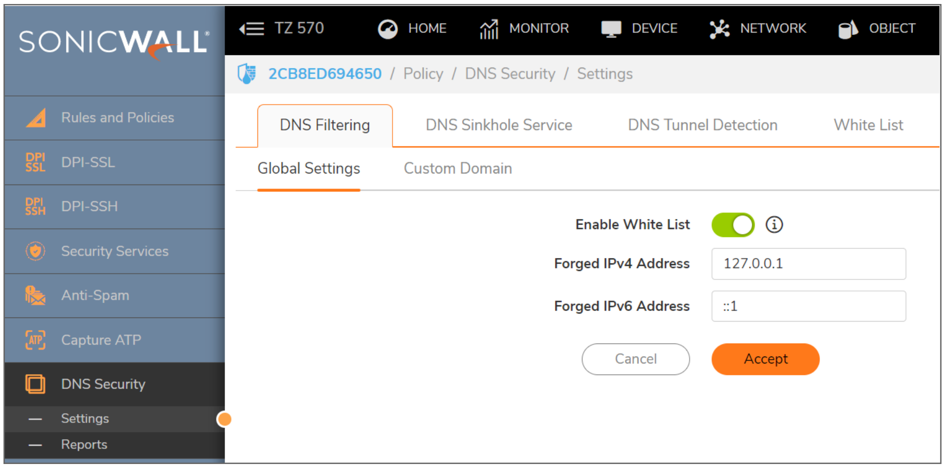
Prerequisite:

To use DNS Filtering, user has to do the following configurations:

- Ensure **DNS Filtering** is licensed under **Gateway Services** in the license page
- Add/Edit/Delete **DNS policy** manually in the **Policy > Rules and Polices > DNS Rules.** For more information on adding DNS policy, refer to the *SonicOS Rules and Policies guide*
- Add/Edit/Delete **DNS Profile** in the **Object > Profile Objects> DNS Filtering.** For more information on adding DNS policy, refer to the *SonicOS Objects guide*
- Set the **DHCP DNS Server Lease Scopes** interface as the interface IP of firewall in the Dynamic Range Configuration. For more information on adding Dynamic, refer to the *SonicOS system guide*
- Enable **Enforce DNS Proxy For All DNS Requests** at **DNS Proxy settings** in the **Network > DNS > DNS Proxy**

To configure Global settings:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Filtering** tab.



Enable White List: on

Forged IPv4 Address: 127.0.0.1

Forged IPv6 Address: ::1

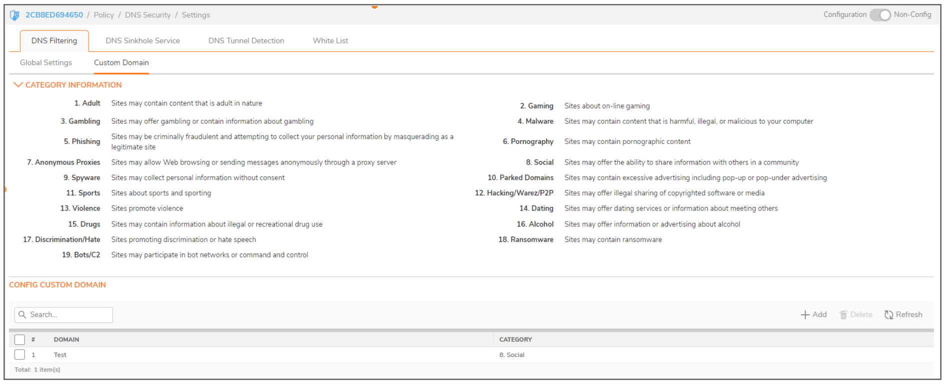
3. Click the **Global Settings** tab. Enable the option **Enable White List**.

   ⓘ | **NOTE:** White List can be used for both **DNS Sinkhole Service** and **DNS Filtering**.

4. Configure both **Forged IPv4 Address** and **Forged IPv6 Address.**
5. Click **Accept.**

To configure Custom Domain:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Filtering** tab.
3. Click the **Custom Domain** tab.
4. Under **Category Information**, you can find the different type of categories and the categories explanation.



CATEGORY INFORMATION

1. Adult	Sites may contain content that is adult in nature	2. Gaming	Sites about on-line gaming
3. Gambling	Sites may offer gambling or contain information about gambling	4. Malware	Sites may contain content that is harmful, illegal, or malicious to your computer
5. Phishing	Sites may be criminally fraudulent and attempting to collect your personal information by masquerading as a legitimate site	6. Pornography	Sites may contain pornographic content
7. Anonymous Proxies	Sites may allow Web browsing or sending messages anonymously through a proxy server	8. Social	Sites may offer the ability to share information with others in a community
9. Spyware	Sites may collect personal information without consent	10. Parked Domains	Sites may contain excessive advertising including pop-up or pop-under advertising
11. Sports	Sites about sports and sporting	12. Hacking/Warez/P2P	Sites may offer illegal sharing of copyrighted software or media
13. Violence	Sites promote violence	14. Dating	Sites may offer dating services or information about meeting others
15. Drugs	Sites may contain information about illegal or recreational drug use	16. Alcohol	Sites may offer information or advertising about alcohol
17. Discrimination/Hate	Sites promoting discrimination or hate speech	18. Ransomware	Sites may contain ransomware
19. Bots/C2	Sites may participate in bot networks or command and control		

CONFIG CUSTOM DOMAIN

□	#	DOMAIN	CATEGORY
□	1	Test	8. Social

Total: 1 item(s)

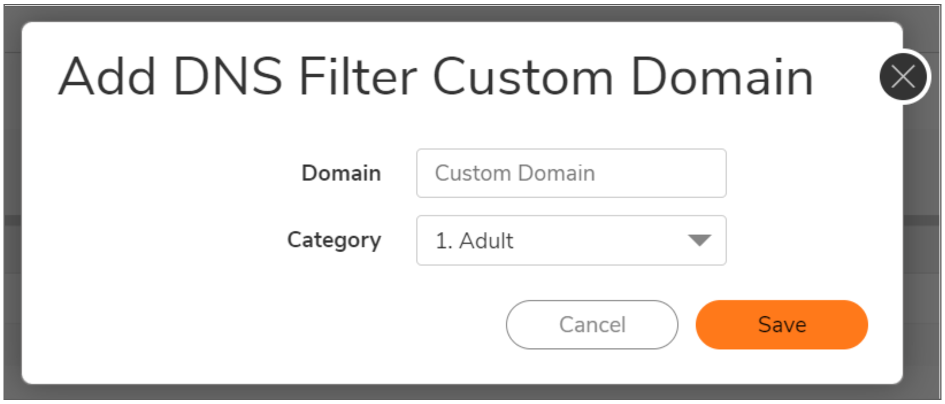
5. For each domain name you want to add as a custom domain name under the **Config Custom Domain** section:

a. Click **+Add**. The **Add DNS filter Custom Domain** dialog displays.

b. Enter the custom domain name in the **Domain Name** field.

c. Select the category type from the drop-down in the **Category** field.

d. Click **Save**.



Add DNS Filter Custom Domain

Domain: Custom Domain

Category: 1. Adult

Configuring DNS Sinkhole Service

A DNS sinkhole also known as a sinkhole server, Internet sinkhole, or Blackhole DNS — is a DNS server that gives out false information to prevent the use of the domain names it represents. DNS sinkholes are effective at detecting and blocking malicious traffic, and used to combat bots and other unwanted traffic.

SonicOS provides the ability to configure a sinkhole with black and white lists.

To configure DNS Sinkhole settings:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Sinkhole Service** tab.
3. Select **Enable DNS Sinkhole Service** under the **Settings** tab. This option is not selected by default.
4. Click the **Global Settings** tab. Enable the option **Enable White List**.
5. From the **Action** drop-down menu, select what the service should do:
   - **Dropping with Logs**
   - **Dropping with Negative DNS reply to Source**
   - **Dropping with DNS reply of Forged IP**
6. Ensure the **IPv4 address and IPv6 address**, **Current Detection**, and **Malicious Domain** in the fields.
7. Click **Accept**.

To configure Custom Malicious Domain Name List:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Sinkhole Service** tab.
3. Click the **Custom Malicious Domain Name** tab.
4. For each domain name you want to add as a malicious domain name:
   a. Click **+Add**. The **Add One Domain Name** dialog displays.
   b. Enter the malicious domain name in the **Domain Name** field.
   c. Click **Save**.

Deleting Entries in the Custom Malicious Domain Name List

To delete the entries in a list:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Sinkhole Service** tab.
3. Click the **Custom Malicious Domain Name** tab.
4. Select an entry to delete or select the top checkbox next to the **Domain Name** column to select all of the items in the list.
5. Click **Delete**.

Configuring DNS Tunnel Detection

DNS tunneling is a method of bypassing security controls and exfiltrating data from a targeted organization. A DNS tunnel can be used as a full remote-control channel for a compromised internal host. Capabilities include Operating System (OS) commands, file transfers, or even a full IP tunnel.

SonicOS provides the ability to detect DNS tunneling attacks, displays suspicious clients, and allows you to create white lists for DNS tunnel detection.

When DNS tunneling detection is enabled, SonicOS logs whenever suspicious DNS packets are dropped.

ⓘ | **NOTE:** DNS Tunneling settings can be made at the group or unit level.

Topics:

- Configuring DNS Tunnel Detection
- Detected Suspicious Client Information
- Creating White list for DNS Tunnel Detection
- Deleting White List Entries for DNS Tunnel Detection

Configuring DNS Tunnel Detection

To configure DNS tunnel detection:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Click the **DNS Tunnel Detection** tab.
3. Under **Settings**, select **Enable DNS Tunnel Detection** to enable DNS tunnel detection.
4. To block all the DNS traffic from the detected clients, select **Block All The Clients DNS Traffic**.
5. Click **Accept**.

Detected Suspicious Client Information

SonicOS displays information about all hosts that have established a DNS tunnel in the **Detected Suspicious Clients Info** table.

To view detected suspicious client Information:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Tunnel Detection** tab.
3. Click on the **Detected Suspicious Clients Info** tab.

This table is populated only if DNS tunnel detection is enabled. Hosts are dropped only if blocking clients DNS traffic is enabled. For more information, refer to Configuring DNS Tunnel Detection.

IP Address	IP address of the suspicious client
MAC Address	MAC address of the suspicious client
Detection Method	DNS type used to detect suspicious clients: • **Normal DNS Type**: A, AAAA, CNAME • **Corner DNS Type**: such as TXT, NULL, SRV, PRIVATE, and MX
Interface	Interface on which the host establishing the DNS tunnel was detected
Block	Indicates whether the host was blocked

Creating White list for DNS Tunnel Detection

You can create white lists for IP address you consider safe. If a detected DNS tunnel IP address matches an address in the white list, DNS tunnel detection is bypassed.

To create a DNS white list:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Tunnel Detection** tab.
3. Click on the **White List for DNS Tunnel Detection** tab.
4. For each IP address you want to add to the white list:
    a. Click **+Add**. The **Add One White Entry** dialog displays.
    b. In the **IP Address** field, enter the IP address of the domain to be added to the whitelist.
    c. Click **Save**.

Deleting White List Entries for DNS Tunnel Detection

To delete all white list entries for DNS tunnel detection:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Hover over to the **DNS Tunnel Detection** tab.
3. Click on the **White List for DNS Tunnel Detection** tab.
4. Select an entry to delete or select the top checkbox next to the **IP Address** column to select all of the items.
5. Click **Delete**.

White List

You can create white lists for IP address you consider safe.

ⓘ | **NOTE:** The default URLs on White List is deleted by design. Now its displays No data as default.

To create a white list:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Click the **White List** tab.

3. For each domain name you want to add to the white list:
    a. Click **+Add**. The **Domain Name** dialog displays.
    b. In the **Domain Name** field, enter the white list domain name.
    c. Click **Save**.

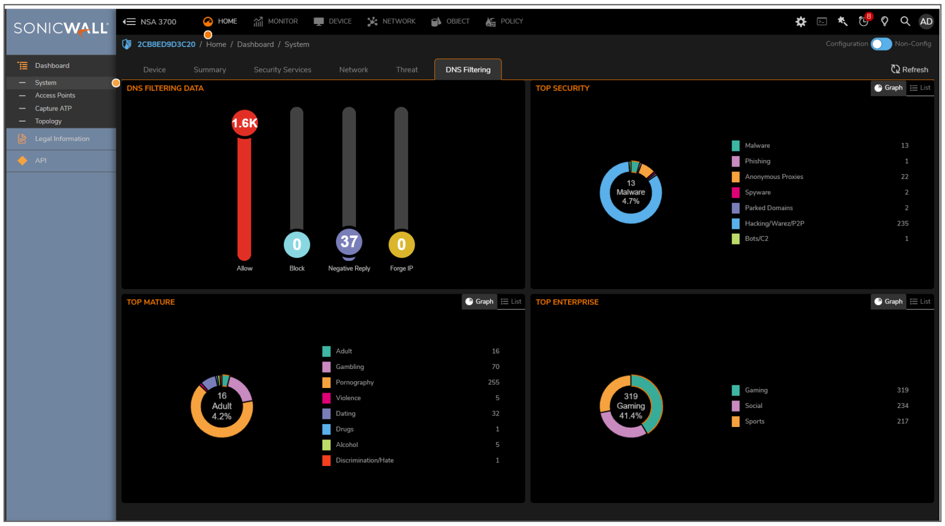
To delete all white list:

1. Navigate to **POLICY | DNS Security > Settings**.
2. Click the **White List** tab.
3. Select an entry to delete or select the top checkbox next to the **IP Address** column to select all of the items.
4. Click **Delete**.

4

Reports

Navigation to **HOME > Dashboard > System**.to view the overview of DNS Filtering data and reports.



🟩 Malware	13
🟪 Phishing	1
🟧 Anonymous Proxies	22
🟥 Spyware	2
🟪 Parked Domains	2
🟦 Hacking/Warez/P2P	235
🟩 Bots/C2	1

🟩 Adult	16
🟪 Gambling	70
🟧 Pornography	255
🟥 Violence	5
🟪 Dating	32
🟦 Drugs	1
🟩 Alcohol	5
🟥 Discrimination/Hate	1

🟩 Gaming	319
🟪 Social	234
🟧 Sports	217

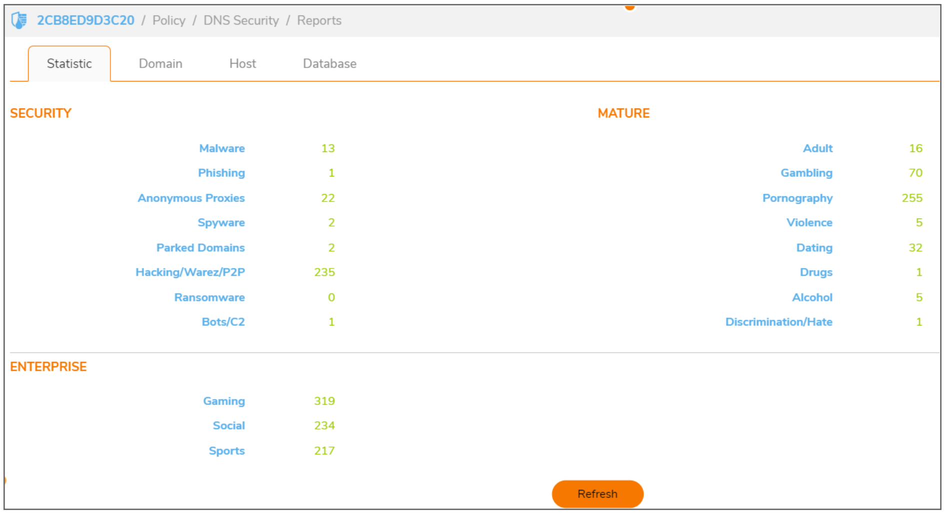
The **POLICY | DNS Security > Reports** page allows you to view the different types of reports and to export data.

Topics:

- Statistic
- Domain
- Host
- Database

Statistic

Navigate to **Policy > DNS Security > Reports** and click **Statistic** tab, this page allows you to view these categories of statistic reports.



SECURITY

Malware	13
Phishing	1
Anonymous Proxies	22
Spyware	2
Parked Domains	2
Hacking/Warez/P2P	235
Ransomware	0
Bots/C2	1

MATURE

Adult	16
Gambling	70
Pornography	255
Violence	5
Dating	32
Drugs	1
Alcohol	5
Discrimination/Hate	1

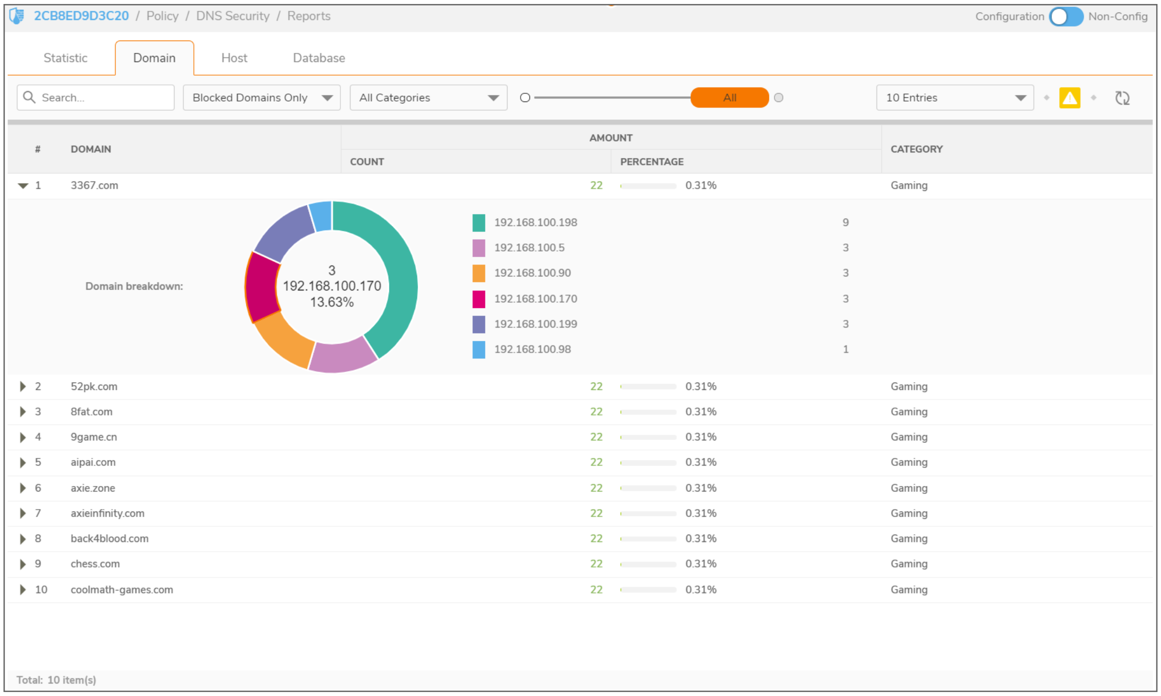
ENTERPRISE

Gaming	319
Social	234
Sports	217

- **Security** - You can view the total number of reports under the following categories.
  - Malware
  - Phishing
  - Anonymous Proxies
  - Spyware
  - Parked Domains
  - Hacking/Warez/P2P
  - Ransomware
  - Bots/C2
- **Mature** - You can view the total number of reports under the following categories
  - Adult
  - Gambling
  - Pornography
  - Violence
  - Dating
  - Drugs
  - Alcohol
  - Discrimination/Hate
- **Enterprise** - You can view the total number of reports under the following categories
  - Gaming
  - Social
  - Sports

Domain

Navigate to **Policy > DNS Security > Reports** and click **Domain** tab, this page allows you to view the list of domains, number of count, percentage, and categories.



#	DOMAIN	AMOUNT		CATEGORY
		COUNT	PERCENTAGE	
1	3367.com	22	0.31%	Gaming
2	52pk.com	22	0.31%	Gaming
3	8fat.com	22	0.31%	Gaming
4	9game.cn	22	0.31%	Gaming
5	aipai.com	22	0.31%	Gaming
6	axie.zone	22	0.31%	Gaming
7	axieinfinity.com	22	0.31%	Gaming
8	back4blood.com	22	0.31%	Gaming
9	chess.com	22	0.31%	Gaming
10	coolmath-games.com	22	0.31%	Gaming

Domain breakdown:

3
192.168.100.170
13.63%

192.168.100.198	9
192.168.100.5	3
192.168.100.90	3
192.168.100.170	3
192.168.100.199	3
192.168.100.98	1

Total: 10 item(s)

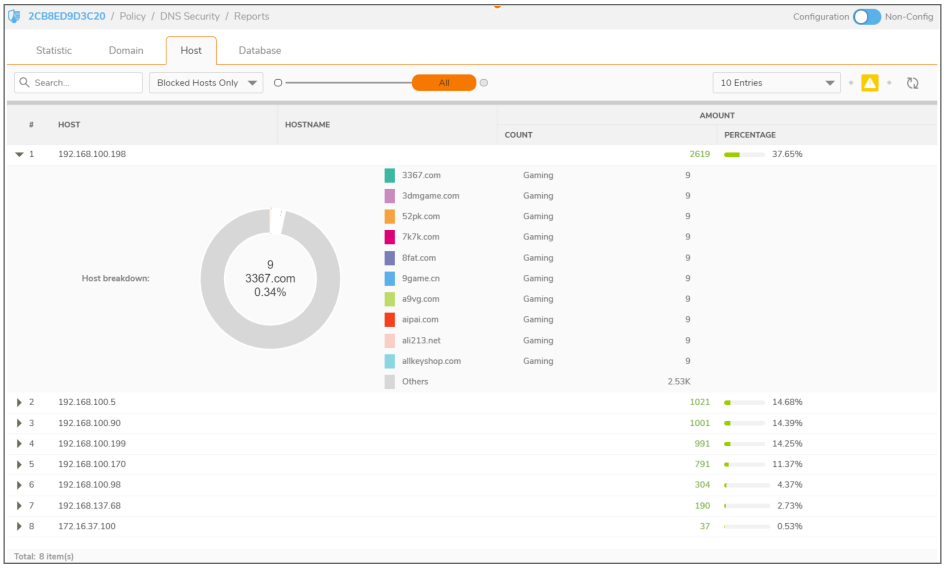
- You can select **All Domains** or the **Blocked Domains only** from the drop-down menu.
- You can select **All Categories** or a specific category from the drop-down menu.
- You can view the list of domains based on the time frame hovering your mouse pointer over one of the following options on the time frame button.
    - 30 Minutes
    - 60 Minutes
    - 12 Hours
    - 24 Hours
    - 7 Days
    - 15 Days
    - 30 Days
    - All
- You can limit the number of domains entries by selecting one of the following options from the drop-down menu.

- 10 Entries
- 50 Entries
- 100 Entries
- 500 Entries
- 1000 Entries
- Unlimited Entries

- You can view the license status of DNS Filtering and availability of External Storage status.

Host

Navigate to **Policy > DNS Security > Reports** and click **Host** tab, this page allows you to view the list of Hosts, number of count, percentage, and categories.



#	HOST	HOSTNAME	AMOUNT	
			COUNT	PERCENTAGE
1	192.168.100.198		2619	37.65%
2	192.168.100.5		1021	14.68%
3	192.168.100.90		1001	14.39%
4	192.168.100.199		991	14.25%
5	192.168.100.170		791	11.37%
6	192.168.100.98		304	4.37%
7	192.168.137.68		190	2.73%
8	172.16.37.100		37	0.53%

Host breakdown:

3367.com	Gaming	9
3dmgame.com	Gaming	9
52pk.com	Gaming	9
7k7k.com	Gaming	9
8fat.com	Gaming	9
9game.cn	Gaming	9
a9vg.com	Gaming	9
aipai.com	Gaming	9
ali213.net	Gaming	9
allkeyshop.com	Gaming	9
Others		2.53K

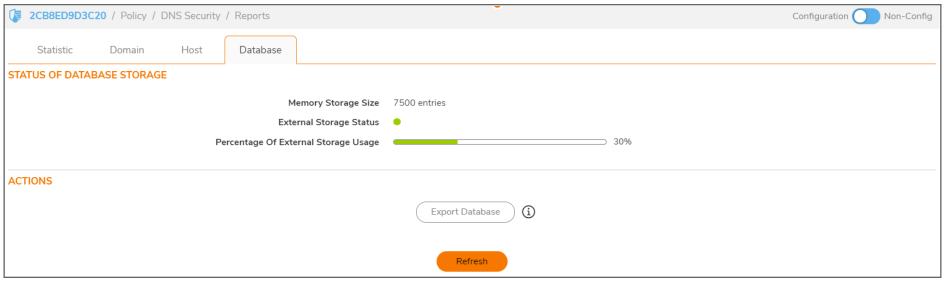
Total: 8 item(s)

- You can select **All Hosts** or the **Blocked Hosts only** from the drop-down menu.
- You can view the list of hosts based on the time frame hovering your mouse pointer over one of the following options from the time frame button.
  - 30 Minutes
  - 60 Minutes
  - 12 Hours
  - 24 Hours
  - 7 Days
  - 15 Days

- 30 Days
    - All
- You can limit the number of hosts entries by selecting one of the following options from the drop-down menu.
    - 10 Entries
    - 50 Entries
    - 100 Entries
    - 500 Entries
    - 1000 Entries
    - Unlimited Entries
- You can view the license status of DNS Filtering and availability of External Storage Status.

Database

Navigate to **Policy > DNS Security > Reports** and click **Database** tab, this page allows you to view the status of database storage and to export the database:



STATUS OF DATABASE STORAGE

Memory Storage Size 7500 entries

External Storage Status ●

Percentage Of External Storage Usage 30%

ACTIONS

- You can view the following status under the **Status of Database Storage** section.
    - **Memory Storage Size**
    - **External Storage Status**
    - **Percentage of External Storage Usage**
- Click **Export Database** under **Action** section to export the database.
  A pop-up appears for the export confirmation.
  Click **OK**.
- Click **Refresh** to view the up to date status of database storage.

5

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

SonicOS DNS Security Administration Guide
Updated - December 2023
Software Version - 7.1
232-005884-00 Rev A

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035