

SonicOS 7.1

DNS

Administration Guide

SONICWALL®

Contents

About SonicOS	4
Working with SonicOS	4
SonicOS Workflow	6
How to Use the SonicOS Administration Guides	7
Guide Conventions	8
About Network	9
DNS Introduction	10
Configuring DNS Settings	11
Configuring DNS for IPv4	11
Specifying which DNS Servers are Used	11
Enabling Proxy of Split DNS Servers	12
DNS Rebinding Attack Prevention	13
DNS Rebinding and Cache Lookup	13
Configuring DNS for IPv6	15
Specifying which DNS Servers are Used	15
Enabling Proxy of Split DNS Servers	15
Enabling DNS Host Name Lookup over TCP for FQDN	16
Configuring Domain-Specific DNS Servers for Split DNS	16
About Split DNS	17
Adding a Split DNS Server	18
Editing Split DNS Entries	19
Deleting Split DNS Entries	19
Configuring Dynamic DNS	21
About Dynamic DNS	21
Supported DDNS Providers	22
Dynamic DNS Profiles	22
Configuring Dynamic DNS Profiles	24
Editing Dynamic DNS Profiles	26
Deleting Dynamic DNS Profiles	26
Configuring DNS Proxy Settings	27
About DNS Proxy	27
Supported Interfaces	28
DNS Server Liveness Detection and Failover	28
DNS Cache	28

High Availability Stateful Synchronization of DNS Cache	29
DHCP Server	29
Enabling Log Settings	30
Monitoring Packets	30
Configuring DNS Proxy Settings	30
Configuring DNS Proxy Settings	30
Deleting Static DNS Cache Entries	31
Viewing DNS Proxy Cache Objects	31
Flushing Dynamic DNS Cache Entries	32
SonicWall Support	33
About This Document	34

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 Workflow
- How to Use the SonicOS Administration Guides
- Guide Conventions

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 HTTPS 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.

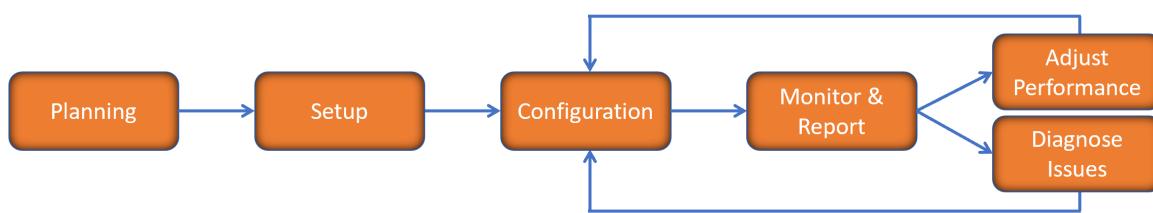
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [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.

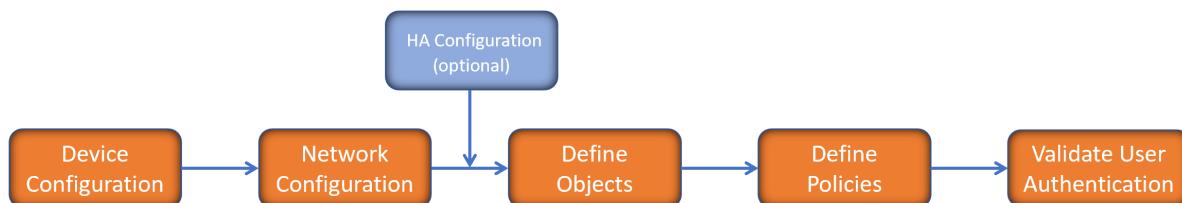


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). 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 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.

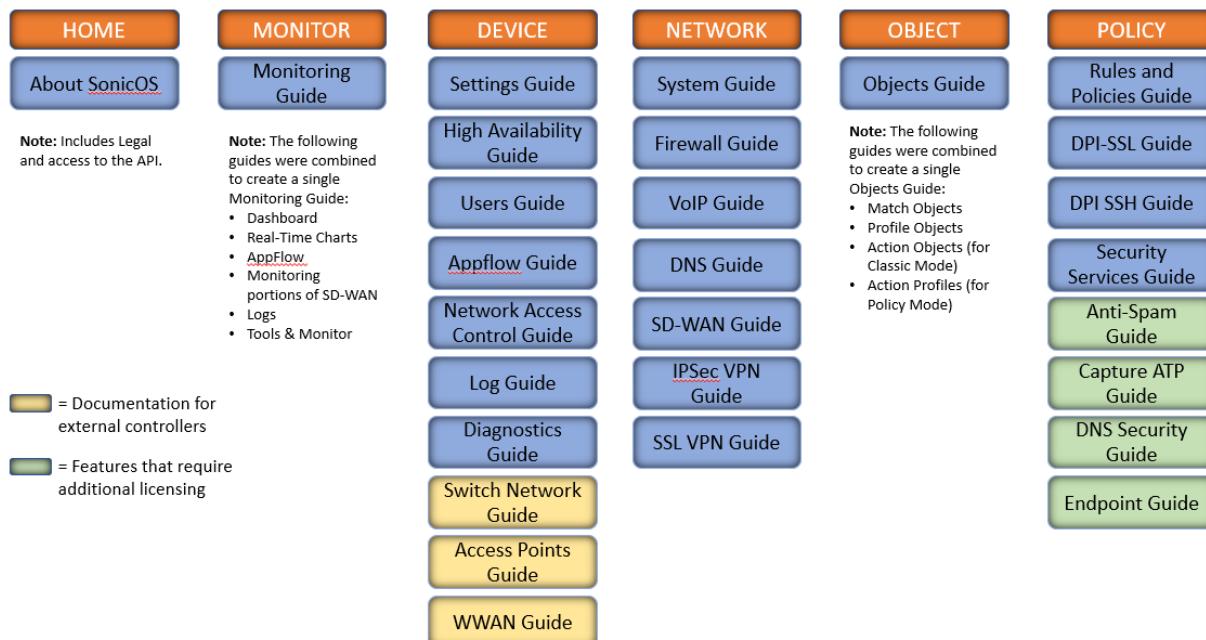


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement 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.



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

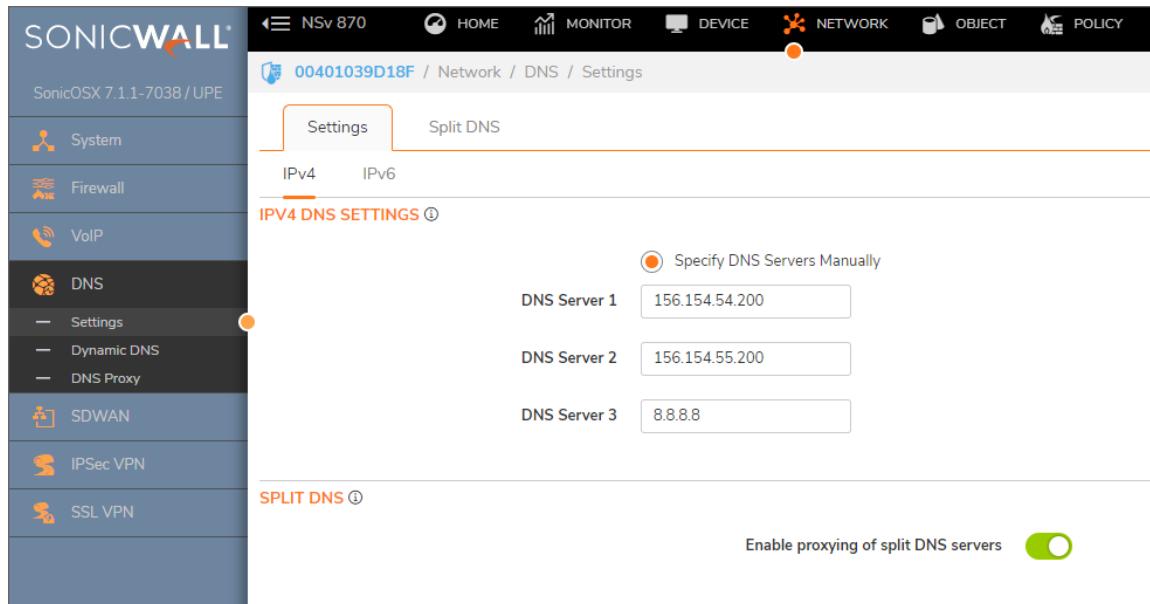
These text conventions are used in this guide:

- ⓘ | **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.

About Network

SonicOS comes equipped with several features to configure Network. Basic Network information can be viewed in the Dashboard (navigate to **HOME > Dashboard>System**). The other Network configuration tools are group under the **NETWORK** option as follows.



- **System** - To manage the Network settings.
- **Firewall** - To manage the Firewall settings and to view the connections.
- **VoIP** - To manage the General settings and to view call status.
- **DNS** - To configure DNS settings, Dynamic DNS, and DNS Proxy settings.
- **SD-WAN** - To configure SD-WAN groups.
- **IPSec VPN** - To configure IPSec VPN settings.
- **SSL VPN** - To configure SSL VPN settings.

Topics:

- [DNS Introduction](#)

DNS Introduction

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

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

- [Configuring DNS Settings](#)
- [Configuring Dynamic DNS](#)
- [Configuring DNS Proxy Settings](#)

Configuring DNS Settings

NETWORK | DNS allows you to manually configure your DNS settings, if necessary.

The options in **NETWORK | DNS > Settings** change depending on whether you select **IPv4** or **IPv6** on the **Settings** tab.

To select the IP version:

1. Navigate to **NETWORK | DNS > Settings**.
2. On the **Settings** tab, select either the **IPv4** or **IPv6** option.

Topics:

- Configuring DNS for IPv4
- Configuring DNS for IPv6
- Configuring Domain-Specific DNS Servers for Split DNS

Configuring DNS for IPv4

The **NETWORK | DNS > Settings > IPv4** page has these sections:

- Specifying Which DNS Servers are Used
- Enabling Proxy of Split DNS Servers
- DNS Rebinding Attack Prevention
- DNS Rebinding and Cache Lookup

Specifying which DNS Servers are Used

Regardless of the IP version, you can specify how SonicOS selects the DNS servers.

To specify which DNS servers are used:

1. Navigate to **NETWORK | DNS > Settings**.
2. In the **IPv4 DNS Settings**, select one of the following:
 - To manually specify the DNS servers:
 1. Select **Specify DNS Servers Manually**.
 2. Enter up to three IP addresses into the **DNS Server #** fields.
 - To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from WAN Zone**. This is the default. The IP address(es) are populated into the **DNS Server** fields automatically.
3. Click **Accept** to save your changes.

Enabling Proxy of Split DNS Servers

Split DNS servers are separate domain-specific DNS servers that you can use optionally with IPv6.

To enable the proxying of split DNS servers:

1. Navigate to **NETWORK | DNS > Settings**.
2. Select **Enable proxying of split DNS servers** under to the **Split DNS** section. This option is selected by default.
3. Click **Accept**.

DNS Rebinding Attack Prevention

DNS rebinding is a DNS-based attack on code embedded in web pages. Normally requests from code embedded in web pages (JavaScript, Java, and Flash) are bound to the website they are originating from (see Same Origin Policy). A DNS rebinding attack can be used to improve the ability of JavaScript-based malware to penetrate private networks and subvert the browser's same-origin policy.

DNS rebinding attackers register a domain that is delegated to a DNS server they control. The server is configured to respond with a very short Time to Live (TTL) parameter, which prevents the result from being cached. The first response contains the IP address of the server hosting the malicious code. Any subsequent requests contain IP addresses from private (RFC 1918) network, presumably behind a firewall, being target of the attacker. Because both are fully valid DNS responses, they authorize the sandbox script to access hosts in a private network. By iterating addresses in these short-term but still valid DNS replies, the script is able to scan the network and perform other malicious activities.

To configure DNS rebinding attack prevention:

1. Navigate to **NETWORK | DNS > Settings**.
2. Select **Enable DNS Rebinding Attack Prevention** under **DNS Rebinding Attack Prevention** section. This option is not selected by default. The two options become available.
3. From the **Action** drop-down menu, select an action to perform when a DNS rebinding attack is detected:
 - **Log Attack**
 - **Log Attack & Return a Query Refused Reply**
 - **Log Attack & Drop DNS Reply**
4. From the **Allowed Domains** drop-down menu, select an allowed domain FQDN Address Object or FQDN Address Object Group containing allowed domain-names (such as *.SonicWall.com) for which locally connected/routed subnets should be considered legal responses.
You can also create new FQDN address objects or FQDN address object groups by selecting **Create new FQDN Address Object Group...** or **Create new FQDN Address Object....**
5. Click **Accept**.

DNS Rebinding and Cache Lookup

This section provides settings related to the prevention of DNS rebinding attacks using FQDN address objects.

DNS Binding For FQDN

To enable DNS binding for FQDN:

1. Navigate to **NETWORK | DNS > Settings**.
2. Scroll to the **DNS Rebinding and Cache Lookup** section.

3. Under the **DNS Binding for FQDN** heading, select **FQDN Object Only Cache DNS Reply from Sanctioned Server**. This option is not selected by default.
4. Click **Accept**.

Enabling DNS Host Name Lookup over TCP for FQDN

By default, DNS queries are sent over UDP. The DNS response can include a Truncated flag if the response length exceeds the maximum allowed by UDP.

When the **Enable DNS host name lookup over TCP for FQDN** option is:

- Enabled and the Truncated flag is set in the DNS response, SonicOS sends an additional DNS query over TCP to determine the full DNS response for multiple IP addresses.
- Disabled, DNS queries are sent over UDP, and SonicOS only processes the IP addresses in the DNS response packet, although the Truncated flag is set in the response.

The DNS query times out after one second if no DNS response over TCP is received from the DNS server.

This option is used to gain more IP addresses when sending DNS queries from FQDN over TCP while the Security Appliance receives DNS responses over UDP.

To enable DNS host name lookup over TCP for FQDN:

1. Navigate to **NETWORK | DNS > Settings**.
2. Under the **DNS host name lookup over TCP for FQDN** heading, select **Enable DNS host name lookup over TCP for FQDN**. This option is not selected by default.
3. Click **Accept**.

DNS Cache Lookup

With the DNS Cache Lookup feature, you can view the cached names and IP addresses from DNS resolution. To show the contents of the general DNS cache, click **Lookup DNS Cache**. A pop-up displays the cache contents.

What	DNS Server name: <ul style="list-style-type: none"> • Forward DNS cache, the host name. • Reverse DNS cache, a string representation of the IP address.
DNS Name	Domain name, such as <code>www.SonicWall.com</code> , or IP address.
IP Address	Resolved IP address.
TTL (secs)	Time to Live; the TTL value from the DNS response.
flush	Clicking this flushes the server's DNS cache entry
flush all	Clicking this flushes all DNS cache entry of all listed servers

Configuring DNS for IPv6

The **NETWORK | DNS > Settings > IPv6** page has these sections:

- [Specifying Which DNS Servers are Used](#)
- [Enabling Proxy of Split DNS Servers](#)
- [Enabling DNS Host Name Lookup over TCP for FQDN](#)

Specifying which DNS Servers are Used

Regardless of the IP version, you can specify how SonicOS selects the DNS servers.

To specify which DNS servers are used:

1. Navigate to **NETWORK | DNS > Settings**.
2. In the **IPv6 DNS Settings**, select one of the following:
 - To manually specify the DNS servers:
 1. Select **Specify DNS Servers Manually**.
 2. Enter up to three IP addresses into the **DNS Server #** fields.
 - To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from WAN Zone**. This is the default. The IP address(es) are populated into the **DNS Server** fields automatically.
3. Select **Prefer IPv6 DNS Servers** to use IPv6 servers only. This option is not selected by default. SonicOS DNS supports these server types:
 - **DNS_SYSTEM_BEHAVIOR** – the system default behavior, which depends on the setting of this option.
 - **DNS_PREFER_V4_DNSSERVER** – IPv4 DNS servers preferred unless there is a failure, then IPv6 DNS servers are requested.
 - **DNS_PREFER_V6_DNSSERVER** – IPv6 DNS servers preferred unless there is a failure, then IPv4 DNS servers are requested.
4. Click **Accept** to save your changes.

 **CAUTION:** Select this option only if you have configured the IPv6 DNS server correctly.

Enabling Proxy of Split DNS Servers

Split DNS servers are separate domain-specific DNS servers that you can use optionally with IPv6.

To enable the proxying of split DNS servers:

1. Navigate to **NETWORK | DNS > Settings**.
2. Select **Enable proxying of split DNS servers** under the **Split DNS** section. This option is selected by default.
3. Click **Accept**.

Enabling DNS Host Name Lookup over TCP for FQDN

By default, DNS queries are sent over UDP. The DNS response can include a Truncated flag if the response length exceeds the maximum allowed by UDP.

When the **Enable DNS host name lookup over TCP for FQDN** option is:

- Enabled and the Truncated flag is set in the DNS response, SonicOS sends an additional DNS query over TCP to determine the full DNS response for multiple IP addresses.
- Disabled, DNS queries are sent over UDP, and SonicOS only processes the IP addresses in the DNS response packet, although the Truncated flag is set in the response.

The DNS query times out after one second if no DNS response over TCP is received from the DNS server.

This option is used to gain more IP addresses when sending DNS queries from FQDN over TCP while the Security Appliance receives DNS responses over UDP.

To enable DNS host name lookup over TCP for FQDN:

1. Navigate to **NETWORK | DNS > Settings**.
2. Select **Enable DNS host name lookup over TCP for FQDN**. This option is not selected by default.
3. Click **Accept**.

Configuring Domain-Specific DNS Servers for Split DNS

You can optionally configure separate domain-specific DNS servers.

Domain	SonicWall.com.
DNS Servers	IPv4/IPv6 IP address of the DNS Server. ⓘ NOTE: On the NETWORK DNS > DNS Proxy page, only the system DNS server status is displayed. If you use a specific DNS server (other than system DNS server) in Add Split DNS, you cannot see the DNS server status.
Local Interface	Interface assigned to the DNS Server.
Configure	Contains Edit and Delete icons for each server.

Topics:

- [About Split DNS](#)
- [Enabling Proxy of Split DNS Servers](#)
- [Adding a Split DNS Server](#)
- [Editing Split DNS Entries](#)
- [Deleting Split DNS Entries](#)

About Split DNS

Split DNS is an enhancement that allows you to configure a set of servers and associate them to a given domain name (which can be a wildcard). When SonicOS DNS Proxy receives a query that matches the domain name, the name is transmitted to the designated DNS server.

As an example, for a topology that has two firewalls with network connectivity:

- One firewall is connected to the Internet.
- Another is a VPN tunnel connected to the corporation network.
- Default DNS queries go to the public ISP DNS Server.
- All queries to *.SonicWall.com go to the DNS server located behind the VPN tunnel.

For viewing and configuring split DNS entries, see [Configuring Domain-Specific DNS Servers for Split DNS](#).

By adding a split DNS entry, all queries to `SonicWall.com` are sent to the specific server (see [Configuring Domain-Specific DNS Servers for Split DNS](#)).

Multiple DNS servers could be configured to handle queries to `SonicWall.com` as well.

Topics:

- [About Per-Partition DNS Servers and Split DNS](#)

About Per-Partition DNS Servers and Split DNS

With or without authentication partitions, it is usually necessary to use a domain's own DNS servers to resolve the names of devices in the domain, and occasionally there can also be a need to use different external DNS servers to resolve external host names. Now, with multiple authentication partitions, this situation is exacerbated as those partitions usually require using different DNS servers to resolve the host names in the different partitions.

① | NOTE: Use of a domain's own DNS servers can be required unexpectedly because LDAP referrals usually give the referred server by DNS name, even when the LDAP servers are configured by IP address.

An example where different external DNS servers to resolve external host names was required involved external-using cloud services that could not be resolved by the internal domain's DNS servers.

The Split DNS feature is used directly by the SonicWall network security appliance to resolve the names of devices in domains without the need to enable DNS Proxy, including for multiple unrelated domains with authentication partitioning.

DNS servers configured in Split DNS (refer to [Configuring Domain-Specific DNS Servers for Split DNS](#)) are used directly for DNS lookups of host names in internal domains as follows:

- This applies for anything that has entries in the main DNS Cache of the network security appliance:
 - SMTP servers
 - SYSLOG servers
 - Web Proxy servers and User (internal) Proxy servers
 - GMS and GMS standby
 - POP servers
 - RADIUS authentication and accounting servers
 - LDAP servers
 - SSO / Terminal Services agents and RADIUS accounting clients
- If partitioning is enabled and a partition has one domain or one tree of parent/sub-domains (AKA one AD Forest), then if Split DNS servers are configured for the partition's top-level domain, then those are copied into the internal partition structure. Those DNS servers are then used to resolve the names of agents, servers, and clients in the partition.
- If partitioning is enabled and a partition is configured with multiple separate domains (which is allowed but is not common), then no DNS servers are copied into the partition structure, relying instead on the mechanism described below.
- If partitioning is disabled or a partition has no DNS servers set, or for resolving items not associated with a partition, the DNS servers to use are selected per-request through the API provided by Split DNS.

Adding a Split DNS Server

To add domain-specific DNS servers and associate them to a given domain name:

① IMPORTANT: The maximum number of entries for Split DNS is 32. If the list is full, new entries cannot be added.

1. Navigate to **NETWORK | DNS > Settings**.
2. Choose the IP version from **View IP Version**.
3. To enable proxying of split DNS servers, select **Enable proxying of split DNS servers**. This option is selected by default.
4. Under the **Split DNS** table, click **+Add**. The **Add Split DNS** dialog displays.

If you selected **DNS Proxy**, a page for it, **DNS Proxy**, also displays on the **Add Split DNS** dialog.

5. Choose the IP version:
 - **IPv4**
 - **IPv6**
 - **Both**
6. In the **Domain Name** field, enter the domain name. The name can contain a wildcard (*; for example, *.SonicWall.com).
7. To configure one or more IPv4/IPv6 Split DNS Servers for this domain, enter the IP addresses in the appropriate fields:
 - **IPv4/IPv6 DNS Server Primary**
 - **IPv4/IPv6 DNS Server Secondary**
 - **IPv4/IPv6 DNS Server Tertiary**
8. From the **Local interface** drop-down menu, select an interface.
9. If you have enabled **DNS Proxy**:
 - a. To specify a **Time to Live**, select **Manually set TTL value in DNS reply**. This option is not selected by default. If this option is not selected, the TTL value is the same as that from the DNS response; if it is set, the TTL value is the same as the setting.
① | NOTE: This option applies only when Split DNS is used by DNS Proxy.
 - b. Enter the maximum time for the cache entry to exist. The minimum is one second, the maximum is 9999999999999999 seconds.

10. Click **Save**.

TIP: The DNS servers display in the **Split DNS** table of both IP versions regardless of which IP version was chosen when configuring them.

Editing Split DNS Entries

To edit a Split DNS entry:

1. Navigate to **NETWORK | DNS > Settings**.
2. In the **Split DNS** table, click the **Edit** icon associated with entry you want to edit. The **Edit Split DNS** dialog displays.
3. Make the changes.
4. Click **Save**.

Deleting Split DNS Entries

To delete a Split DNS entry:

1. In the **Split DNS** table, click the **Delete** icon in the row associated with entry you want to delete.

To delete two or more Split DNS entries:

1. In the **Split DNS** table, select the check boxes of the entries to be deleted. **Delete** becomes available.
2. Click **Delete** and **Refresh**.

To delete all Split DNS entries:

1. Click **Delete All**.

Configuring Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change.

Topics:

- [About Dynamic DNS](#)
- [Dynamic DNS Profiles](#)
- [Configuring Dynamic DNS Profiles](#)
- [Editing Dynamic DNS Profiles](#)
- [Deleting Dynamic DNS Profiles](#)

About Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, if a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Refer to the use policies posted on the provider's pages and abide by the guidelines. SonicWall does not provide technical support for DDNS providers; the providers themselves must be contacted.

Dynamic DNS is supported for both IPv4 and IPv6.

Topics:

- Supported DDNS Providers

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the services from providers listed here:

dns.org	SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org .
changeip.com	A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
no-ip.com	Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
Yi.org	Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Some common additional services offered by Dynamic DNS providers include:

Wildcards	Allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, for example, server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org.
Mail Exchangers	Creates MX record entries for your domain so that SMTP servers can locate it through DNS and send mail. NOTE: Inbound SMTP is frequently blocked by ISPs. Check with your provider before attempting to host a mail server.
Backup MX (offered by dns.org, yi.org)	Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
Groups	Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
Off-Line IP Address	Allows for the specification of an alternative address for your registered host names if primary registered IP is offline.

For information on setting up DDNS Profiles, refer to [Configuring Dynamic DNS](#).

Dynamic DNS Profiles

The **Dynamic DNS Profiles** table provides information about configured DDNS profiles.

View IP Version	Allows you to toggle the table between IPv4 and IPv6 DDNS profiles.	
Profile Name	Name assigned to the DDNS entry during its creation. This can be any value and is used only for identification.	
Domain	Fully qualified domain name (FQDN) of the DDNS entry.	
Provider	DDNS provider with whom the entry is registered.	
Status	Last reported/current status of the DDNS entry:	
	Online	DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
	Taken Offline Locally	DDNS entry is administratively offline. If the entry is enabled, the action configured in the Offline Settings section of the Advanced page of Add DDNS Profile is taken.
	Abuse	DDNS provider has considered the type or frequency of updates to be abusive. Check with the DDNS provider's guidelines to determine what is considered abuse.
	No IP change	Abuse possible. A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates only occur when address or state changes occur. Manual or forced updates should only be made when absolutely necessary, such as when registered information is incorrect.
	Disabled	Account has been disabled because of a configuration error or a policy violation. Check the profile's settings and verify the DDNS account status with the provider.
	Invalid Account	Account information provided is not valid. Check the profile's settings and verify the DDNS account status with the provider.
	Network Error	Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
	Provider Error	DDNS provider is unable to perform the requested action at this time. Check the profile's settings and verify the DDNS account status with the provider. Try the action again later.
	Not Donator Account	Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Check with the provider for more details on which services may require payment or donation.
Enabled	When selected, this profile is administratively enabled, and the network security appliance takes the Online Settings action configured on the Advanced page of Add DDNS Profile . This setting can also be controlled using the Enable this DDNS Profile option of the entry's Add DDNS Profile . Deselecting this option disable the profiles, and no communications with the DDNS provider occurs for this profile until the profile is again enabled.	

Online	When selected, this profile is administratively online. The setting can also be controlled using the Use Online Settings option on the entry's Add DDNS Profile . Deselecting this option while the profile is enabled takes the profile offline, and the network security appliance takes the Offline Settings action that is configured on the Advanced page.
Configure	Includes the Edit icon for configuring the DDNS profile settings and the Delete icon for deleting the DDNS profile entry.

Topics:

- [Configuring Dynamic DNS Profiles](#)
- [Editing Dynamic DNS Profiles](#)
- [Deleting Dynamic DNS Profiles](#)

Configuring Dynamic DNS Profiles

For general information on setting up DDNS Profiles, refer to [Configuring Dynamic DNS](#).

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the various providers listed in Dynamic DNS providers. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically add or manage) and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **NETWORK | DNS > Dynamic DNS** page provides the settings for configuring your SonicWall network security appliance to use your DDNS service.

To configure Dynamic DNS on the SonicWall Security Appliance:

1. Navigate to **NETWORK | DNS > Dynamic DNS**.
2. Click **+Add**. The **Add DDNS Profile** dialog displays.
3. If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the network security appliance takes the actions defined in the **Online Settings** section on the **Advanced** page. This option is selected by default.
4. If **Use Online Settings** is checked, the profile is administratively online. This option is selected by default.
5. Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table. The minimum length is one character, and the maximum length is 63 characters.
6. From **Provider**, select the dynamic DNS provider; these providers are described in [Supported DDNS Providers](#). The default is **dyn.com**.
 (i) | IMPORTANT: You must have created a dynamic service record with the DNS provider you select.
 (i) | TIP: Not all options are available for all DNS providers. Also, the **Note** at the bottom of the page displays whether the DNS provider uses HTTP or HTTPS protocol along with a link to the provider's website.

7. In the **User Name** field, enter the username for your DNS-provider account. The minimum length is 1 character, and the maximum length is 63 characters.
8. In the **Password** field, enter your DNS password. The minimum length is one character, and the maximum length is 31 characters.
9. In the **Domain Name** field, enter the fully qualified domain name (FQDN) of the host name you registered with the DNS provider. Make sure you provide the same host name and domain as you configured. The minimum length is one character, and the maximum length is 63 characters.
10. Optionally, to assign this DDNS profile to a specific WAN interface, select that WAN interface from **Bound to**. If you are configuring multiple-WAN load balancing, this option allows you to advertise a predictable IP address to the DDNS service. By default, this is set to **ANY**, which means the profile is free to use any of the WAN interfaces on the network security appliance.
11. If you selected **dyn.com** for **Provider**, go to Step 13.
12. When using **dyn.org**, select the service type that corresponds to your type of service from **Service Type**:

Dynamic	Free Dynamic DNS service. This is the default.
Custom	Managed primary DNS solution that provides a unified primary/secondary DNS service and a Web-based interface. Supports both dynamic and static IP addresses.
Static	Free DNS service for static IP addresses.

13. Click **Advanced**.
14. The **Online Settings** section provides control over what address is registered with the dynamic DNS provider. Choose:

Let the DDNS provider detect the IP Address	The Security Appliance allows the DNS provider to specify the IP address ① NOTE: IPv4 only. This option is selected by default.
Automatically set IP Address to the Primary WAN Interface IP Address	Causes the Security Appliance to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly. This option is selected by default. ① NOTE: In IPv6: This option is selected by default.
Specify IP Address manually	Allows for the IP address to be registered to be manually specified and asserted.

15. The **Offline Settings** section controls what IP address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the network security appliance. Choose:

Do nothing	Allows the previously registered address to remain current with the dynamic DNS provider. This option is selected by default.
-------------------	---

Use the Off-line IP address previously configured at Provider's site	If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.
Make Host Unknown	Hides the name of the DDNS service.
Specify IP Address manually	Allows for the IP address to be registered to be manually specified and asserted.

16. Click **Add**.

Editing Dynamic DNS Profiles

To edit a DDNS profile:

1. Navigate to **NETWORK | DNS > Dynamic DNS**.
2. In the **Dynamic DNS Profiles** table, click the **Edit** icon of the profile. The **Edit DDNS Profile** dialog displays.
3. Make changes. For a description of the options, follow the instructions for [Configuring Dynamic DNS Profiles](#).
4. Click **Save**.

Deleting Dynamic DNS Profiles

You can delete one or all DDNS profiles.

To delete a DDNS profile:

1. Navigate to **NETWORK | DNS > Dynamic DNS**.
2. Click the **Delete** icon of the profile to be deleted. A confirmation message displays.
3. Click **OK**.

To delete all DDNS entries:

1. Navigate to **NETWORK | DNS > Dynamic DNS**.
2. Select the profiles you want to delete.
3. Click **Delete All**. A confirmation message displays.
4. Click **OK**.

Configuring DNS Proxy Settings

Topics:

- [About DNS Proxy](#)
- [Enabling Log Settings](#)
- [Monitoring Packets](#)
- [Configuring DNS Proxy Settings](#)

About DNS Proxy

An IPv4 interface can do name resolution on an IPv4 Internet, and an IPv6 interface can only do name resolution on an IPv6 Internet through DNS proxy. To allow IPv4 clients to access DNS services in a network with mixed IPv4 and IPv6 interfaces, SonicOS supports DNS proxy.

The DNS proxy feature provides a transparent mechanism that allows devices to proxy hostname resolution requests on behalf of clients. The proxy can use existing DNS cache, which is either statically configured by you or learned dynamically, to respond to the queries directly.

The proxy can redirect the DNS queries selectively to specific DNS servers, according to partial or complete domain specifications. This is useful when VPN tunnels or PPPoE virtual links provide multiple network connectivity, and it is necessary to direct some DNS queries to one network, and other queries to another network.

With DNS Proxy, LAN Subnet devices use the SonicWall network security appliance as the DNS Server and send DNS queries to the network security appliance. The network security appliance proxies the DNS queries to the real DNS Server. In this way, the network security appliance is the central management point for the network DNS traffic, providing the ability to manage the DNS queries of the network at a single point.

ⓘ | NOTE: To maintain security, an incoming DNS Query is proxied only after Access Rule and DPI checking.

About the access rule, behavior depends on the device mode:

On global mode devices:

Access rules will be auto-added according to the DNS rule configurations.

On policy mode devices:

Access rules need to be manually added after enabling DNS rules. Navigate to **POLICY | Rules and Policies > DNS Rules** page to enable DNS rules. For more information about DNS Rules, refer to *Rules and Policies guide*.

Topics:

- [Supported Interfaces](#)
- [DNS Server Liveness Detection and Failover](#)
- [DNS Cache](#)
- [High Availability Stateful Synchronization of DNS Cache](#)

Supported Interfaces

The DNS proxy feature is supported on:

- Physical interfaces
- VLAN interfaces
- VLAN trunk interfaces

The zone for each interface should only be:

- LAN
- DMZ
- WLAN

DNS Server Liveness Detection and Failover

When multiple DNS servers are configured, to determine the “best” server, SonicOS considers these factors:

- DNS server priority
- DNS server status (up, down, unknown)
- Time duration after failover

DNS Cache

In DNS Proxy, a DNS cache memory saves the most commonly used domains and host addresses, and when it receives the DNS query that match the domain in DNS cache, the firewall directly responds to clients by using the cache records, without processing DNS query and reply proxy.

There are two kinds of DNS Cache:

Static	Manually configured by you.
Dynamic	Auto-learned by the GMS. For each DNS Query, the SonicOS DNS Proxy does the deep inspection on the URI and records the valid response to the caches.

When a DNS query matches an existing cache entry, the SonicOS DNS Proxy responds directly with the cached URI. This usually decreases the network traffic and, therefore, improves overall network performance.

Static DNS Cache Size

Static DNS cache entry size is always 256 regardless of platform. The static DNS cache is never be deleted unless it is done manually.

Dynamic DNS Cache Size

Dynamic DNS cache size depends on the platform. Some examples are shown here:

Platform	Maximum Cache Size
SM 9400	4096
SM 9600	
SM 9200	2048
NSA 4600	2048
NSA 5600	
NSA 6600	
NSA 2600	1024
NSA 3600	
TZ600	512
TZ300/TZ300W	512
TZ400/TZ400W	
TZ500/TZ500W	

If the maximum DNS cache size has been reached when the network security appliance attempts to add an entry to it, the network security appliance will:

1. Delete the DNS cache entry with the earliest expire time.
2. Add the new DNS cache entry.

High Availability Stateful Synchronization of DNS Cache

DNS proxy supports stateful synchronization of DNS cache. When the DNS cache is added, deleted, or updated dynamically, it synchronizes to the idle firewall.

DHCP Server

Configure DNS Proxy on the **POLICY | Rules and Policies> DNS Rules** page. Navigate to **NETWORK | System> DHCP Server**, you have to manually configure the interface IP as DNS server in **DHCP Server Lease Scope** tab. Click **Add Dynamic**.

In the **Dynamic Range Configuration** dialog, enable **Specify manually** option and the DNS server IP is added manually into the **DNS/WINS** page. For more information about configuring the DHCP server, refer to [Configuring DNS Settings](#).

Enabling Log Settings

Several events logs are related to DNS Proxy and need to be configured. For more information refer to [SonicOS 7.1 Device log Guide](#).

Monitoring Packets

The process of DNS Proxy is monitored with **MONITOR > Tools & Monitors > Packet Monitor**. For information refer to [SonicOS 7.1 Monitoring Guide](#).

Configuring DNS Proxy Settings

Topics:

- [Configuring DNS Proxy Settings](#)
- [Viewing and Configuring Static DNS Cache Entries](#)
- [Deleting Static DNS Cache Entries](#)
- [Viewing DNS Proxy Cache Objects](#)
- [Flushing Dynamic DNS Cache Entries](#)

Configuring DNS Proxy Settings

To configure DNS Proxy:

1. Navigate to **POLICY | Rules and Policies> DNS Rules** page to configure DNS Proxy. For more information about DNS Rules, refer to *Rules and Policies guide*.
2. From the **Adding DNS Policy** option, to use UDP only or UDP and TCP. Choose the following Service from the Source/Service tab:
 - **DNS (Name Service)**
 - **DNS (Name Service) TCP**
 - **DNS (Name Service) UDP**
3. For DNS over UDP requests only, select **Enforce DNS Proxy for All DNS Requests**. This option is not selected by default

4. For DNS over UDP requests only, select **Enable DNS Proxy Cache**. This option is not selected by default.
5. Click **Accept**.

To configure Split DNS servers, refer to [Configuring Domain-Specific DNS Servers for Split DNS](#).

Deleting Static DNS Cache Entries

To delete a static DNS cache entry:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Select Static DNS Cache entry that you want to delete.
4. Click the **Delete** icon associated with the entry.

To delete two or more static DNS cache entries:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Select the checkboxes of the entries to be deleted. **Delete** becomes available.
4. Click **Delete** or the **Delete** icon in the **Configure** column.

To delete all static DNS cache entries:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Click the top checkbox next to the **Domain Name** column. All entries are selected.
4. Click **Delete**.

Viewing DNS Proxy Cache Objects

View IP Version	Select either IPv4 or IPv6.
Domain Name	Name of the DNS Server.
Type	Dynamic or Static.
IP Address	IPv4 or IPv6 address of the DNS Server.
Time to Leave	Either: <ul style="list-style-type: none">• Expires in n minutes x seconds (Dynamic DNS)• Expired (Dynamic DNS)• Permanent (Static DNS)
Flush	Flush icon for each entry.

Dynamic DNS cache is added automatically during the DNS Proxy process; static DNS cache is added when you configure it. Dynamic DNS cache has a TTL value and can be flushed. Static DNS cache must be deleted (refer to [Deleting Static DNS Cache Entries](#)).

Flushing Dynamic DNS Cache Entries

To flush a dynamic DNS cache entry:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Select the entry you want to flush.
4. Click the **Flush** icon associated with the entry.

To flush two or more dynamic DNS cache entries:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Select the checkboxes of the entries to be deleted. **Flush** becomes available.
4. Click **Flush**.

To flush all dynamic DNS cache entries:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Click the **Static DNS Proxy Cache Entries** tab.
3. Click **Flush All**.

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 Administration Guide

Updated - December 2023

Software Version - 7.1

232-005873-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

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