SonicOS and SonicOSX 7

Network DNS

Administration Guide

SONICWALL®

Contents

1

Configuring DNS Settings

ⓘ | **NOTE:** References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.

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. **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

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

Specifying which DNS Servers are Used

Regardless of the IP version, you can specify how SonicOS/X selects the DNS servers. The method is the same for both IP versions.

To specify which DNS servers are used:

1. Navigate to **NETWORK | DNS > Settings**.
2. In the **IPv4 DNS Settings** or **IPv6 DNS Settings** section (depending on which version you chose), 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 IPv4/IPv6 DNS Settings Dynamically from WAN Zone**. This is the default. The IP address(es) are populated into the **DNS Server** fields automatically.
3. If you selected **IPv6**, and want to use ONLY IPv6 servers, select **Prefer IPv6 DNS Servers**. This option is not selected by default.

    SonicOS/X 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.

    △ | **CAUTION: Select this option only if you have configured the IPv6 DNS server correctly.**
4. 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 IPv4 or IPv6.

To enable the proxying of split DNS servers:

1. Navigate to **NETWORK | DNS > Settings**.
2. Scroll to the **Split DNS** section.
3. Select **Enable proxying of split DNS servers**. This option is selected by default.
4. 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. Scroll to the **DNS Rebinding Attack Prevention** section.
3. Select **Enable DNS Rebinding Attack Prevention**. This option is not selected by default. The two options become available.
4. 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** (default)
5. 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…**.
6. Click **Accept**.

DNS Rebinding and Cache Lookup

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

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/X 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/X 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. Scroll to the **DNS host name lookup over TCP for FQDN** section.
3. Select **Enable DNS host name lookup over TCP for FQDN**. This option is not selected by default.
4. 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: • Forward DNS cache, the host name. • Reverse DNS cache, a string representation of the IP address.
DNS Name	Domain name, such as `www.SonicWall.com`, 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/X selects the DNS servers. The method is the same for both IP versions.

To specify which DNS servers are used:

1. Navigate to **NETWORK | DNS > Settings**.
2. In the **IPv4 DNS Settings** or **IPv6 DNS Settings** section (depending on which version you chose), 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 IPv4/IPv6 DNS Settings Dynamically from WAN Zone**. This is the default. The IP address(es) are populated into the **DNS Server** fields automatically.
3. If you selected **IPv6**, and want to use ONLY IPv6 servers, select **Prefer IPv6 DNS Servers**. This option is not selected by default.

    SonicOS/X 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.

    △ | **CAUTION: Select this option only if you have configured the IPv6 DNS server correctly.**
4. 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 IPv4 or IPv6.

To enable the proxying of split DNS servers:

1. Navigate to **NETWORK | DNS > Settings**.
2. Scroll to the **Split DNS** section.
3. Select **Enable proxying of split DNS servers**. This option is 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/X 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/X 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. Scroll to the **DNS host name lookup over TCP for FQDN** section.
3. Select **Enable DNS host name lookup over TCP for FQDN**. This option is not selected by default.
4. Click **Accept**.

Configuring Domain-Specific DNS Servers for Split DNS

You can optionally configure separate domain-specific DNS servers.

Domain	Name of the DNS Server.

DNS Servers	IPv4/IPv6 IP address of the DNS Server. **NOTE:** The status of the DNS servers is displayed on the **NETWORK | DNS > DNS Proxy** page.
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/X 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 Se 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.

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:

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:
   - **Primary Server (v4/v6)**
   - **Secondary Server (v4/v6)** (optional)
   - **Tertiary Server (v4/v6)** (optional)
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.
      ⓘ | **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 checkboxes of the entries to be deleted. **Delete** becomes available.
2. Click **Delete**.

To delete all Split DNS entries:

1. Click **Delete All**.

2

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 (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, is 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/X currently supports the services from providers listed here:

dns.org	SonicOS/X 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/X configuration.
no-ip.com	Dynamic DNS service requiring only username, password, and domain name for SonicOS/X configuration. Also supports hostname grouping.
Yi.org	Dynamic DNS service requiring only username, password, and domain name for SonicOS/X 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

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/X. 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**.

   ⓘ **IMPORTANT:** You must have created a dynamic service record with the DNS provider you select.

   ⓘ **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**.

    ⓘ | **TIP:** You can usually leave the default settings on this page.
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 ⓘ | **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. ⓘ | **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**.

3

Configuring DNS Proxy Settings

Topics:

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/X 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.

When DNS proxy is enabled on an interface, one Allow Rule is auto-added by SonicOS/X.

When **DNS Proxy over TCP** is enabled, another Allow Rule is auto-added.

Topics:

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/X 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/X 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/X 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 SM 9600	4096
SM 9200	2048
NSA 4600 NSA 5600 NSA 6600	2048
NSA 2600 NSA 3600	1024
TZ600	512
TZ300/TZ300W TZ400/TZ400W TZ500/TZ500W	512

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

When DNS Proxy is enabled on an interface, the device needs to push the interface IP as a DNS server address to clients, so the DHCP server must be configured manually, using the interface address as the DNS Server 1 address in the DHCP Server settings on DNS/WINS. The **Interface Pre-Populate** option in the **Dynamic Range**

Configuration dialog makes this easy to configure; if the selected interface has enabled DNS Proxy, the DNS server IP is added automatically 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.

Monitoring Packets

The process of DNS Proxy is monitored with **MONITOR > Tools & Monitors > Packet Monitor**.

Configuring DNS Proxy Settings

Topics:

Enabling DNS Proxy

Enabling DNS Proxy must be done first globally on the **NETWORK > DNS > DNS Proxy** page and then again on each interface. This provides a gradual control to enable the feature for different network segments independently.

To enable DNS Proxy:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. Select **Enable DNS proxy**. This option is not selected by default.
3. Click **Accept**.
4. Navigate to **NETWORK > System > Interfaces**.
5. For each interface on which to enable DNS Proxy:

a. Click the **Edit** icon for the interface on which to enable DNS Proxy. The **Edit Interface** dialog displays.

b. Click **Advanced**.

c. Select **Enable DNS Proxy**. This option displays only when DNS Proxy is enabled globally.

d. Click **OK**.

6. Click **Accept**.

Configuring DNS Proxy Settings

To configure DNS Proxy:

1. Navigate to **NETWORK | DNS > DNS Proxy**.
2. From the **DNS Proxy Mode** options, choose the IP version for sending/receiving DNS Proxy packets between the firewall and the DNS Servers:
   - **IPv4 to IPv4** (default)
   - **IPv4 to IPv6**
3. From the **Enforce DNS Proxy For All DNS Requests** option, choose the protocol for sending/receiving DNS Proxy packets between the firewall and the DNS Servers:

   ⓘ **NOTE:** DNS Proxy protocol is an advanced setting. For more information about configuring this setting, contact SonicWall Technical Support.

   - **UDP and TCP** (default)
   - **UDP only**
4. To allow all DNS Proxy requests regardless of destination, select **Enforce DNS Proxy for All DNS Requests**. If this option is disabled, only DNS Proxy requests destined for SonicWall network security appliances are processed. This option is not selected by default.
5. For DNS over UDP requests only, select **Enable DNS Proxy Cache**. This option is not selected by default.
6. 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: • 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 D 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**.

4

Configuring DNS Security

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

Topics:

About DNS Sinkholes

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

Configuring DNS Security Settings

To configure DNS Security settings:

1. Navigate to **NETWORK | DNS > DNS Security**.
2. Select **Enable DNS Sinkhole Service**. This option is not selected by default.
3. 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**: Enter the IPv4 and IPv6 addresses in the fields that become visible.

4. Click **Accept**.
5. Click the **Custom Malicious Domain Name** tab.
6. 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**.
7. Click the **White List** tab.
8. 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 whitelist domain name.
    c. Click **Save**.
9. Click **Update** to save your changes.

Deleting Entries in the Lists

To delete the entries in a list:

1. Navigate to **NETWORK | DNS > DNS Security**.
2. 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.
3. 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/X 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/X logs whenever suspicious DNS packets are dropped.

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

Topics:

Configuring DNS Tunneling Detection

To configure DNS tunneling detection:

1. Navigate to **NETWORK | DNS > DNS Security**.
2. Click the **DNS Tunnel Detection** tab.
3. To enable DNS tunnel detection, select **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**.

Viewing Detected Suspicious Clients

SonicOS/X 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 **NETWORK | DNS > DNS Security**.
2. 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 Tunneling 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, MX
Interface	Interface on which the host establishing the DNS tunnel was detected
Block	Indicates whether the host was blocked

Creating DNS Tunnel Detection White Lists

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 **NETWORK | DNS > DNS Security**.
2. Click on the **White List for DNS Tunnel Detection** tab.
3. 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**.
4. Click **Accept**.

Deleting DNS Tunnel Detection White List Entries

To delete all DNS tunnel detection white list entries:

1. Navigate to **NETWORK | DNS > DNS Security**.
2. Click the **White List for DNS Tunnel Detection** 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**.

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
- 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

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.

SonicOS and SonicOSX Network DNS Administration Guide
Updated - February 2022
Software Version - 7
232-005331-00 Rev C

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