SonicWall® Management Services WAN Acceleration Setup

Administration

Contents

2

Configuring WAN Acceleration

ⓘ **IMPORTANT:** If WAN Acceleration is not licensed, it is not listed in the navigation panel. WAN Acceleration is configured on the unit level only.

SonicWall NSA and TZ series appliances configured with WXA series appliances can be managed through SonicWall® (Management Service) to accelerate WAN traffic using Transmission Control Protocol (TCP), Windows File Sharing (WFS), and the Web Cache. The Management Service management interface allows you to configure basic WAN Acceleration settings and view the WAN Acceleration status.

Topics:

- On the Status Page
- Using Firewall Sandwich
- HTTP/HTTPS Redirection

On the Status Page

The **WAN Acceleration > Status** page gives you the option to configure a network interface for WAN Acceleration, enable WAN Acceleration for NetExtender, and view the status of the TCP Acceleration, WFS Acceleration, and Web Cache services.

To configure WAN Acceleration:

1 Navigate to the **Network > Interfaces** page.

2 Click the **Edit** icon for the interface to which you want the WXA series appliance to connect.

3 Complete these options:

   - **Zone**: drop-down menu— *LAN*
   - **Mode/IP Assignment**: drop-down menu — *Static IP Mode*
   - IP **Address**: field — Enter the IP Address for the port. This example uses *10.203.30.162*.
   - **Subnet Mask**: field — Enter the subnet mask for the port.
   - (Optional) **Comment**: field — Enter text that describes the device. For example, *WXA connection*.
   - (Optional) **Management**: checkboxes — Select the management methods.
   - Click **OK**.

4 Navigate to the **DHCP > Settings** page.

   ⓘ **NOTE:** Configuring DNS is only required if you plan to use WFS Acceleration for Signed SMB. This example assumes that the correct DNS server has already been entered in the **FIREWALL | Mange > Network > DNS** page. If you have not entered the DNS server, you can overwrite the DNS specified in the **Network > DNS** page. Enter the **DNS IP Addresses** in the text fields provided.

5 Connect an Ethernet cable from the WXA series appliance to the X5 port on the NSA/TZ security appliance.

6 Navigate to **WAN Acceleration > Status** page.

7 Select **Enable WAN Acceleration**.

8 From the **WXA Interface** drop-down menu, select the interface to which the WXA series appliance is connected.

9 To enable NetExtender to accelerate WAN traffic, click **Enable NetExtender WAN Acceleration Client (WXAC**).

10 Click **Update**. The **Modify Task Description and Schedule** dialog displays.

11 Click **Accept**.

12 Confirm that the NSA/TZ series appliance has a DCHP lease for the WXA series appliance by navigating to the **Network > DHCP Server** page.

13 Navigate to **WAN Acceleration > Status**.

14 Click **Create static DHCP lease for WXA**. A DHCP lease is set for the WXA series appliance. The **Modify Task Description and Schedule** dialog displays; see Step 1 through Step 11.

15 Verify that the lease was created by navigating to the **Network > DHCP Server** page and checking that a dynamic range is set for the WXA appliance.

Using Firewall Sandwich

You can deploy and configure a SonicWall™ Firewall Sandwich to improve availability, scalability, and manageability across the IT infrastructure. Deployment of the Firewall Sandwich provides these features:

- **Scalability** - add more capacity as you go, reusing existing equipment
- **Redundancy and resiliency** – primary and secondary components
- **Inline upgrades** – upgrade firewalls and switches without shutting down the system
- **Single point of management** - manage policies for multiple firewall clusters and blades
- **Full security services** - including DPI-SSL capability

Firewall Sandwich deployment and configuration can be implemented using the following supported equipment and services:

- SonicWall Force10 S series switches, such as the S5000, S4810, S4048, or S6000 running FTOS v9.8+
- SonicWall NSA 2600 (and higher) appliances or SuperMassive series appliances.
- SonicWall services, such as GAV, IPS, ASPR, DPI-SSL, and CFS in conjunction with Single Sign-On All in Wire Mode.

HTTP/HTTPS Redirection

When the firewall configuration requires user authentication, HTTP/HTTPS traffic from an unauthenticated source is redirected to the Management Service login screen for the user to enter their credentials. A problem occurs when HTTP and HTTPS traffic arrive from sources from which users do not log in, and one or more such sources repeatedly tries to open new connections, which keeps triggering this redirection. These could be non-user devices that are validly trying to get access or could be malicious code attempting a Denial of Service (DOS) attack. The effect that it has on the firewall is to cause high CPU load in the CP, both in the data plane task initiating the redirections and in the web server thread tasks that are serving up the target redirect pages.

To minimize this effect, ensure the **Add rule to enable redirect from HTTP to HTTPS** option on the **Add/Edit Interface** dialog is selected when adding or editing an interface. Enabling this option causes Management Service to add an access rule that allows HTTP to the interface; a side effect of this rule is that it also allows Management Service to be able to redirect HTTPS to HTTP in certain cases without security issues. One such case is the first step of redirecting traffic that needs to be authenticated, at which point there is no sensitive data that needs to be hidden. Then, HTTP processing can occur on the data plane (DP) rather than on the CP.

ⓘ **NOTE:** This option is not available when adding or editing VPN tunnel interfaces or when Wire Mode (2-Port Wire), Tap Mode (1-Port Tap), or PortShield Switch Mode is selected for Mode/IP Assignment.

3

Configuring TCP Acceleration

The Configuration page gives you the option to select the mode, service object, and address object or group that are always excluded from the TCP Acceleration service.

To configure TCP Acceleration:

1. Navigate to the **WAN Acceleration > TCP Acceleration** page.
2. In the **WXA Groups** section, click **Add New Group**. The **Add Group** dialog displays.
3. Ensure **TCP** is displayed.
4. Select **Enable TCP Acceleration**.
5. Select an acceleration mode from **TCP Acceleration Mode**:
   - **All TCP services except those excluded by default** (default)
   - **All TCP services except those specified in the Service Object**
   - **All TCP services except those specified in the Service Object and those excluded by default**
   - **Only TCP services specified in the Service Object**
6. Select an Acceleration Service Object from **TCP Acceleration Service Object**. The default is **AD Directory Services**.

   ⓘ **TIP: TCP Acceleration Service Objec**t option may be greyed out if the selected TCP Acceleration mode does not support it.

   ⓘ **NOTE:** To view a list of, create, and edit service objects, navigate to the **Firewall > Address Objects** page.
7. Select an excluded Address Object from **Address Objects always excluded**. The default is **None**.

   ⓘ **TIP:** To add an address object to the drop-down list, navigate to **Firewall > Address Objects** and create new address objects.
8. Click **Group**.
9. Enter a name for the group in the **Name** field.
10. To specify this group as the default group, select **Use as default group**.
11. Click **OK**. The **Modify Task Description and Schedule** dialog displays.
12. Click **Accept**. The group is added to the **WXA Groups** table on the **TCP Acceleration** page.

4

Configuring WFS Acceleration

The **WFS Acceleration** page provides details on configuring the WFS Acceleration service. There are several different ways to configure WFS Acceleration depending on the user requirements and type of network environment used:

Unsigned SMB In a network that supports unsigned SMB traffic, the WFS Acceleration service configuration is greatly simplified. The reason for this is unsigned SMB traffic does not have a security layer, so the WXA series appliance can intercept the traffic without joining the domain, eliminating the need to configure custom zones, configuring reverse lookup, and add file shares. Unsigned SMB is enabled by default.

Support SMB Signing In a network that supports SMB signing, it is required that the WXA series appliance join the domain, because of the presence of a security layer in signed SMB traffic. Although this type of configuration is more complex than unsigned SMB, it offers a more granular configuration of the WFS Acceleration service.

To configure WFS Acceleration:

1. Navigate to the **WAN Acceleration > WFS Acceleration** page.
2. In the **WXA Groups** section, click **Add New Group**. The **Add Group** dialog displays.
3. Select **Enable WFS Acceleration**.
4. Click **Group**.
5. Enter a name for the group in the **Name** field.
6. To specify this group as the default group, select **Use as default group**.
7. Click **OK**. The **Modify Task Description and Schedule** dialog displays.
8. Click **Accept**. The group is added to the **WXA Groups** table on the **WFS Acceleration** page.

5

Configuring the Web Cache

The Web Cache feature stores copies of Web pages passing through the network that are frequently and recently requested. So when a user requests one of these Web pages, it is retrieved from the local Web cache instead of the Internet, saving bandwidth and response time.

Consider the following when configuring the Web Cache service:

- When **Web Cache** is enabled, the Web Proxy fields are automatically populated in the **Network > Web Proxy** page.
- There is no need to configure the HTTP clients with proxy settings because the NGFW transparently redirects standard HTTP connections onto the proxy.
- When the Web Cache is enabled, the NGFW disables redirection of HTTP connections to the WXA series appliance if it becomes unavailable.
- The Web Cache service is not available in WXA 500 Live CD Memory Mode.

To enable the Web Cache:

1. Navigate to the **WAN Acceleration > Web Cache** page.
2. In the **WXA Groups** section, click **Add New Group**. The **Add Group** dialog displays.
3. Select **Enable Web Cache**.
4. From **Web Server Ports**, select the type of port service. **AD Directory Services** is the default.
5. From **Client Inclusion Address Object**, select the Address Object to be used. The default is **None**.
6. From **Server Exclusion Address Object**, select the Address Object to be excluded. The default is **None**.
7. Select the caching strategy from **Caching Strategy**:
    - **minimal** (default)
    - **moderate**
    - **aggressive**
8. Optionally enter the administrator’s email address in the **Administrator Email** field.
9. Click **Group**.
10. Enter a name for the group in the **Name** field.
11. To specify this group as the default group, select **Use as default group**.
12. Click **OK**. The **Modify Task Description and Schedule** dialog displays.

Click **Accept**. The group is added to the **WXA Groups** table on the **Web Cache** page.

6

SonicWall Support

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

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 video tutorials
- Access MySonicWall
- 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

Legend

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

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

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Management Services WAN Acceleration Setup Administration
Updated - October 2018
232-004551-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

Open Source Code

SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035