SonicOS 7.1

DPI-SSH

Administration Guide

Contents

1

About SonicOS

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

Topics:

Working with SonicOS

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

The SonicOS management interface facilitates:

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

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

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

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

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

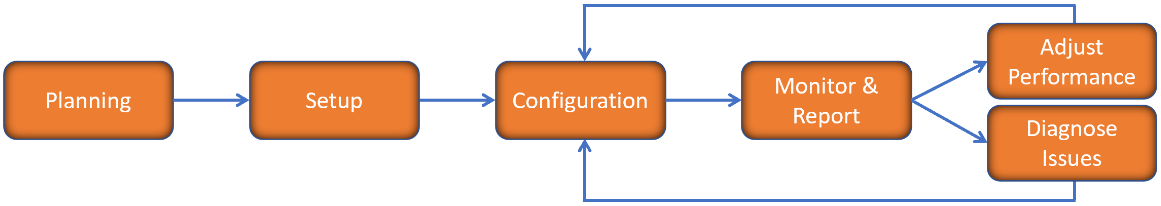
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide

- *SonicOS Command Line Interface Reference Guide*

SonicOS Workflow

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

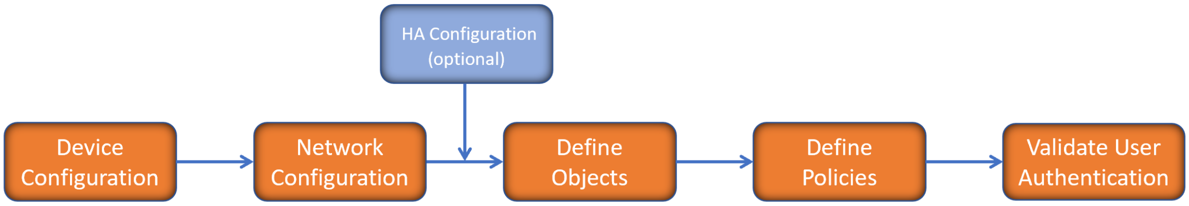


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting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

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

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

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

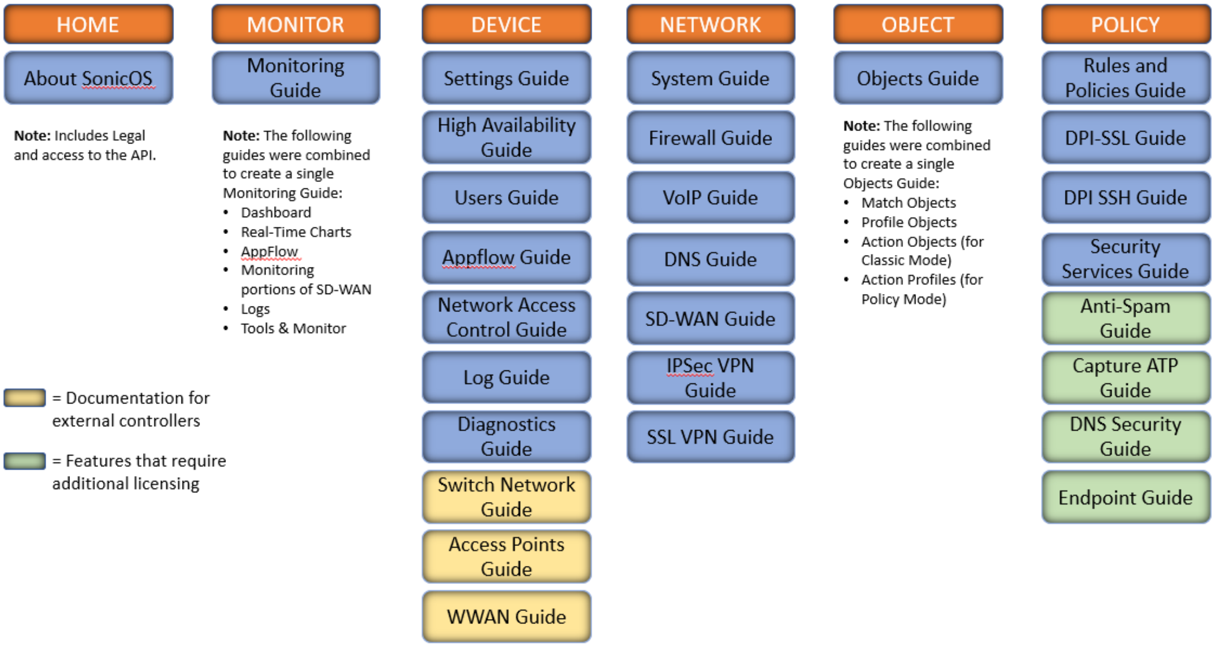


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement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

How to Use the SonicOS Administration Guides

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

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



HOME	MONITOR	DEVICE	NETWORK	OBJECT	POLICY
About SonicOS	Monitoring Guide	Settings Guide	System Guide	Objects Guide	Rules and Policies Guide
Note: Includes Legal and access to the API.	**Note:** The following guides were combined to create a single Monitoring Guide: • Dashboard • Real-Time Charts • AppFlow • Monitoring portions of SD-WAN • Logs • Tools & Monitor	High Availability Guide	Firewall Guide	**Note:** The following guides were combined to create a single Objects Guide: • Match Objects • Profile Objects • Action Objects (for Classic Mode) • Action Profiles (for Policy Mode)	DPI-SSL Guide
		Users Guide	VoIP Guide		DPI SSH Guide
		Appflow Guide	DNS Guide		Security Services Guide
		Network Access Control Guide	SD-WAN Guide		🟩 Anti-Spam Guide
		Log Guide	IPSec VPN Guide		🟩 Capture ATP Guide
		Diagnostics Guide	SSL VPN Guide		🟩 DNS Security Guide
		🟨 Switch Network Guide			🟩 Endpoint Guide
		🟨 Access Points Guide			
		🟨 WWAN Guide			

🟨 = Documentation for external controllers

🟩 = Features that require additional licensing

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

Guide Conventions

These text conventions are used in this guide:

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

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

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

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

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

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

2

About DPI-SSH

Deep Packet Inspection (DPI) technology allows a packet filtering-firewall to classify passing traffic based on signatures of the Layer 3 and Layer 4 contents of the packet. DPI also provides information that describes the contents of the packet's payload (the Layer 7 application data). DPI is an existing SonicOS feature that examines the data and the header of a packet as it passes through the SonicWall firewall, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet might pass or if it needs to be routed to a different destination for action or other tracking.

SSH (Secure Shell) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. SSH connects, by way of a secure channel over an insecure network—a server and a client running SSH server and SSH client programs, respectively. The protocol distinguishes between two different versions, referred to as SSH-1 and SSH-2. SonicWall only supports SSH-2; SSH-1 sessions are not intercepted and inspected.

ⓘ | **IMPORTANT:** SSH clients with different version numbers cannot be used at the same time.

To effectively inspect an encrypted message, such as SSH, the payload must be decrypted first. DPI-SSH works as a man-in-the-middle (MITM) or a packet proxy. Any preset end-to-end communication is broken, and preshared keys cannot be used.

DPI-SSH divides the one SSH tunnel into two tunnels as it decrypts the packets coming from both tunnels and performs the inspection. If the packet passes the DPI check, DPI-SSH sends the re-encrypted packet to the tunnels. If the packet fails the check, it is routed to another destination, based on the policies, or submitted for collecting statistical information, and DPI-SSH resets the connection.

Topics:

- Supported Clients/Servers and Connections
- Supported Key Exchange Algorithms
- Caveats

Supported Clients/Servers and Connections

SSH is not a shell, but a secure channel that provides different services over this channel (tunnel), including shell, file transfer, or X11 forwarding.

DPI-SSH supports both route mode and Wire Mode. For Wire Mode, DPI-SSH is only supported in the secure (active DPI of inline traffic) mode. For route mode, there is no limitation.

SSH supports different client and server implementations, as listed in Supported Clients/Servers.

SUPPORTED CLIENTS/SERVERS

DPI-SSH Client Supported	DPI-SSH Servers Supported
SSH client for Cygwin	SSH server on Fedorz
Putty	SSH server on Ubuntu
secureCRT	
SSH on Ubuntu	
SSH n centos	
SFTP client on Cygwin	
SCP on Cygwin	
Winscp	

DPI-SSH supports up to 250 connections.

Supported Key Exchange Algorithms

DPI-SSH supports these key exchange algorithms:

- Diffie-Hellman-group1-sha1
- Diffie-Hellman-group14-sha1
- ecdh-sha2-nistp256

DPI-SSH supports DSA keys on the client side and RSA keys on the server side.

Caveats

If there is already an SSH server key stored in the local machine, it must be deleted. For example, if you already SSH to a server, and the server DSS key is saved, the SSH session fails if the DSS key is not deleted from the local file.

The `ssh-keygen` utility cannot be used to bypass the password.

Putty uses GSSAPI. This option is for SSH2 only, which provides stronger encrypted authentication. It stores a local token or secret in the local client and server for the first time communication. It exchanges messages and operations before DPI-SSH starts, however, so DPI-SSH has no knowledge about what was exchanged before, including he GSSAPI token. DPI-SSH fails with the GSSAPI option enabled.

On the client side, either the SSH 2.x or 1.x client can be used if DPI-SSH is enabled. Clients with different version numbers, however, cannot be used at the same time.

Gateway Anti-Virus and Application Firewall inspections are not supported even if these options are selected on the **POLICY | DPI-SSH > Settings** page.

3

Configuring DPI-SSH

DPI-SSH provides deep packet inspection of encrypted information.

ⓘ **NOTE:** Gateway Anti-Spyware service is not compatible with DPI-SSH because TCP streams for anti-spyware are not supported. If the checkbox is checked, the system takes no action.

Topics:

- About DPI-SSH
- Activating Your DPI-SSH License
- Managing DPI-SSH

Activating Your DPI-SSH License

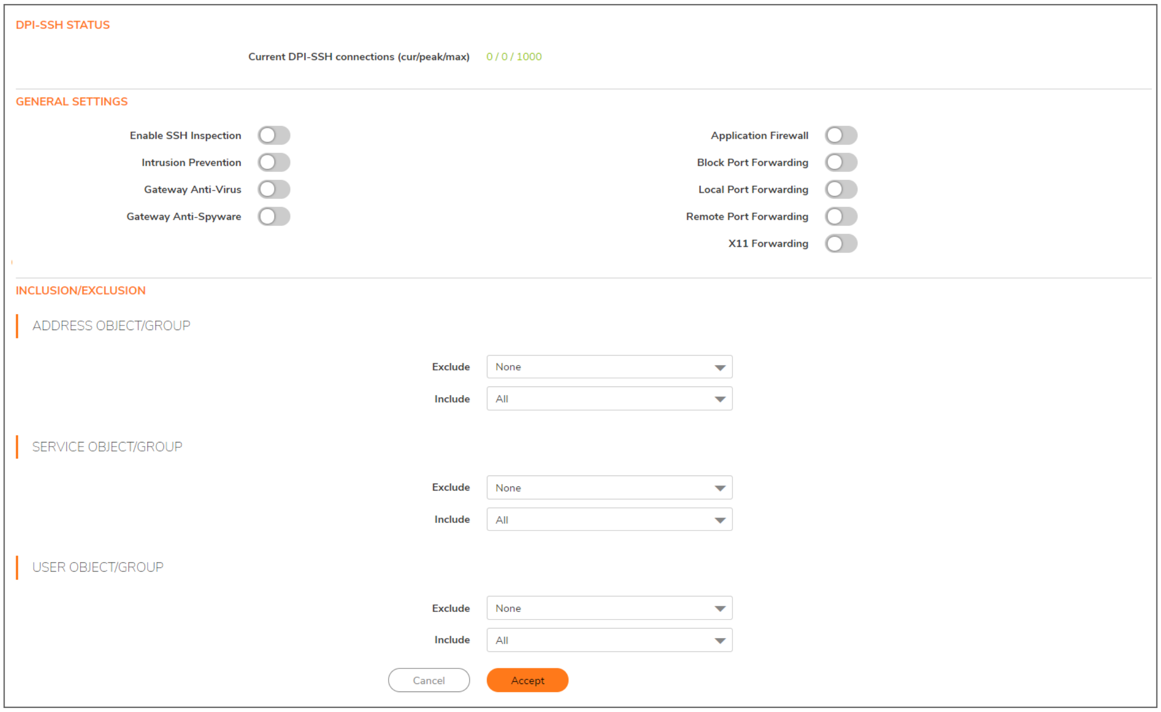
DPI-SSH is fully licensed by default, but you need to activate your license. When you first select **POLICY | DPI-SSH > Settings**, you receive the message: Upgrade Required.

If the upgrade is not required, skip to *Configuring DPI-SSH*. For information about activating your license, see the *Quick Start Guide* for your appliance.

Managing DPI-SSH

Gateway Anti-Virus service does not work for DPI-SSH because TCP streams for Anti-Spyware are not supported. If the checkbox is checked, the system takes no action.

Configure DPI-SSH on the **POLICY | DPI-SSH > Settings** page.



DPI-SSH STATUS

Current DPI-SSH connections (cur/peak/max) 0 / 0 / 1000

GENERAL SETTINGS

Enable SSH Inspection ○

Intrusion Prevention ○

Gateway Anti-Virus ○

Gateway Anti-Spyware ○

Application Firewall ○

Block Port Forwarding ○

Local Port Forwarding ○

Remote Port Forwarding ○

X11 Forwarding ○

INCLUSION/EXCLUSION

ADDRESS OBJECT/GROUP

Exclude: None

Include: All

SERVICE OBJECT/GROUP

Exclude: None

Include: All

USER OBJECT/GROUP

Exclude: None

Include: All

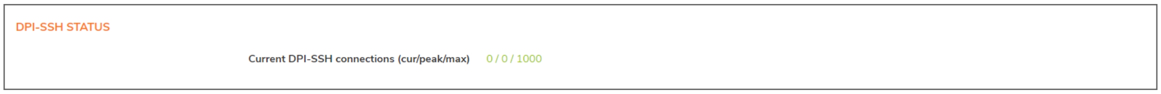
Topics:

- Viewing Connection Status
- Configuring Client DPI-SSH Inspection
- DPI-SSH Blocking of Port Forwarding
- Customizing Client DPI-SSH Inspection

Viewing Connection Status

To view the status of DPI-SSH connections:

1. Navigate to **POLICY | DPI-SSH > Settings**.
2. Scroll to **DPI-SSH Status.**

   DPI-SSH STATUS

   Current DPI-SSH connections (cur/peak/max) 0 / 0 / 1000

   The status displays the number of:

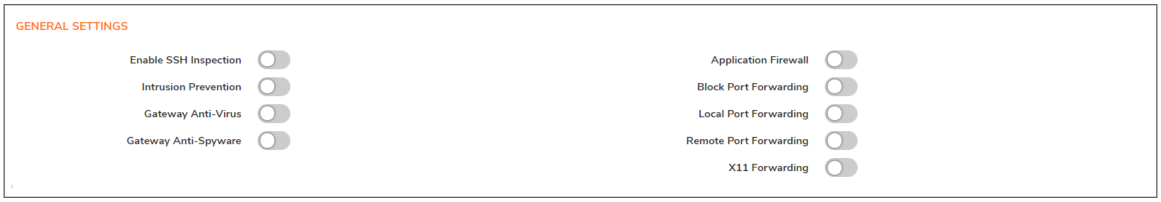
   - Current DPI-SSH connections
   - Peak DPI-SSH connections
   - Maximum number of DPI-SSH connections

Configuring Client DPI-SSH Inspection

You configure Client DPI-SSH inspection in the General Settings section of Decryption Services > DPI-SSH.

To enable Client DPI-SSH inspection:

1. In the **General Settings** section, select the **Enable SSH Inspection** option. This option is not selected by default.



GENERAL SETTINGS

Enable SSH Inspection ○
Intrusion Prevention ○
Gateway Anti-Virus ○
Gateway Anti-Spyware ○

Application Firewall ○
Block Port Forwarding ○
Local Port Forwarding ○
Remote Port Forwarding ○
X11 Forwarding ○

2. Select one or more types of service inspections; none are selected by default:
   - **Intrusion Prevention**
   - **Gateway Anti-Virus**
   - **Gateway Anti-Spyware**

     ⓘ **IMPORTANT:** Gateway Anti-Virus service does not work for DPI-SSH because TCP streams for Anti-Spyware are not supported. If the option is checked, the system takes no action.
   - **Application Firewall**
   - **Block Port Forwarding**: for more information about these options, see *DPI-SSH Blocking of Port Forwarding*:
     - **Local Port Forwarding**
     - **Remote Port Forwarding**
     - **X11 Forwarding**
3. Click **Accept.**

DPI-SSH Blocking of Port Forwarding

SSH makes it possible to tunnel other applications through SSH by using port forwarding. Port forwarding allows local or remote computers (for example, computers on the internet) to connect to a specific computer or service within a private LAN. Port forwarding translates the address and/or port number of a packet to a new destination address and forwards it to that destination according the routing rules. Because these packets have new destination and port numbers, they can bypass the firewall security policies.

To prevent circumvention of the application-based security policies on the SonicWall network security appliance, SonicOS supports blocking SSH port forwarding for both Local and Remote port forwarding.

- *Local port forwarding* allows a computer on the local network to connect to another server, which might be an external server.
- *Dynamic port forwarding* allows you to configure one local port for tunneling data to all remote destinations. This can be considered as a special case of Local port forwarding.
- *Remote port forwarding* allows a remote host to connect to an internal server.

SSH port forwarding supports the following servers:

- SSH server on Fedora
- SSH server on Ubuntu

SSH port forwarding supports both:

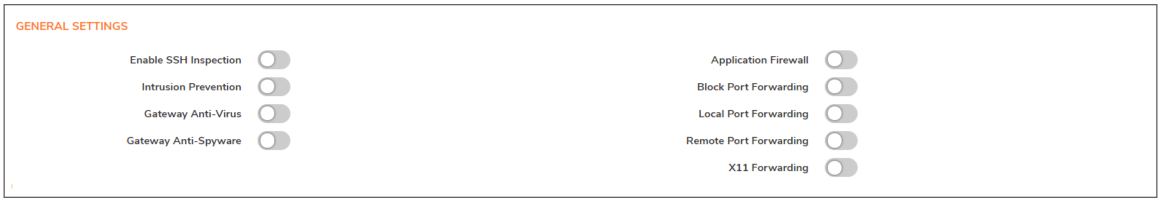
- Route mode
- Wire mode – only supported in Secure Mode

SSH port forwarding supports a maximum of 1000 connections, matching the maximum supported by DPI-SSH.

DPI-SSH must be enabled for blocking of SSH port forwarding to work. If any local or remote port forwarding requests are made when the blocking feature is enabled, SonicOS blocks those requests and resets the connection.

To enable blocking of SSH port forwarding:

1. Navigate to the **POLICY | DPI-SSH > Settings** page.



GENERAL SETTINGS

Enable SSH Inspection ○
Intrusion Prevention ○
Gateway Anti-Virus ○
Gateway Anti-Spyware ○

Application Firewall ○
Block Port Forwarding ○
Local Port Forwarding ○
Remote Port Forwarding ○
X11 Forwarding ○

2. In the **General Settings** section, select **Block Port Forwarding**.
3. Select either or both **Local Port Forwarding** and **Remote Port Forwarding** to block that type of port forwarding.
4. Click **Accept**.

DPI-SSH port forwarding supports the following clients:

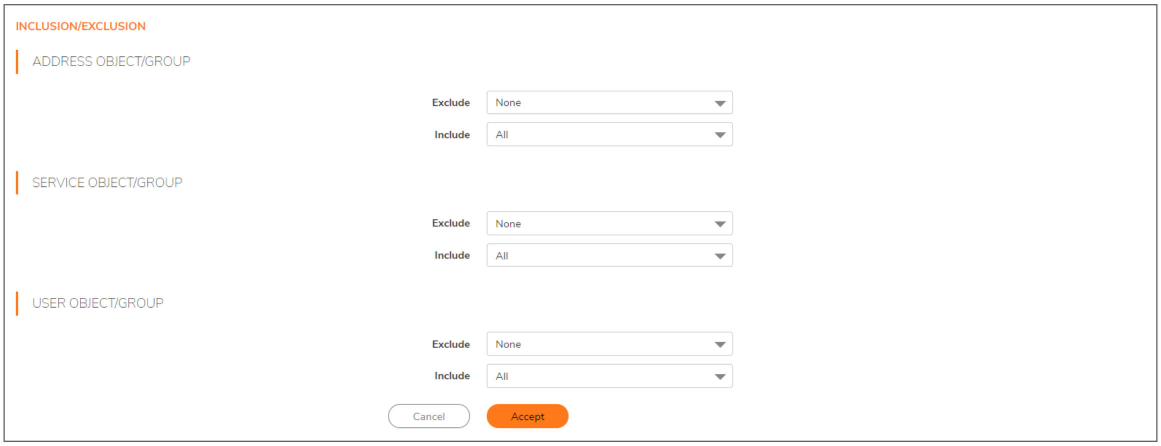
- SSH client for Cygwin
- Putty
- SecureCRT
- SSH on Ubuntu
- SSH on CentOS

Customizing Client DPI-SSH Inspection

By default, when DPI-SSH is enabled, it applies to all traffic on the firewall. You can customize to which traffic DPI-SSH inspection applies in the **Inclusion/Exclusion** section.

To customize DPI-SSH client inspection:

1. Go to the **Inclusion/Exclusion** section of the **POLICY | DPI-SSH > Settings** page.



INCLUSION/EXCLUSION

ADDRESS OBJECT/GROUP

Exclude: None

Include: All

SERVICE OBJECT/GROUP

Exclude: None

Include: All

USER OBJECT/GROUP

Exclude: None

Include: All

2. From the **Address Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and Include is set to **All**.
3. From the **Service Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and Include is set to **All**.
4. From the **User Object/Group Exclude** and **Include** drop-down menus, select an address object or group to exclude or include from DPI-SSH inspection. By default, **Exclude** is set to **None** and Include is set to **All**.
5. Click **Accept**.

4

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 DPI-SSH Administration Guide
Updated - December 2023
Software Version - 7.1
232-005880-00 Rev A

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

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

End User Product Agreement

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

Open Source Code

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

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