



Contents

About DPI-SSH	3
Supported Clients/Servers and Connections	3
Supported Key Exchange Algorithms	4
Caveats	4
Configuring DPI-SSH	6
Activating Your DPI-SSH License	6
Managing DPI-SSH	6
Viewing Connection Status	7
Configuring Client DPI-SSH Inspection	8
DPI-SSH Blocking of Port Forwarding	8
Customizing Client DPI-SSH Inspection	10
SonicWall Support	11
About This Document1	12

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.

2

Configuring DPI-SSH

DPI-SSH provides deep packet inspection of encrypted information.

(i) **NOTE:** Gateway Anti-Spyware service is not compatible with DPI-SSH because TCP streams for antispyware 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		Applica	ation Firewall
Intrusion Prevention		Block Por	t Forwarding
Gateway Anti-Virus		Local Por	t Forwarding
Gateway Anti-Spyware		Remote Por	t Forwarding
1		X1:	1 Forwarding
INCLUSION/EXCLUSION			
ADDRESS OBJECT/GROUP			
	Exclude	None	
	Include		
	include		
SERVICE OBJECT/GROUP			
	Exclude	None	
	Include	All	
USER OBJECT/GROUP			
	Exclude	None 💌	
	Include	All	
(Cancel	Accept	

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	Application Firewall	
Intrusion Prevention	O Block Port Forwarding	
Gateway Anti-Virus	Local Port Forwarding	
Gateway Anti-Spyware	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

(i) **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	Application Firewall	
Intrusion Prevention	Block Port Forwarding	
Gateway Anti-Virus	O Local Port Forwarding	
Gateway Anti-Spyware	C 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
Cancel	Accept

- 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**.
- 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.

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS DPI-SSHAdministration Guide Updated - April 2024 Software Version - 7.0 232-005333-10 Rev C

Copyright © 2024 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