Secure Web Gateway
Version 11.8
SOCKS Proxy Guide

Legal Notice

Copyright © 2016 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: **support@trustwave.com**

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Revision History

Version	Date	Changes
1.0	June 2016	First edition

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or e-mail address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and checkbox names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in `Courier New 9 pt in blue` indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Cautions

Note: This symbol indicates information that applies to the task at hand.

Tip: This symbol denotes a suggestion for a better or more productive way to use the product.

Caution: This symbol highlights a warning against using the software in an unintended manner.

Question: This symbol indicates a question that the reader should consider.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

Table of Contents

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

1 Introduction

SOCKS is an IETF-approved security protocol that uses a proxy server to allow application users on one network to connect transparently to hosts on another network across a firewall.

Access control can be applied at the beginning of each browsing session, after which the server relays the data between the client and the application server.

The SOCKS protocol supports two commands; CONNECT and BIND.

- CONNECT – The Application client asks the SOCKS server to connect to the Application server. When the connection is made, application data is relayed in both directions.
- BIND – The Application client asks the SOCKS server to accept connections from the Application server. It then notifies the application which endpoint to connect to. When the connection is made, application data is relayed in both directions.

1.1 SOCKS Versions

The SOCKS protocol has two major versions, SOCKS4 and SOCKS5.

Note: SOCKS4 evolved into version SOCKS4a that added the ability to connect to named servers instead of only to IP addressed servers.

SOCKS4 does not support any authentication mechanism. There is an identification mechanism through the IDENT protocol.

SOCKS5 added several features, including:

- Support for relaying UDP packets using the UDP_ASSOC command.
- Support for an authentication mechanism prior to the SOCKS handshake.
- Support for IPV6.

1.2 SOCKS and SWG

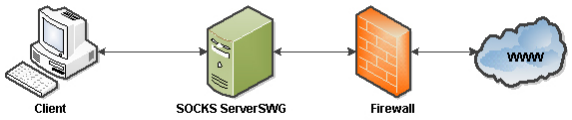
Trustwave SWG acts as the SOCKS proxy server and accepts connections from clients on port 1080. The SOCKS Server works out-of-the-box with supplied parameters and configuration files. No additional configuration is needed after installation as long as operating conditions remain the same. However, the SOCKS server is reconfigurable by administrators.

The SOCKS server handles network errors without interrupting normal operation. In case of network failure, relevant connections are closed and close events are propagated to their corresponding connections. However, in case of a network shortage, the SOCKS server does not provide any guarantees as to data that was being transferred prior to the shortage; some or all of it may be lost.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

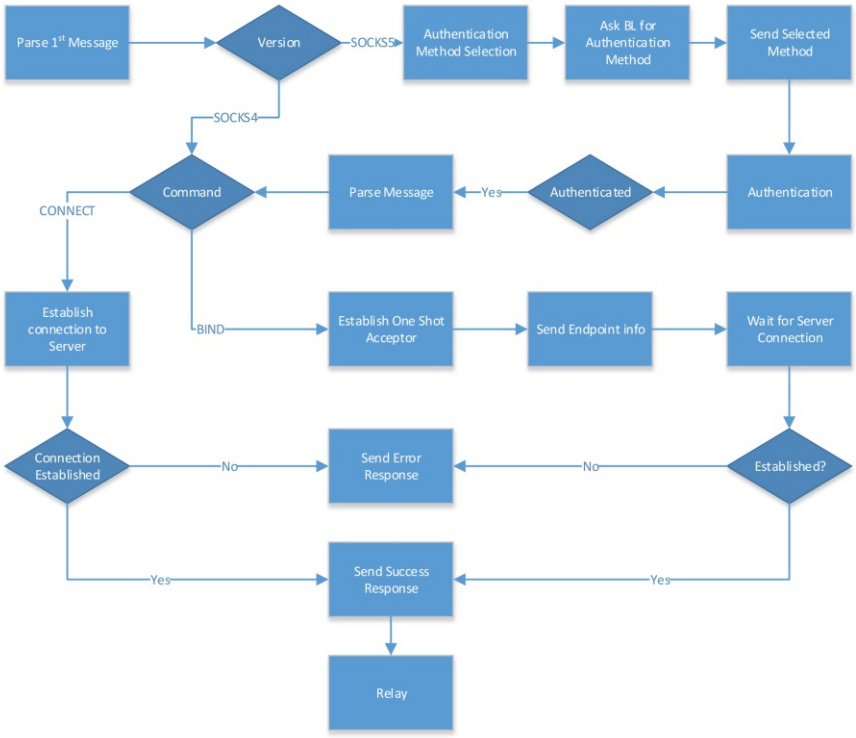
2 How it Works

2.1 Typical SOCKS Topology



2.2 Data Flows

After handshake, the SOCKS Server relays data between the application client and the application server.



2.3 CONNECT Handling

The Application client asks the SOCKS server to connect to the application server.

If successful, a success message is sent to the client and the SOCKS server switches to relay mode. If connection fails, a fail message is sent to the client and the SOCKS server closes the connection from the client.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

2.4 BIND Handling

- The Application client asks the SOCKS server to connect to the application server.
- The SOCKS server starts an acceptor on a dynamic port and sends a message containing the port it listens on.
- The Application client sends the endpoint values to the Application server.
- If the Application server successfully connects to the SOCKS Server, a success message is sent to the client and the SOCKS server switches to relay mode. On failure, a fail message is sent to the client and the SOCKS server closes the connection from the client.

2.5 SOCKS5 Authentication Mechanism Selection

- When the client establishes a connection to the SOCKS server, the first message contains the supported authentication methods. The SOCKS server then selects a method from the suggested methods and informs the client.
- Both the client and the SOCKS server start authentication and if successful, continue with the SOCKS handshake.

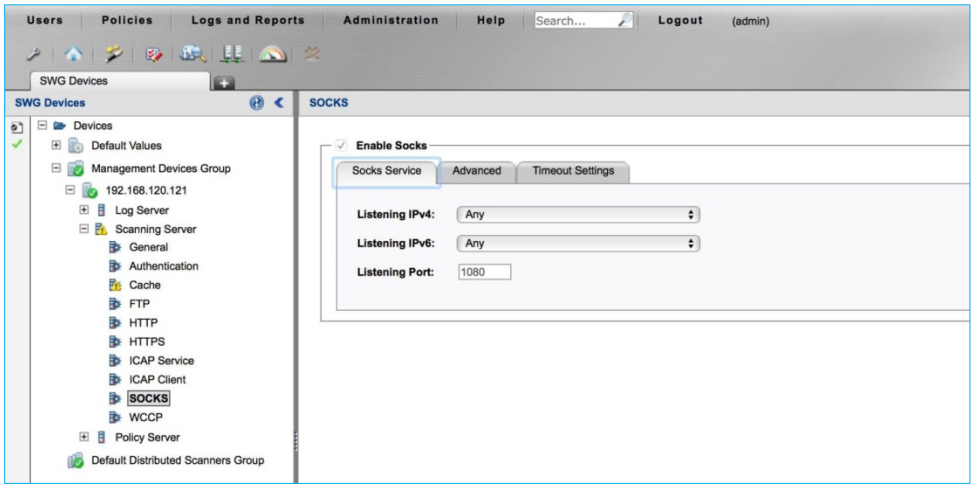
3 Configuration

SOCKS configuration in Trustwave SWG is defined in the GUI.

3.1 Configuring SOCKS in SWG

To configure SOCKS in SWG:

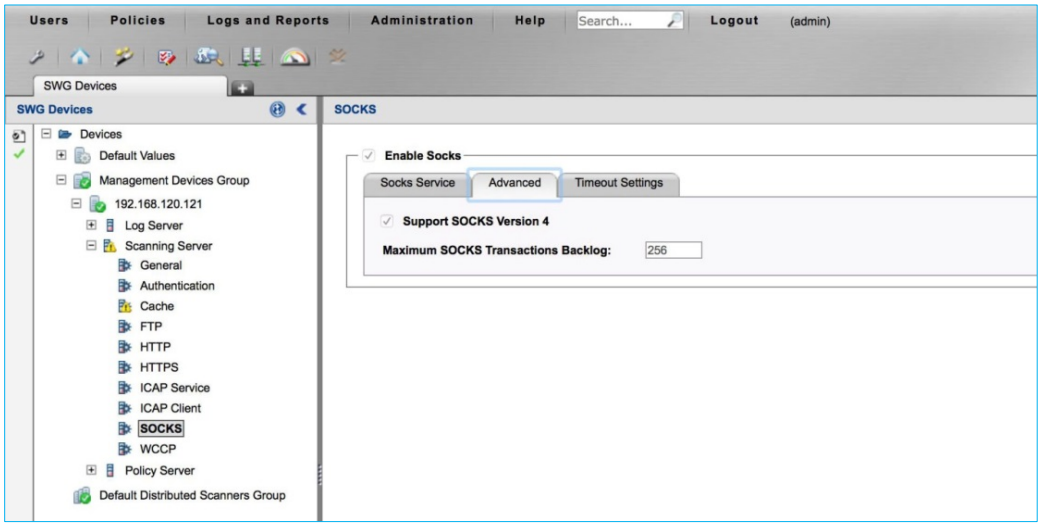
1. Navigate to **Administration | System Settings | SWG Devices** and in the **Scanning Server** node of the relevant device, select **SOCKS**.
2. In the right pane, select the **Enable Socks** check box.
3. In the **Socks Service** tab, specify the IPv4 and IPv6 listening addresses or select **Any** from the list.



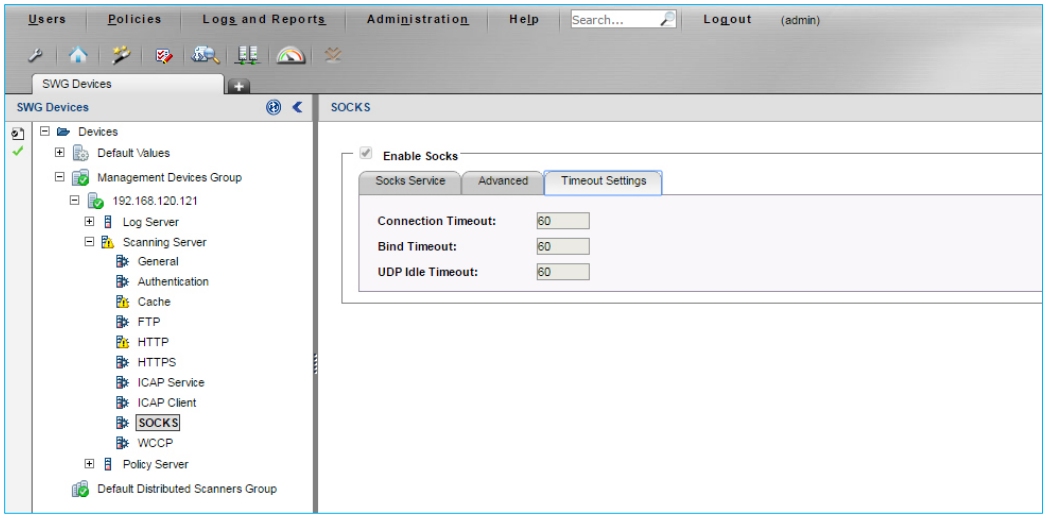
4. Specify the **Listening Port** on the device. The default is 1080.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

5. If SOCKS4 support is required, open the **Advanced** tab and select the **Support SOCKS Version 4** check box. By default, this check box is not selected.



6. If required, change the maximum transactions backlog. The default is 256.
7. In the **Timeout Settings** tab, specify the SOCKS **Connection** and **Bind** timeouts, and the UDP idle timeout, in seconds.



8. Click **Save** when your configuration is complete.

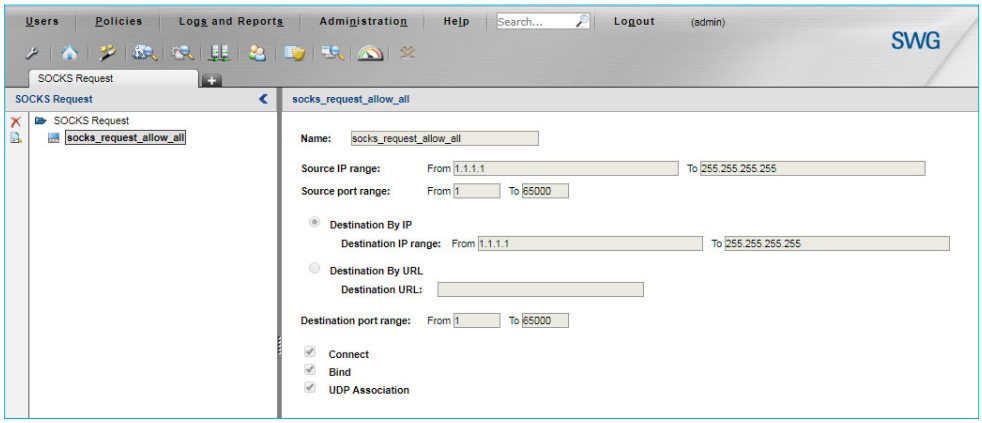
Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

3.2 Configuring SOCKS Policy Rules

SWG enables you to define rules that specify the Socks commands applied to specific or a range of source and destination IPs, and specific or a range of source and destination ports.

To configure a rule for a SOCKS request:

1. Navigate to **Policies | Condition Elements | Socks Request**.



2. In the left pane, right-click **SOCKS Requests** and select **Add Component**.
3. Define the Rule parameters as required:
   a. Enter a descriptive Name.
   b. Enter the source and destination IP range.
   c. Enter the source and destination port range.
   d. Enter the Destination URL.
   e. For this Rule, select the relevant Socks commands applicable to the defined IPs and ports.
      i. **Connect** allows outgoing connections between proxy and server
      ii. **Bind** allows incoming connections from the server to the proxy
      iii. **UDP Association** allows UDP connections
4. Click **Save** when your rule configuration is complete.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries.

For more information about Trustwave, visit https://www.trustwave.com.