Contents

Overview ..........................................................................................................................3
Pre-requisites ..................................................................................................................3
Configuration ................................................................................................................3
Configuration on XG Firewall ..........................................................................................4
   Method A: Disable QUIC with Application Control on XG Firewall .............................4
      Step 1: Create Application Filter policy ..................................................................4
      Step 2: Edit Application Filter ................................................................................4
      Step 3: Create a Firewall Rule ..................................................................................5
   Method B: Block QUIC Protocol with Firewall Rule ....................................................6
Configuration on Client Machine ....................................................................................8
   Method C: Disable QUIC in Chrome ............................................................................8
Result ...............................................................................................................................8
Copyright Notice ............................................................................................................9
Overview

QUIC (Quick UDP Internet Connection) is an experimental transport layer protocol developed by Google to speed up Internet connections and reduce bandwidth congestion. It is enabled by default on Chrome browsers version 52 onwards.

Since QUIC works over UDP ports 80 and 443, and not over TCP, connections over QUIC bypass transparent proxies. Hence, security features of Sophos XG Firewall, like Sophos Sandstorm, HTTPS decryption, malware and content scanning may not function well on Google Chrome. Blocking QUIC traffic will make the connection fall back to TCP, ensuring that all web traffic traverses through the proxy and that filtering is not bypassed.

This article describes how to block Google’s QUIC protocol, to prevent bypass of Sophos XG Firewall’s security and scanning features, and filtering of web traffic related to Google services, including HTTPS decryption, malware scanning, and content filter scanning. Configuration steps provided in this article are specific to version SFOS 17.0.0 GA.

Prerequisites

- Read-write permissions on XG Firewall Admin Console for the relevant features.
- Valid Web Protection, Email Protection and Sandstorm subscription [Administration > Licensing].

Configuration

You can use one of the following methods to block QUIC protocol:

1. Application control on XG Firewall
2. Firewall rule on XG Firewall
3. Google Chrome browser on client machine

Note: When QUIC protocol is blocked by any of these methods, Chrome will revert to standard HTTP/HTTPS, hence the changes will not impact services.
Configuration on XG Firewall

Method A: Disable QUIC with Application Control

Step 1: Create Application Filter Policy

- Go to Protect > Applications > Application Filter and click Add.
- Enter a Name for the policy.
- Set template to Allow All.
- Click Save.

Step 2: Edit Application Filter

- Go to Application Filter. Click the edit button next to the filter you have created.
How to Block Google QUIC Protocol

- Click Add.
- Click Select Individual Application.
- Set Technology filter to Network Protocol.
- Select the check box next to the QUIC application.
- Set Action to Deny.
- Click Save.

Step 3: Create a Firewall Rule

- Go to Protect > Firewall, click + Add Firewall Rule and click User/Network Rule.
- Set Rule Position to Top.
- Set Source Zones to LAN and set Destination Zones to WAN.
• **Under Advanced**, set **Application Control** to the application filter you have created.

![Advanced](image)

• **Click Save.**

**Method B: Block QUIC Protocol with Firewall Rule**

• Go to **Protect > Firewall**, click **+ Add Firewall Rule** and click **User/Network**
• Enter a **Rule Name**.
• Set **Rule Position** to **Top**.
• Enter the **Source** and **Destination** networks whose traffic you wish to drop if it uses QUIC protocol.

![Firewall](image)
- **Under Destination & Services, for Services**, click **Add New Item**.
- **Click Create New and Add Service** with the parameters shown in the screen to block UDP ports 80 and 443.
- **Click Save**.

**Note:** Make sure that the firewall rule remains at the top of the firewall rules table to drop QUIC traffic.
Configuration on Client Machine

Method C in the scenario is based on Chrome version: 61.0.3163.100. We recommend that you undertake the same procedure for other versions too.

Method C: Disable QUIC in Chrome

- Launch Google Chrome browser on client machine.
- In the address bar, type: chrome://flags/
- In the listed flags, go to Experimental QUIC protocol Mac, Windows, Linux, Chrome OS, and Android.
- In the drop-down box, select Disabled.
- Click Relaunch Now.

Result

You have now blocked QUIC protocol. Google services accessed through Chrome browser will no longer bypass XG Firewall’s security scanning.
Copyright Notice

Copyright 2017-2018 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.