

How to Configure Google Accounts Filtering in the Firewall

https://campus.barracuda.com/doc/48660874/

The X-Series Firewall can filter traffic to Google services based on the domain attached to the G Suite account. This allows you to block access to personal Google accounts and other non-whitelisted G Suite accounts, while still allowing your whitelisted G Suite domains. Google Accounts are enforced on a per-access-rule basis. Since Google requires HTTPS for almost all services, SSL Inspection is required. Google Chrome uses the QUIC protocol by default to communicate with Google servers. To force Chrome to use the HTTPS fallback, you must block QUIC traffic.

Before you begin

• Enable SSL Inspection. For more information, see **How to Configure SSL Inspection**.

Step 1. Add your domains to the Google domain whitelist

Google accounts using the domains in the whitelist will be exempted from filtering when a Google account-enabled access rule matches.

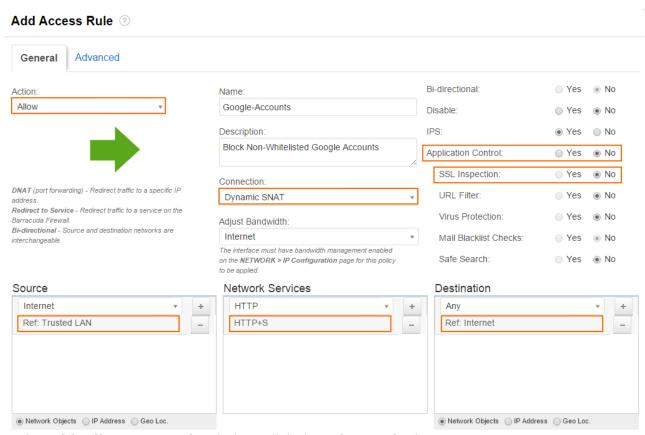
- 1. Go to **FIREWALL > Settings.**
- 2. Make sure that **Application Control** is enabled.
- 3. In the **Google Accounts** section, add domains to the **Domain White List**. Click + after each entry.
- 4. Click Save.

Step 2. Create an access rule to block non-whitelisted Google accounts

You can block Google accounts not on the whitelist for all web traffic that matches an access rule by enabling **Google Accounts** in the advanced settings of the access rule.

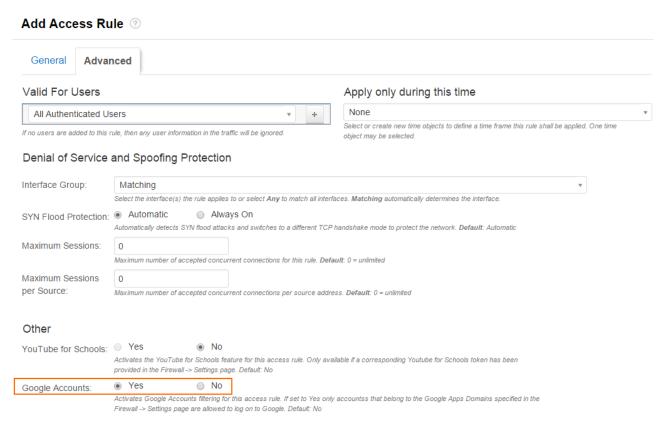
- 1. Go to FIREWALL > Firewall Rules.
- 2. Create an access rule with the following settings:
 - Action Select Allow.
 - Connection Select Dynamic SNAT.
 - **Source** Select the source addresses of the traffic.
 - Network Services Select HTTP+S.
 - **Destination** Select **Internet**.
- 3. Enable Application Control and SSL Inspection.





- 4. In the Add/Edit Access Rule window, click the Advanced tab.
- 5. (optional) Set additional matching criteria:
 - Valid for Users For more information, see <u>User Objects</u>.
 - Apply only during this time For more information, see <u>Schedule Objects</u>.
- 6. In the Other section, set Google Accounts to Yes.





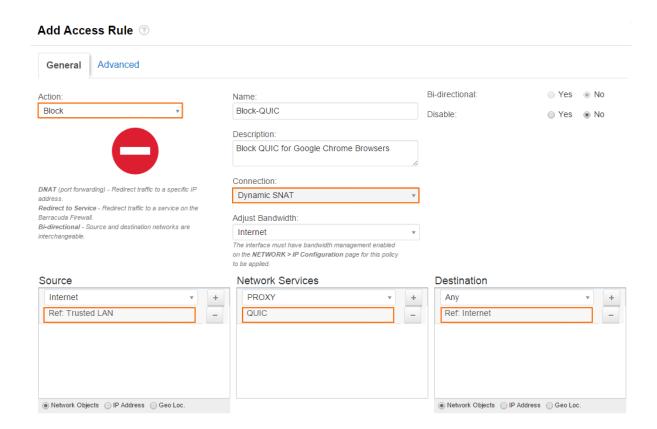
- 7. Click Save.
- 8. Drag and drop the access rule in the ruleset, so that no access rule above it matches this traffic.

Step 3. Block QUIC for Google Chrome browsers

To force Google Chrome browsers to use HTTPS instead of QUIC on UDP port 443, you must create a BLOCK access rule.

- 1. Go to FIREWALL > Firewall Rules.
- 2. Create an access rule with the following settings:
 - Action Select Block.
 - Connection Select Dynamic SNAT.
 - Source Add the source addresses of the traffic. Use the same source as the access rule in step 2.
 - Network Services Create and select the service object for UDP 443. For more information, see Service Objects.
 - Destination Select Internet.
- 3. (optional) Set additional matching criteria:
 - Valid for Users Use the same user object as in step 2.
 - **Apply only during this time** Use the same schedule object as in step 2.





- 4. Click Save.
- 5. Drag and drop the access rule above the rule created in step 2.

Web traffic matching this rule can now only access Google accounts for domains that are included in the whitelist. When users access a non-whitelisted domain, they are automatically redirected to a Google block page.



This service is not available

Gmail is not available for @gmail.com within this network. Gmail is only available for accounts in the following domains:

Please talk to your network administrator for more information.

Did you use this product with a different Google Account? Sign out of your current Google Account and then sign in to the account you want.

©2015 Google - Google Home - Terms of Service - Privacy Policy - Help

Barracuda NextGen Firewall X



Figures

- 1. google accounts68 02.png
- 2. google accounts68 03.png
- 3. google_accounts68_04.png
- 4. google_accounts68_05.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.