
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**.

Add Access Rule ?

General
Advanced

Action: Allow



DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: Google-Accounts

Description: Block Non-Whitelisted Google Accounts

Connection: Dynamic SNAT

Adjust Bandwidth: Internet

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: Yes No

Disable: Yes No

IPS: Yes No

Application Control: Yes No

SSL Inspection: Yes No

URL Filter: Yes No

Virus Protection: Yes No

Mail Blacklist Checks: Yes No

Safe Search: Yes No

Source

Internet +

Ref. Trusted LAN -

Network Objects IP Address Geo Loc.

Network Services

HTTP +

HTTP+S -

Destination

Any +

Ref: Internet -

Network Objects IP Address Geo Loc.

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

Add Access Rule ?

General

Advanced

Valid For Users

If no users are added to this rule, then any user information in the traffic will be ignored.

Apply only during this time

Select or create new time objects to define a time frame this rule shall be applied. One time object may be selected.

Denial of Service and Spoofing Protection

Interface Group:

Select the interface(s) the rule applies to or select **Any** to match all interfaces. **Matching** automatically determines the interface.

SYN Flood Protection: Automatic Always On

Automatically detects SYN flood attacks and switches to a different TCP handshake mode to protect the network. **Default:** Automatic

Maximum Sessions:

Maximum number of accepted concurrent connections for this rule. **Default:** 0 = unlimited

Maximum Sessions per Source:

Maximum number of accepted concurrent connections per source address. **Default:** 0 = unlimited

Other

YouTube for Schools: Yes No

Activates the YouTube for Schools feature for this access rule. Only available if a corresponding Youtube for Schools token has been provided in the Firewall -> Settings page. **Default:** No

Google Accounts: Yes No

Activates Google Accounts filtering for this access rule. If set to Yes only accounts that belong to the Google Apps Domains specified in the Firewall -> Settings page are allowed to log on to Google. **Default:** No

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.

Add Access Rule ?

General **Advanced**

Action: Block

Name: Block-QUIC Bi-directional: Yes No
Disable: Yes No

Description: Block QUIC for Google Chrome Browsers

Connection: Dynamic SNAT

Adjust Bandwidth: Internet
The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Source **Network Services** **Destination**

Internet + -
Ref: Trusted LAN -

PROXY + -
QUIC -

Any + -
Ref: Internet -

Network Objects IP Address Geo Loc.

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 [redacted]@gmail.com within this network. Gmail is only available for accounts in the following domains:

- [redacted]

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.

Figures

1. google_accounts68_02.png
2. google_accounts68_03.png
3. google_accounts68_04.png
4. google_accounts68_05.png

© Barracuda Networks Inc., 2019 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.