How to Configure Google Accounts Filtering in the Firewall

https://campus.barracuda.com/doc/17556/

The CloudGen Firewall can filter traffic to Google services based on the domain attached to the Google Workplace account. This allows you to block all consumer accounts with the @gmail.com domain and other non-allow-listed Workplace accounts, while only allow-listed workspace accounts will work. However, the login for the gmail.com domain accounts will not work even if allow-listed. Google accounts are enforced on a per-access-rule basis.

Since Google requires HTTPS for almost all services, TLS 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

- The **Feature Level** of the Forwarding Firewall must be **7.2** or higher.
- Enable Application Control. For more information, see How to Enable Application Control.
- Enable TLS Inspection. For more information, see How to Configure Outbound TLS Inspection.

Step 1. Add Your Domains to the Google Domain Allow List

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Google Personal Accounts** section, click **+** to add domains to the **Domain Allow List**.

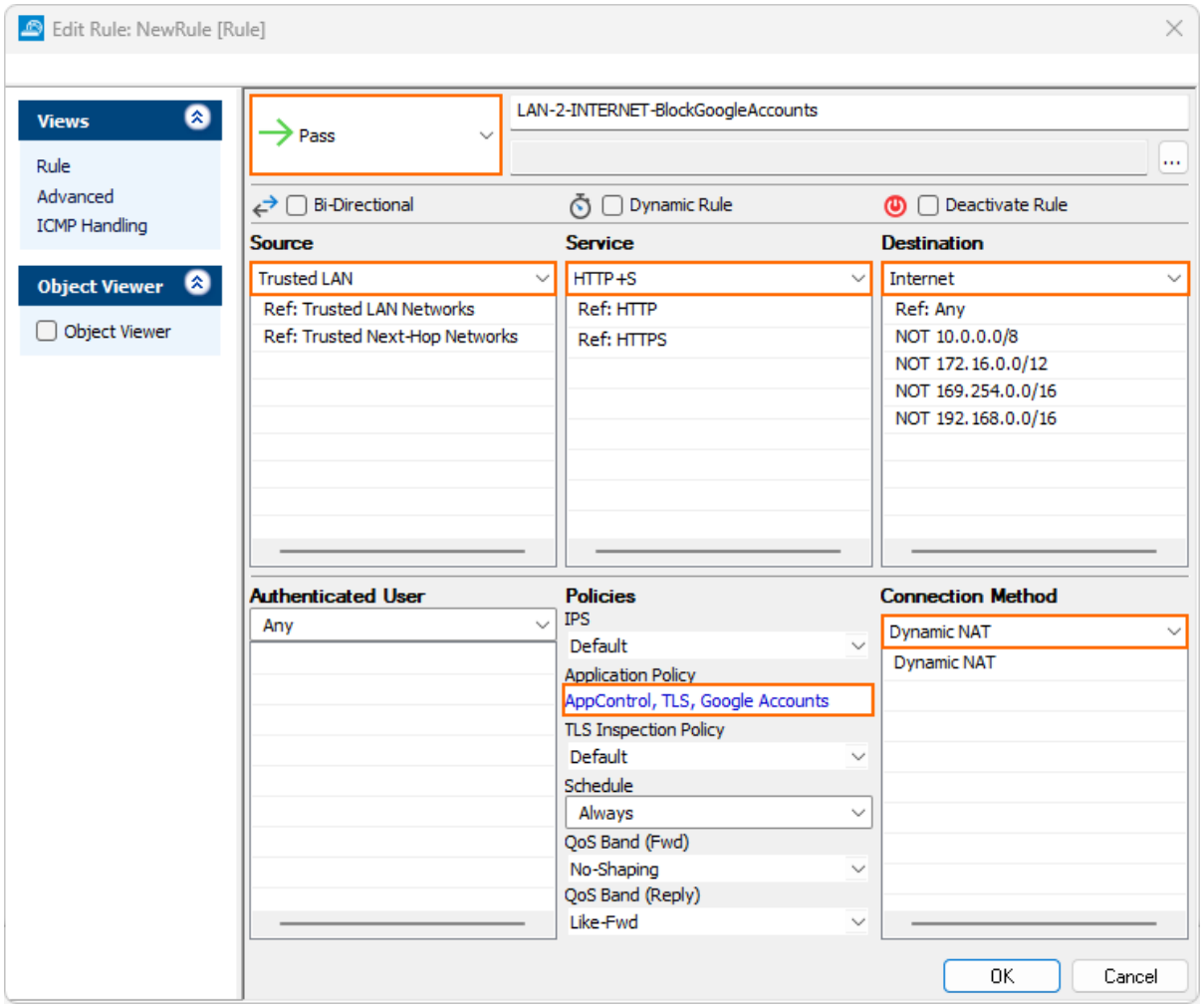
4. Click **Send Changes** and **Activate**.

Step 2. Create an Access Rule to Block Non-Allow-Listed Google Accounts

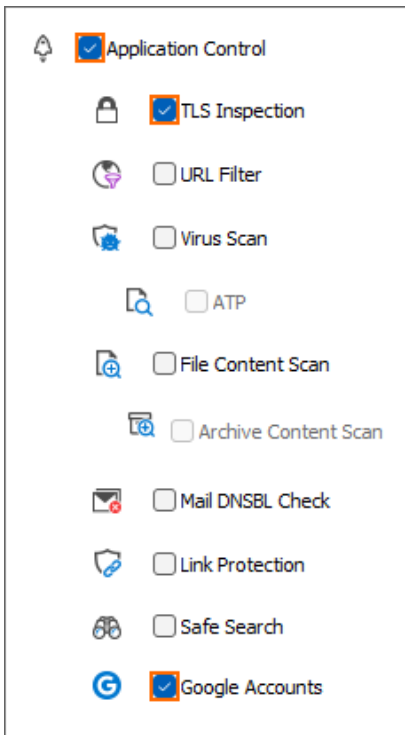
You can block Google accounts not on the allow-list for all web traffic that matches an access rule by enabling **Google Accounts** in the Application Control settings of the access rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your web traffic:
   - **Source** – The source addresses of the traffic.
   - **Service** – Select **HTTP+S**.
   - **Destination** – Select **Internet**.
   - **Connection Method** – Select **Dynamic NAT**.



7. Click on the **Application Policy** link and select**:**
   - **Application Control** – Required.
   - **TLS Inspection** – Required, since Google services are available exclusively via HTTPS.
   - **Google Accounts** – Required.



8. Select a policy from the **TLS Inspection Policy** drop-down list.
9. (optional) Set additional matching criteria:
   - **Authenticated User** – For more information, see User Objects.
   - **Schedule Object** – For more information, see Schedule Objects.
10. Click **OK**.
11. Place the access rule via drag-and-drop in the ruleset, so that no access rule above it matches this traffic.
12. Click **Send Changes** and **Activate**.

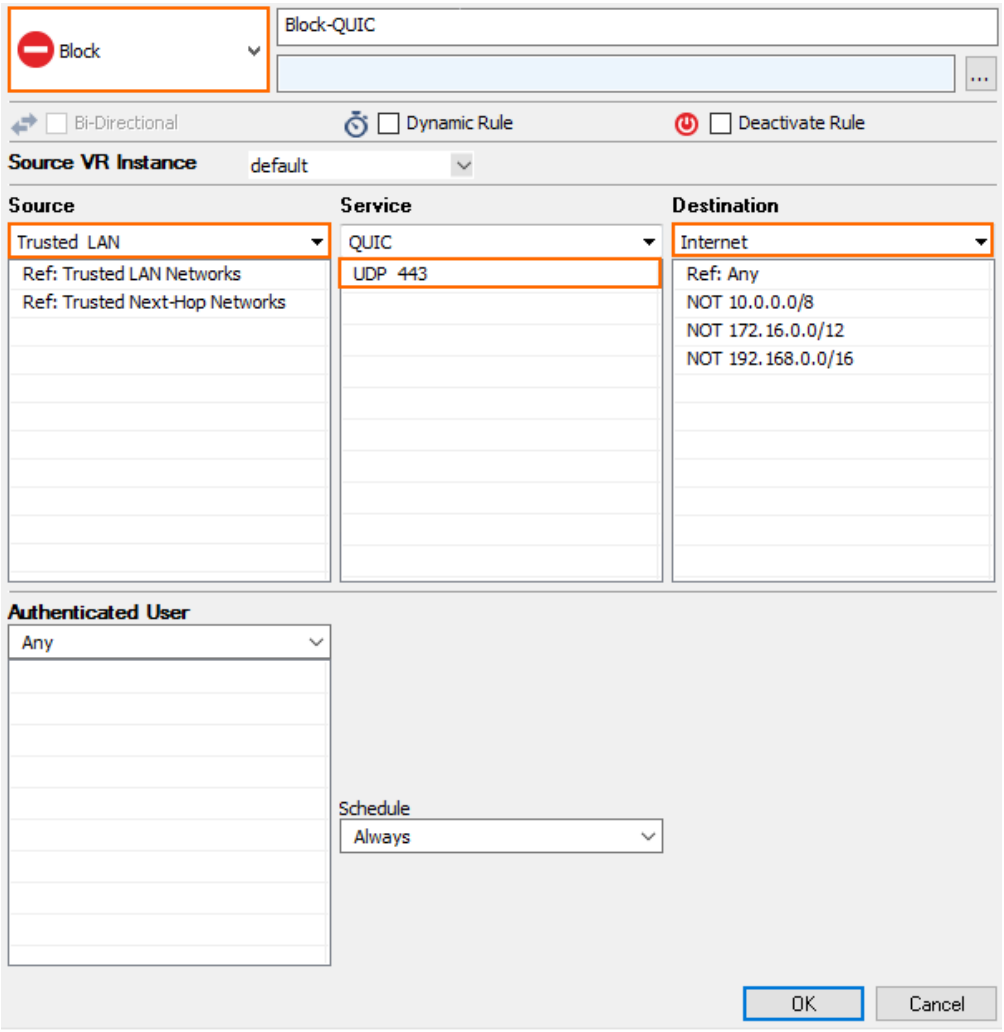
Step 3. Block QUIC for Google Chrome Browsers

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 **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

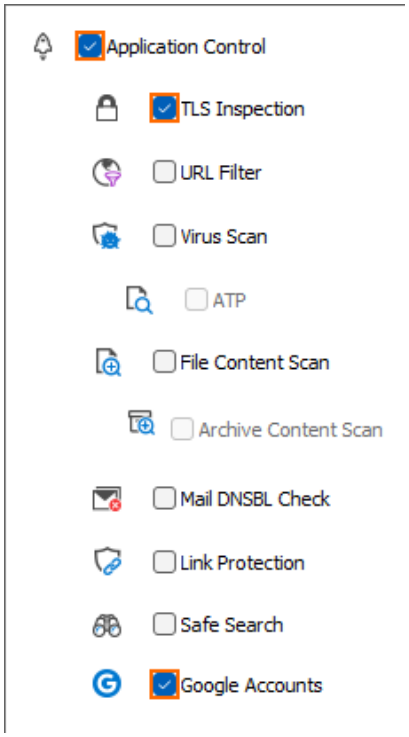
4. Select **Block** as the action.
5. Enter a **Name** for the rule.
6. Specify the following settings to match your web traffic:

- **Source** – The source addresses of the traffic. Use the same source as the access rule in Step 2.
- **Service** – Create and select the service object for UDP 443. For more information, see Service Objects.
- **Destination** – Select **Internet**.



7. (optional) Set additional matching criteria:
   - **Authenticated User** – Use the same user object as in Step 2.
   - **Schedule Object** – Use the same schedule object as in Step 2.
8. Click **OK**.
9. Place the access rule via drag-and-drop before the rule created in Step 2.
10. Click **Send Changes** and **Activate**.

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


Application Control
TLS Inspection
URL Filter
Virus Scan
ATP
File Content Scan
Archive Content Scan
Mail DNSBL Check
Link Protection
Safe Search
Google Accounts

Figures

1. Google_accounts_01.png
2. FW_Rule_Add01.png
3. access_rule_block_lan_to_google_accounts.png
4. app_control_google_accounts.png
5. FW_Rule_Add01.png
6. Google_accounts_05.png
7. app_control_google_accounts.png

© Barracuda Networks Inc., 2025 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.