Blocking access to consumer email accounts while allowing access to the corporate Google account with Cisco Cloud Web Security (CWS)

Jonny Noble
Technical Marketing Engineer
Security Technology Business Unit

July 2014

TABLE OF CONTENTS

CONFIDENTIALITY NOTICE

This document is **Cisco Public**.

PURPOSE OF THIS DOCUMENT

This guide is intended to explain how to configure Cisco Cloud Web Security to block access to common consumer web-based email accounts, while still allowing access to a corporate account hosted on Google docs

Product Knowledge Requirements

- Configuring web filtering policies in the CWS ScanCenter Admin Portal

Configuring CWS to allow access only to a corporate Google email account

This procedure is performed in three stages in the ScanCenter admin portal.

- A web filtering policy is defined that blocks access to all web-based email accounts, with the exception of Google's Gmail accounts.
- HTTPS inspection is defined for web-based email applications.
- A Custom Header is defined to tell Google to allow access only to the corporate account. After the Custom header is configured in ScanCenter it will later get added to all web requests sent to Google by the CWS cloud proxy.

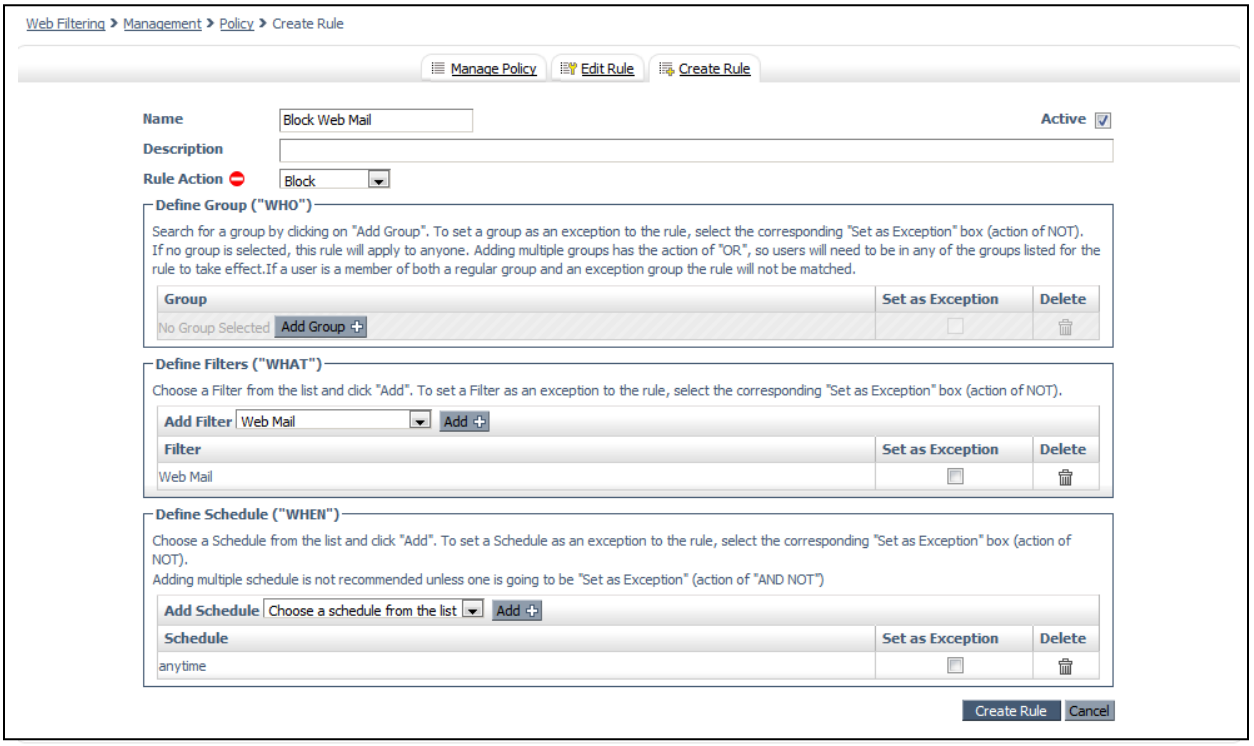
Configuration Steps

Blocking web-based email access

1. Log in to your ScanCenter account and navigate to the **Web Filtering** tab.
2. Click the **Management > Filters** menu, and then click **Create Filter**.
3. Create a new filter that will block all access to web-based email. This can be done in a number of methods, including a combination of methods in a single filter:
    a. On the **Categories** page, select **Web-based Email**.
    b. On the **Applications** page, select **Webmail**.
    c. On the **Domains** page, create a list of any other required web-based email hosts that may not be covered by the above two steps.

    Note: If a combination of methods are used in a single filter, any of them could trigger a match for that filter (OR operator).
4. Save your filter with a meaningful name.

5. Return to the web filtering policy page via the **Management > Policy** menu
6. Create a new web filtering rule by clicking **Create Rule**:
    a. Give it a meaningful name.
    b. The description is optional.
    c. Select the **Active** checkbox.
    d. Select **Block** from the **Rule Action** dropdown list.
    e. If necessary, click **Add Group** to add relevant groups. If none are selected, the rule will apply to all users.
    f. Select the filter you created in step 3 and click **Add**.
    g. If necessary, select a schedule for when the rule will apply, otherwise leave the default anytime schedule for the rule to apply at all times.
    h. Click **Create Rule** at the foot of the page to save the new rule.



7. Back in the web filtering policy page, use the up/down arrows to position your new rule at the relevant priority in the policy and click **Apply Changes** to save.

Adding an exception to allow access to Gmail

This exception can be created in one of two ways. Follow either step 8, or step 9 according to your needs:

8. Create a new rule similar to the above rule, which will allow access to Gmail, and place it at a higher priority in the web filtering policy:

a. Create a new filter in which Gmail is selected from the list under **Webmail** on the **Applications** page.

b. Create a new rule with the **Allow** action which includes the new filter from the above step.

c. In the web filtering policy, place the new rule higher than the previously created rule that blocks all web-based email.

This option can be used if you want to differentiate between groups associated with the two rules.

9. It is also possible to edit the filter previously created in step 3 to exclude blocking of access to Gmail:

    a. Under the **Management > Filters** menu, find the filter created in step 3 and click the **Edit** icon.

    b. Click **Exceptions** from the list on the left pane.

    c. Under the list of **Domains**, add **mail.google.com**.

    d. Save your settings.

    This option can be used if the Gmail exception is to apply to the same group of users already associated to the block rule.

    There is no need to make any changes to the block rule, as the filter included in the rule was updated.

HTTPS Inspection

As Google mail and most other web-based email applications are HTTPS based, an HTTPS inspection policy should be created in ScanCenter.

10. Follow the chapter in the ScanCenter Admin Guide for creating an HTTPS inspection policy, and ensure that all end-user client machines have the trusted certificate installed in all browsers.

11. Ensure that your HTTPS inspection policy includes the **Web-based Email** category, and the **Applications** checkbox at the least (other Categories and Hosts can be included as necessary, but are not required for this procedure). If necessary, also include the **Search Engines and Portals** category, and the **google.com** domain.

Custom Headers for Google accounts

12. In ScanCenter, navigate to the **Admin** tab, and then to **Management > Custom Headers**.

13. Click **Add New Header**, and configure as follows:

    a. In the **Domain** field, type **mail.google.com**.

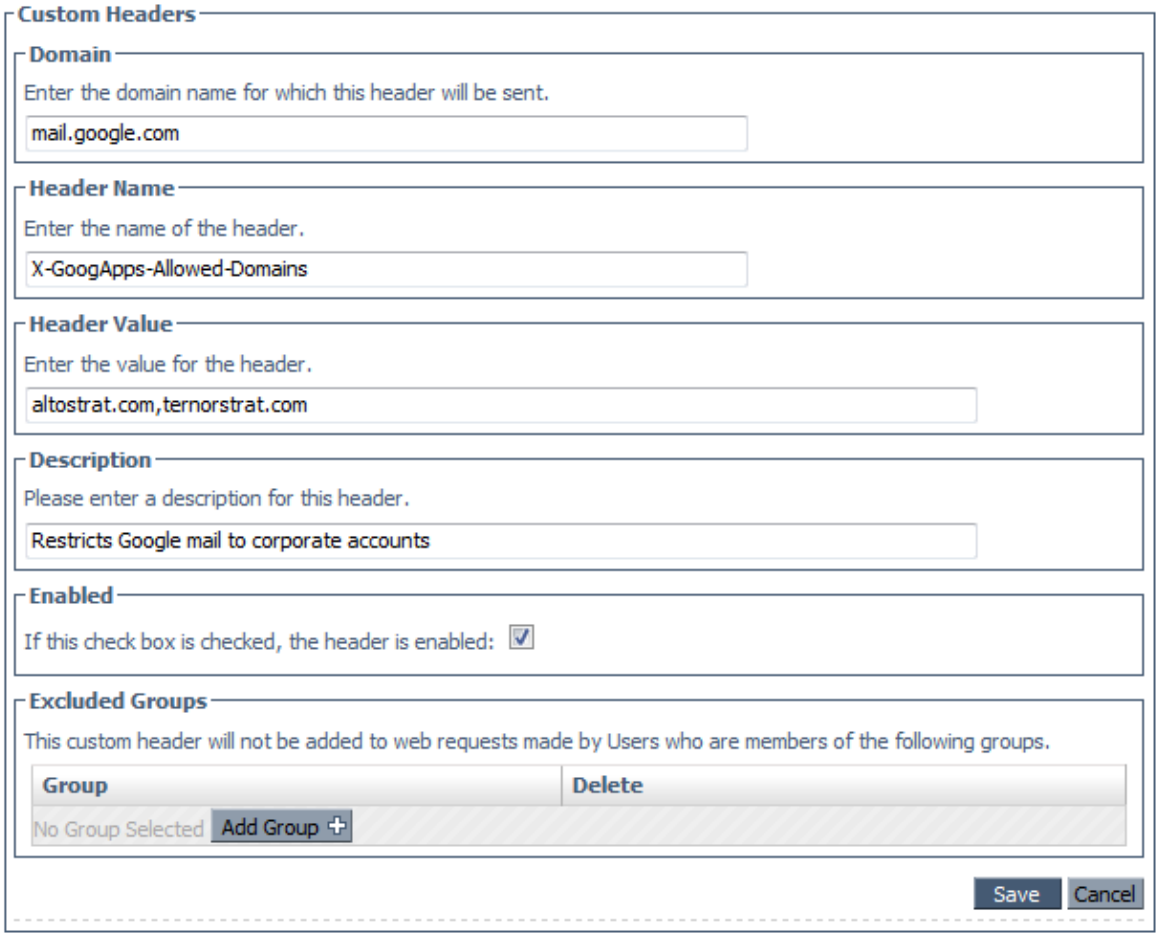
    b. In the **Header Name** field, type **X-GoogApps-Allowed-Domains**.

c. In the **Header Value** field, type the name of the domain that was registered with Google mail, for example **altostrat.com** or **ternorstrat.com**. Multiple domains can be included with comma separation.

d. Ensure the **Enabled** checkbox is selected.

e. Optionally you can add a group to the custom header. The header will not be added to any members of groups added. This means that these users will be able to access any Google mail account as configured in the web filtering policy.

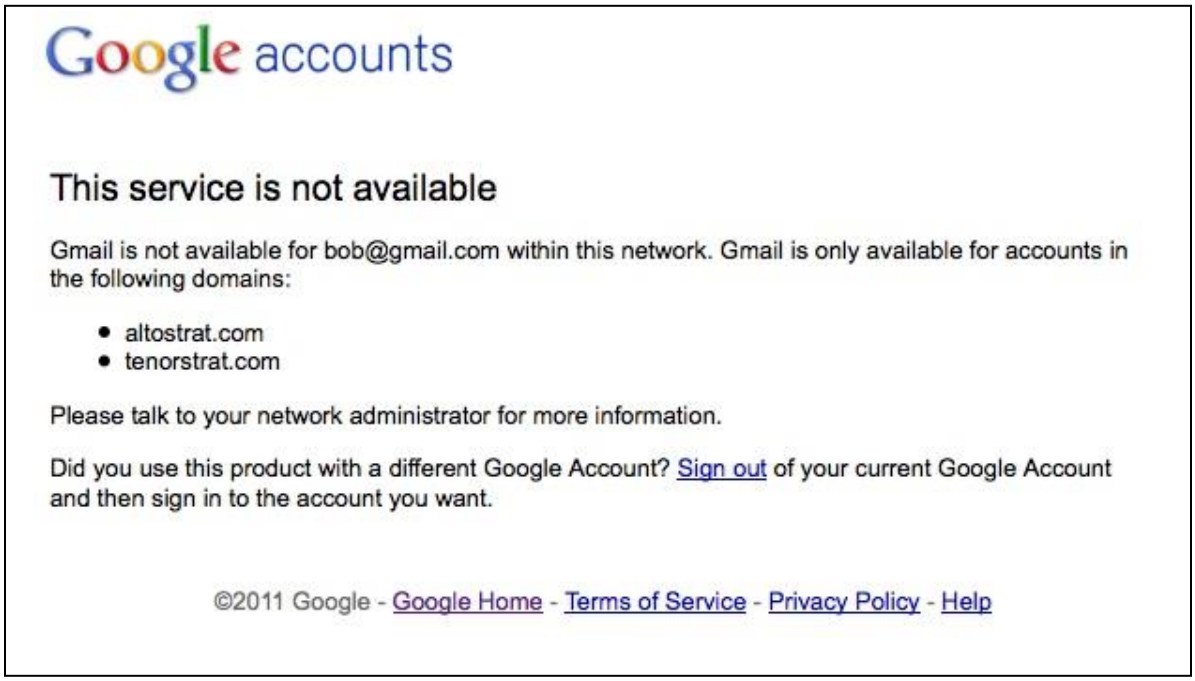
f. Save the new custom header.



User Experience

If a user attempts to access any web-based email application other than Google mail (for example Yahoo), they will be presented with the standard CWS block page (which may be customized by the admin).

If a user accesses Google mail, they will reach the Gmail login page. If they then log in to their corporate email account (based on the domain that was used in the custom header), they will be allowed to access their corporate email account. However, if they try to access another email account other than the corporate account, they will be presented with a block page hosted by Google:



Additional Information

Custom Headers in Cisco ScanCenter Admin Guide: http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011.html#task_CCE248BE73384D3FA47DFC940080CD64

Managing Google Apps accounts: https://support.google.com/a/answer/1668854?hl=en

Disclaimer

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**