Netskope Security Cloud helps you reduce your attack surface on public cloud deployments by providing unified visibility into all of your cloud infrastructure, including inventory and configuration of your critical IaaS and PaaS services. It also helps you differentiate between corporate, partner, and personal instances of cloud applications, like Google Drive. Netskope Security Cloud delivers comprehensive threat protection for cloud and web services and simplifies compliance with pre-defined profiles that align to industry standards such as CIS, PCI, and NIST.
Part 1: Subscribing to Netskope Security Cloud

Step 1  
Locate Netskope Security Cloud in AWS Marketplace. Select the Continue to Subscribe button.

Step 2  
Select your contract options and click the Create Contract button.

Part 1 complete

Part 2: Demonstration Guide for Netskope Security Cloud
Steps 1-2 of 30
Part 2: Demonstration Guide for Netskope Security Cloud

**Step 1**  In this demonstration, we'll be using both a Partner and Corporate instance of Google Drive.

**Step 2**  After subscribing and signing into Netskope, you will see the main dashboard. On the left-side of the dashboard, select *Skope IT*.

Steps 3 - 4 of 30
Step 3  Select **Application Events**.

You will see sessions that are specific to unique Google Drive instances. Under the Instance ID column, you can see unique ID's for each instance.
**Step 5**  
Select the top instance from the Application Events dashboard.

**Step 6**  
Select the plus sign at the top-right of the page.
**Step 7** Enter the name as Partner and click the **Submit** button.

**Step 8** Select the **second instance** from the Application Events dashboard.

**Steps 9 - 10** of 30
Step 9  Select the **plus sign** at the top-right of the page.

Step 10 Enter the name as Corporate and click the **Submit** button.

Steps 11 - 12 of 30
Step 11  We now have one instance labeled as Partner and one labeled as Corporate.

Step 12  Navigate back to the main Netskope dashboard by selecting the arrow next to Skope IT at the top left of the page.

Steps 13 - 14 of 30
Step 13  
Next select the **Policies** option.

Step 14  
Under Policies, select **Inline**.

Steps 15 - 16 of 30
Step 15  Choose the first policy on the page for the Corporate Google Drive instance.

This policy allows activity to be performed against the Corporate Instance of Google Drive.

Steps 17 - 18 of 30
Step 17  Select **Inline** on the left-side of the page.

Step 18  Select the first Partner instance policy.

Steps 19 - 20 of 30
Step 19  This policy allows all activities on the Partner instance of Google Drive.

Step 20  Select **Inline** on the left-side again and choose the **Block PCI Data** rule for the Partner instance.
Step 21  This policy will block uploads of sensitive data on the Partner instance of Google Drive.

Step 22  Select Inline on the left-side and choose the fourth policy from the top.

Steps 23 - 24 of 30
Step 23  This policy blocks all activities in Google Drive instances that are not tied to the Corporate or Partner instance.

Let’s navigate to Google Drive.

Steps 25 - 26 of 30
Step 25  We’ll upload a file containing sensitive information to our Corporate instance of Google Drive.

Step 26  As you can see, the upload is successful because we have allowed all activity on the Corporate instance in the policy.

Steps 27 - 28 of 30
Step 27  
Next, upload the sensitive data to the Partner instance.

Step 28  
As expected, the upload fails because our policy blocks sensitive data from being uploaded to the Partner instance of Google Drive.
Step 29

Next, let's look at a sample phishing email, where there is a document linked that is not part of either the Partner or Corporate Google Drive instances.

Step 30

If we click the Open in Docs button from the email, we are blocked from launching this instance of Google Drive per our policy.

Part 2 Complete
Thank you.

For more information, visit https://amzn.to/39OVoWP