Tech Note--Using CloudSOC Audit AppFeed in Symantec ProxySG Policies

Symantec CloudSOC Tech Note

Copyright statement

Table of Contents

Introduction

Blocking applications by name

Blocking applications by attribute

Blocking applications by combined attributes

Attributes and Values

Revision history

Introduction

Symantec ProxySG has integrated data for thousands of cloud applications using CloudSOC Audit AppFeed. This data is made available in ProxySG appliances and Management Center in the form of reporting and policies. In order to access this data, you must subscribe to CloudSOC Audit. This TechNote describes how to create policies in ProxySG that use the AppFeed data.

Blocking applications by name

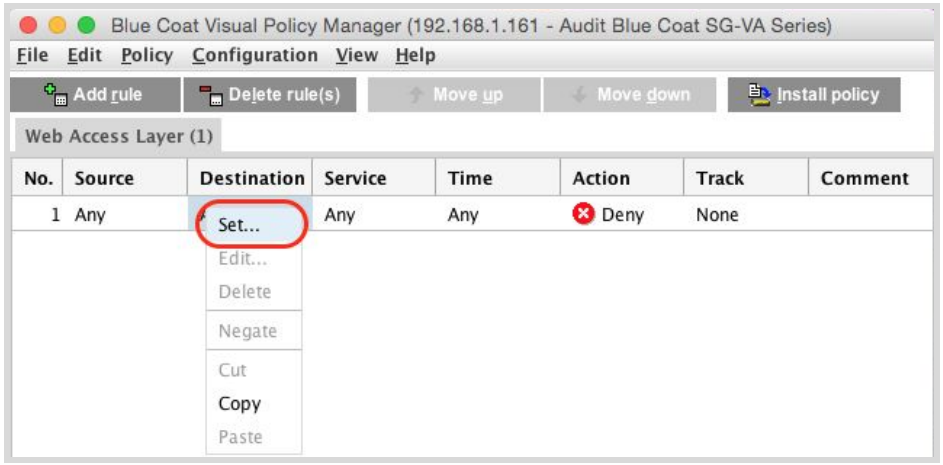
To create a rule that blocks one or more applications by name:

1. On the Symantec ProxySG Management Console, click the **Configuration** tab, select **Policy**, then select **Visual Policy Manager**, and then click **Launch**.

   The application launches Visual Policy Manager (VPM). It might take up to a minute for VPM to open and retrieve data from your appliance.

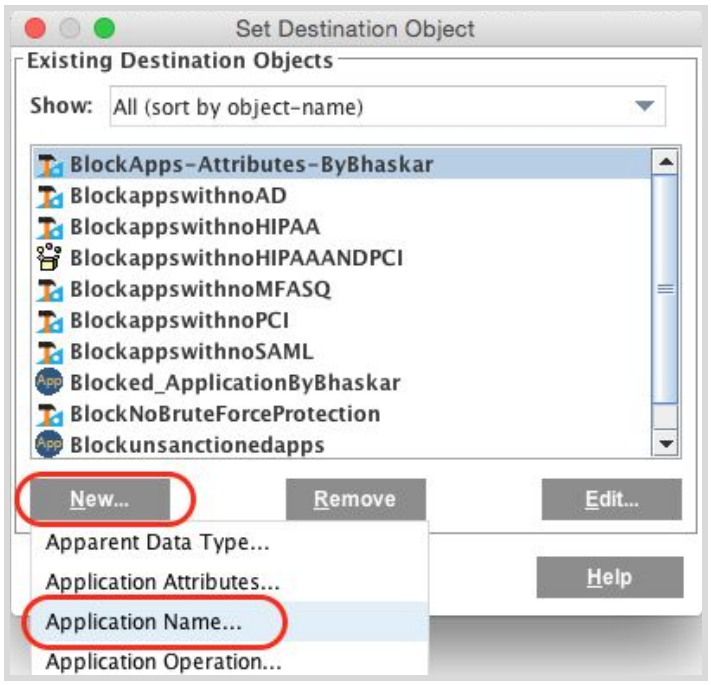
2. In VPM, click **Add Rule**.

3. In the new rule entry, right-click the Destination column and select **Set**.



   VPM opens the Set Destination Object box.

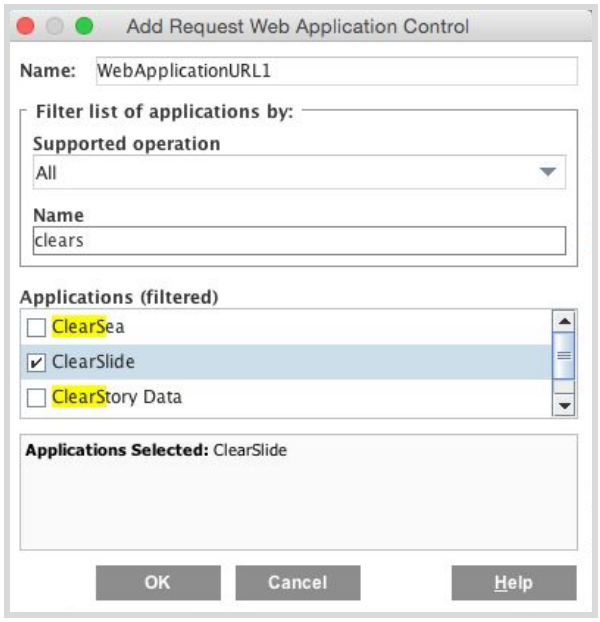
4. Click **New** and select **Application Name** from the menu, as shown in the following.



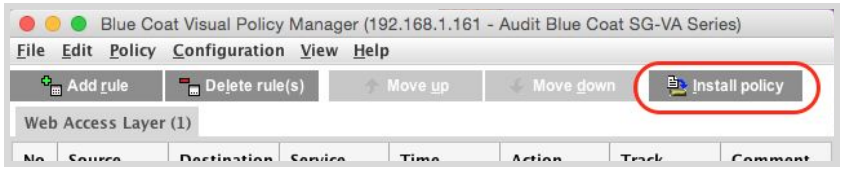
5. VPM opens an Add Request Web Application Control box to show you the available applications.

6. Enter a name for the new attribute object.

7. Find and select one or more applications from among those listed. You can either scroll the list or use the Name tool to narrow your search.



8. Click **OK**.
9. Click **OK** on the Set Destination Object box.
10. On the VPM window, click **Install Policy** to push the new rule to the appliance.



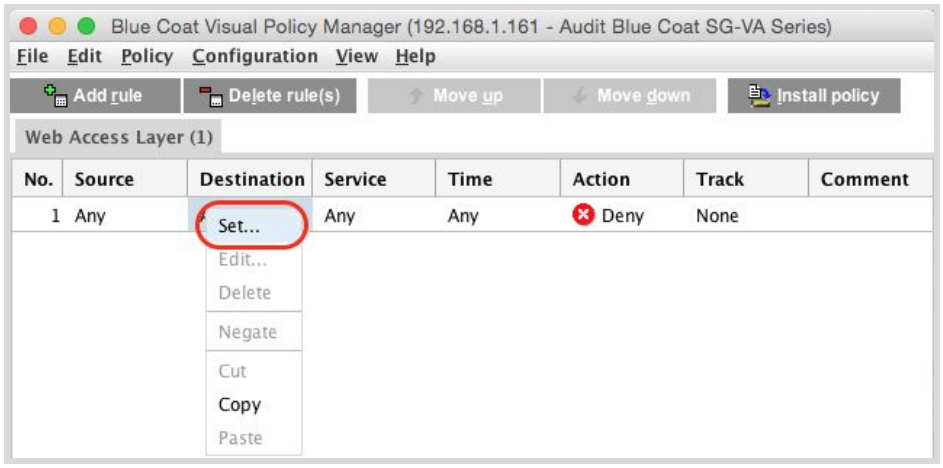
Blocking applications by attribute

To create a rule that blocks applications according to attribute values:

1. On the Symantec ProxySG Management Console, click the **Configuration** tab , select **Policy**, then select **Visual Policy Manager**, and then click **Launch**.

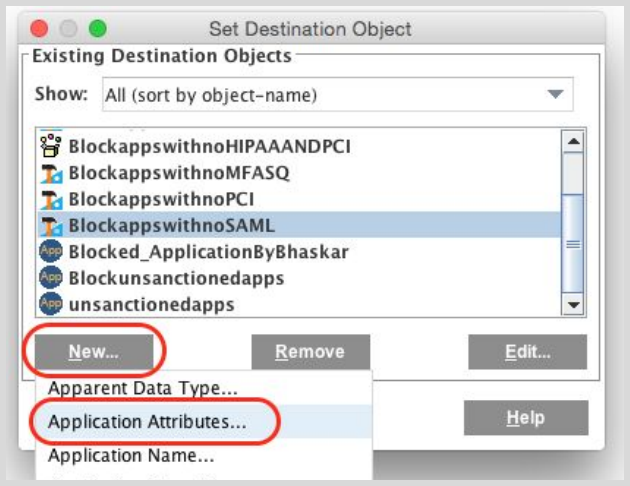
   The application launches Visual Policy Manager (VPM). It might take up to a minute for VPM to open and retrieve data from your appliance.

2. In VPM, click **Add Rule**.
3. In the new rule entry, right-click the Destination column and select **Set**.



   VPM opens the Set Destination Object box.

4. Click **New** and select **Application Attributes** from the menu, as shown in the following.



VPM opens the Add Application Attributes Object box.

5. Enter a name for the new attribute object.

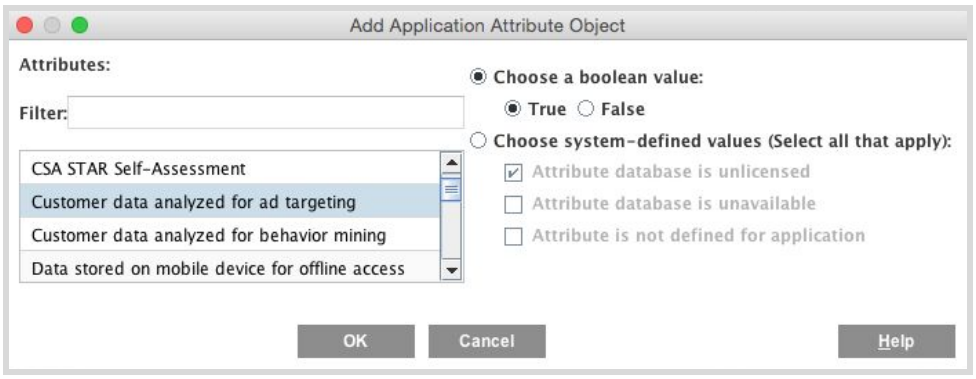
6. Click **Add Attribute**. VPM opens the Add Application Attribute Object box.

7. Find and select the attribute you want to use from those listed. You can either scroll the list or use the Filter box to search the list for text strings that appear in the attribute names.

8. For the attribute value, do one of the following:

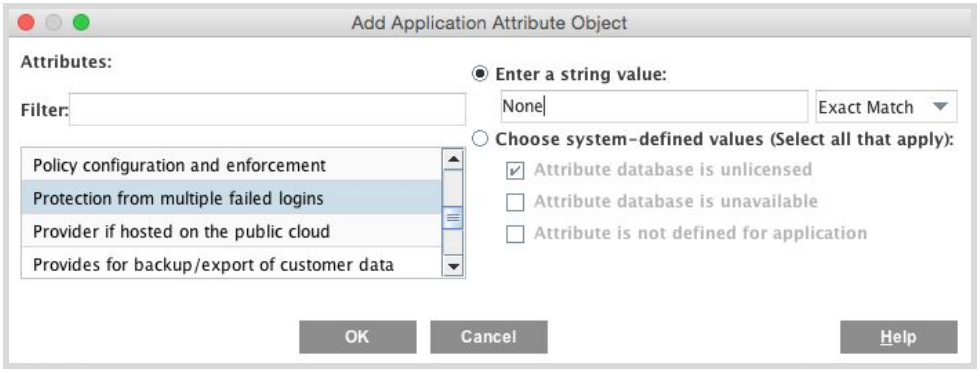
    - Where the attribute takes a boolean value, mark either the True or False radio button.

For example, if you want the rule to block applications that analyze customer data for ad targeting, you would select that attribute and mark the **True** radio button.

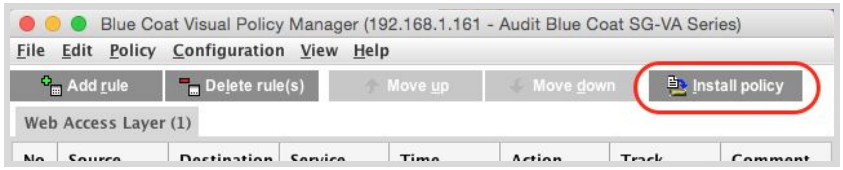


- Where the attribute takes a string value, enter the string exactly as shown in the table in Attributes and Values.

  For example, if you want to block applications that do not protect against brute-force password attacks, you might select **Protection from Multiple Failed Logins** and set the value to **None**.



9. Click **OK** on the Add Attributes Object box.
10. Click **OK** on the Set Destination Object box.
11. On the VPM window, click Install Policy to push the new rule to the appliance.



Blocking applications by combined attributes

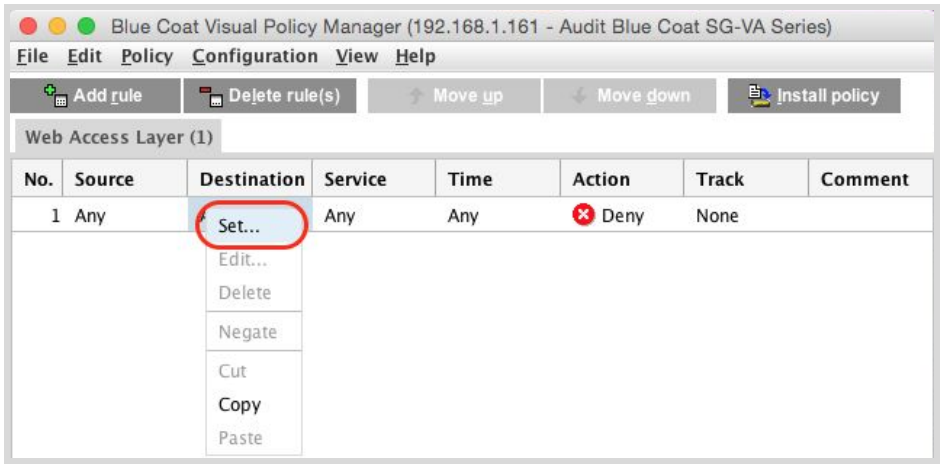
You can create rules that block applications according to combinations of the available attributes. For example, you can create a rule that blocks applications that do not offer either Capcha or brute force login protection, as described in the following.

1. On the Symantec ProxySG Management Console, click **Configuration**, select **Policy**, then select **Visual Policy Manager**, and then click **Launch**.

   The application launches Visual Policy Manager (VPM). It might take up to a minute for VPM to open and retrieve data from your appliance.

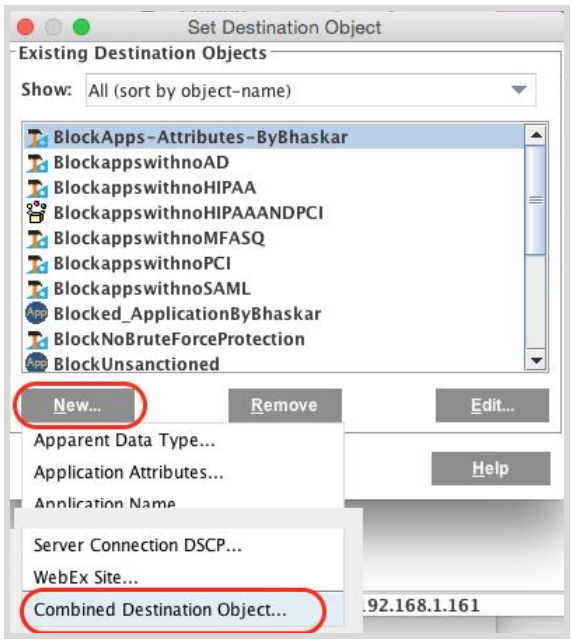
2. In VPM, click **Add Rule**.

3. In the new rule entry, right-click the Destination column and select **Set**.



   VPM opens the Set Destination Object box.

4. Click **New** and select **Combined Destination Object** from the menu, as shown in the following.



   VPM opens the Add Combined Destination Object box.

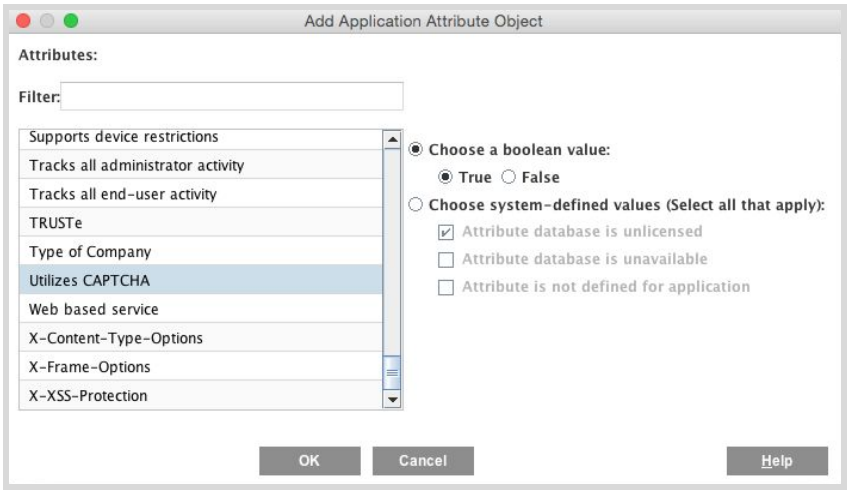
5. Enter a name for the new object.

6. If necessary, create the required objects to combine:

   a. Click **New** and select **Application Attributes**.

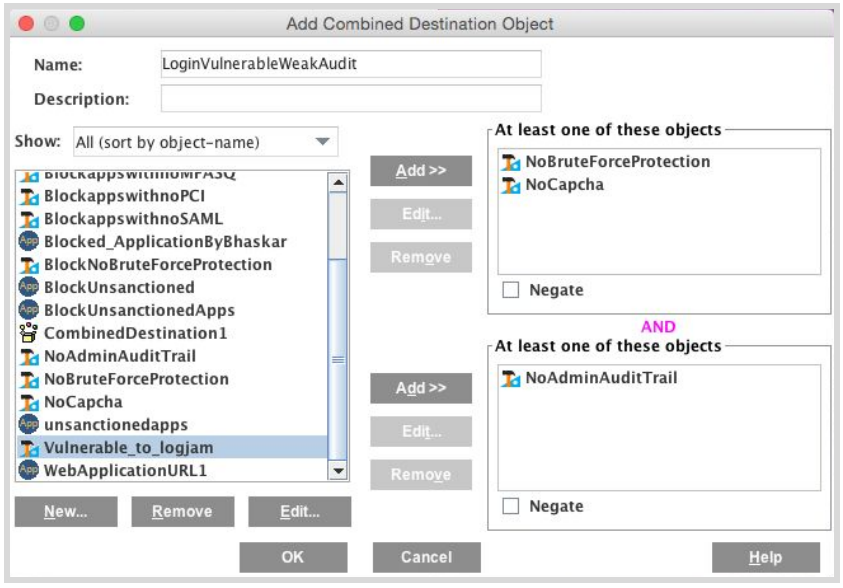
   b. Click Add **Attribute**.

   c. Select an attribute from the list and set its value as appropriate, as shown in the following.



d. Click **OK**.

7. Select objects from the lists on the left to add to the lists on the right as shown in the following.



8. Click **OK** on the Add Combined Destination Object box.

9. On the VPM window, click **Install Policy** to push the new rule to the appliance.

Attributes and Values

This table describes all of the application attributes, and the values you can assign them, in application attribute objects. For the Boolean attribute type, you select either **True** or **False** when you add the attribute object. In all other cases you select **Enter a string value** and enter the string value exactly as shown here.

Attribute Name	**Type**	**Possible Values**
Active Directory integration	Boolean	True, False (Buttons)
Consumer oriented service	Boolean	True, False (Buttons)
Content security policies	Boolean	True, False (Buttons)
Controls IP range from which login is allowed	String	Yes No Partial
Controls sharing with external users	Boolean	True, False (Buttons)
Controls sharing with internal users	Boolean	True, False (Buttons)
CSA STAR Self-Assessment	String	Yes No Partial
Customer data analyzed for ad targeting	Boolean	True, False (Buttons)
Customer data analyzed for behavior mining	Boolean	True, False (Buttons)
Data stored on mobile device for offline access	Boolean	True, False (Buttons)
Default BRR score	String	Number
Desktop client	Boolean	True, False (Buttons)
Encryption keys in control of the Enterprise	Boolean	True, False (Buttons)
Encrypts data at rest	Boolean	True, False (Buttons)
Enterprise oriented service	Boolean	True, False (Buttons)
Force change of password after some time period	Boolean	True, False (Buttons)
HIPAA	String	Yes No Partial
Hosting Platform Type	String	Hybrid Public Private
HTTP STS	Boolean	True, False (Buttons)
ISO 27001	String	Yes No Partial
ISO 27018	Boolean	True, False (Buttons)
LDAP integration	Boolean	True, False (Buttons)

Attribute Name	Type	Possible Values
Multi-factor authentication - Security Questions	Boolean	True, False (Buttons)
Multi-factor authentication via Biometrics	Boolean	True, False (Buttons)
Multi-factor authentication via Mobile App	Boolean	True, False (Buttons)
Multi-factor authentication via secondary email	Boolean	True, False (Buttons)
Multi-factor authentication via Smartcard	Boolean	True, False (Buttons)
Multi-factor authentication via SMS	Boolean	True, False (Buttons)
Multi-factor authentication via USB Token	Boolean	True, False (Buttons)
Native mobile app	Boolean	True, False (Buttons)
Not Vulnerable to FREAK	Boolean	True, False (Buttons)
Not Vulnerable to Logjam	Boolean	True, False (Buttons)
Not Vulnerable to OpenSSL Heartbleed defect	Boolean	True, False (Buttons)
Not Vulnerable to Poodle SSLv3	Boolean	True, False (Buttons)
OAuth support	Boolean	True, False (Buttons)
Offline data encrypted or otherwise protected	Boolean	True, False (Buttons)
OpenID support	Boolean	True, False (Buttons)
PCI	String	Yes No Partial
Policy configuration and enforcement	Boolean	True, False (Buttons)
Protection from multiple failed logins	String	None Account Lockout Progressive Backoff
Provider if hosted on the public cloud	String	Amazon Digital Ocean Google Heroku Linode MS Azure Rackspace Verizon Other
Provides for backup/export of customer data	Boolean	True, False (Buttons)
Provides password reset and recovery	Boolean	True, False (Buttons)
Published SLA	Boolean	True, False (Buttons)
Remember me functionality for login	Boolean	True, False (Buttons)

Attribute Name	Type	Possible Values
Requires minimum password length	Boolean	True, False (Buttons)
Requires strong password format	Boolean	True, False (Buttons)
REST API Support	Boolean	True, False (Buttons)
Role based access control	Boolean	True, False (Buttons)
Safe Harbor	String	Both US-Swiss No US-EU
SAML support	Boolean	True, False (Buttons)
Separation of Customer Data	String	None Data level Isolated database Separate VM
SSAE 16 SOC2 Type II	String	Yes No Data center only
SSL certificate strength	String	Less than 2048 bits No SSL 2048 bits or greater
SSL key strength	String	256 bits or greater Less than 256 bits No SSL
SSL used for data in motion	Boolean	True, False (Buttons)
Supports device restrictions	Boolean	True, False (Buttons)
Tracks all administrator activity	Boolean	True, False (Buttons)
Tracks all end-user activity	Boolean	True, False (Buttons)
TRUSTe	String	Yes No Partial
Type of Company	String	Funded Startup Startup Public Private
Utilizes CAPTCHA	Boolean	True, False (Buttons)
Web based service	Boolean	True, False (Buttons)
X-Content-Type-Options	Boolean	True, False (Buttons)
X-Frame-Options	Boolean	True, False (Buttons)
X-XSS-Protection	Boolean	True, False (Buttons)

Revision history

Date	Version	Description
19 July 2016	1.0	Initial release
30 April 2019	1.1	Address Symantec branding, other minor changes
23 September 2020	1.2	Minor changes