Configuring, Automating and Analyzing Custom Reports

Professional Services - Security Management Framework

PAN-OS 8.1

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

About This Document

The Operational Enablement documents are designed to enable and inform customers on how to manage Palo Alto Networks technologies consistently and efficiently. These documents assume that the reader is already familiar with Palo Alto Networks technology and they are meant to serve as sections within a runbook on how to manage the platform once deployed.

These documents do not replace other technical documentation published by Palo Alto Networks on their products and features. For more information about anything referenced in this document, see the technical documentation found at:
https://www.paloaltonetworks.com/documentation

Table of Contents

Overview

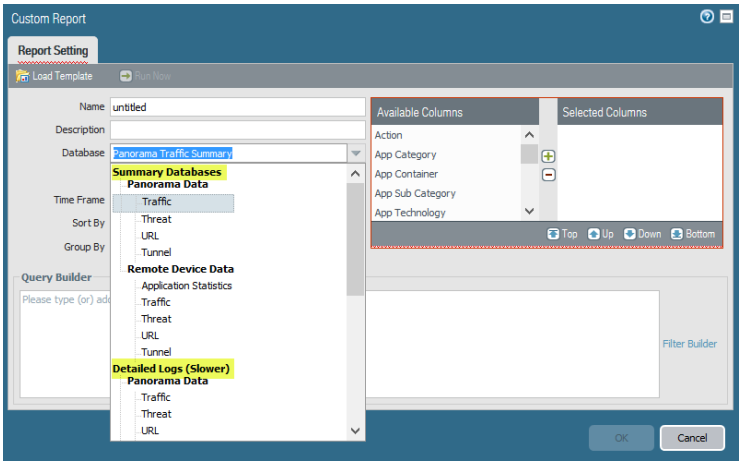
Customized reports can provide useful and specific information by filtering on conditions and columns to display the information we need. This document will provide the steps to create custom reports, automate delivery and frequency, and how to analyze them.

Custom Reports Components

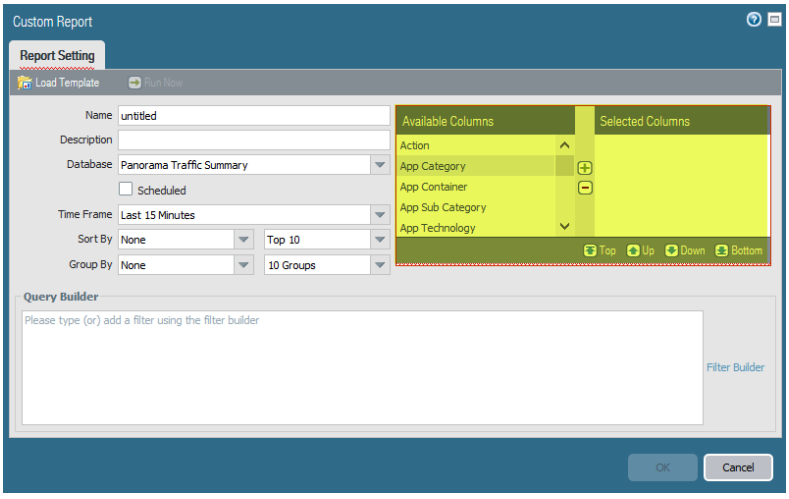
The firewall or Panorama can create powerful reports based on attributes and key pieces of information that need to be retrieved and analyzed.

The components of a custom report are described below.

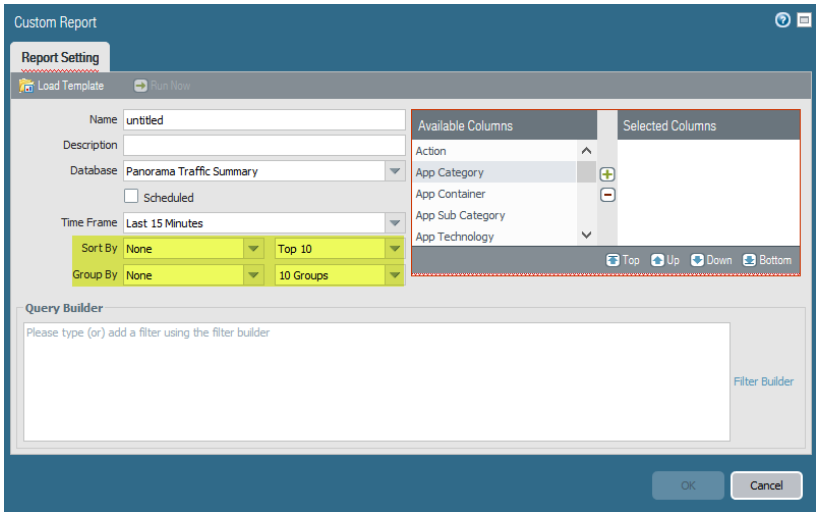
1. Database
   - Summary databases - Available for Application Statistics, Traffic, Threat, URL Filtering, and Tunnel Inspection logs.
   - Detailed logs - These databases itemize the logs and list all the attributes (columns) for each log entry.



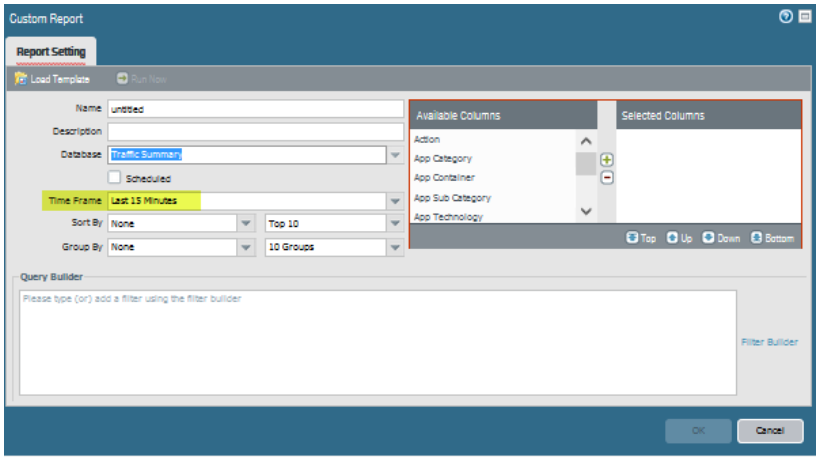
2. Attributes: - The attributes are the columns that are available for selection in a report. From the list of Available Columns, you can add the selection criteria for matching data and for aggregating the details (the Selected Columns).



3. Sort By and Group By
   - The Sort By option specifies the attribute that is used for aggregation. If you do not select an attribute to sort by, the report will return the first N number of results without any aggregation.
   - The Group By option allows you to select an attribute and use it as an anchor for grouping data; all the data in the report is then presented in a set of top 5, 10, 25 or 50 groups.



4. Time Frame: The date range for which you want to analyze data. You can define a custom range or select a time period ranging from the last 15 minutes to the last 30 days. The reports can be run on demand or scheduled to run at a daily or weekly cadence.



5. Query Builder - The query builder allows you to define specific queries to further refine the selected attributes. It allows you see just what you want in your report using *and* and *or* operators and a match criteria, and then include or exclude data that matches or negates the query in the report.

   To build a report query, specify the following and click **Add.** Repeat as needed to construct the full query.

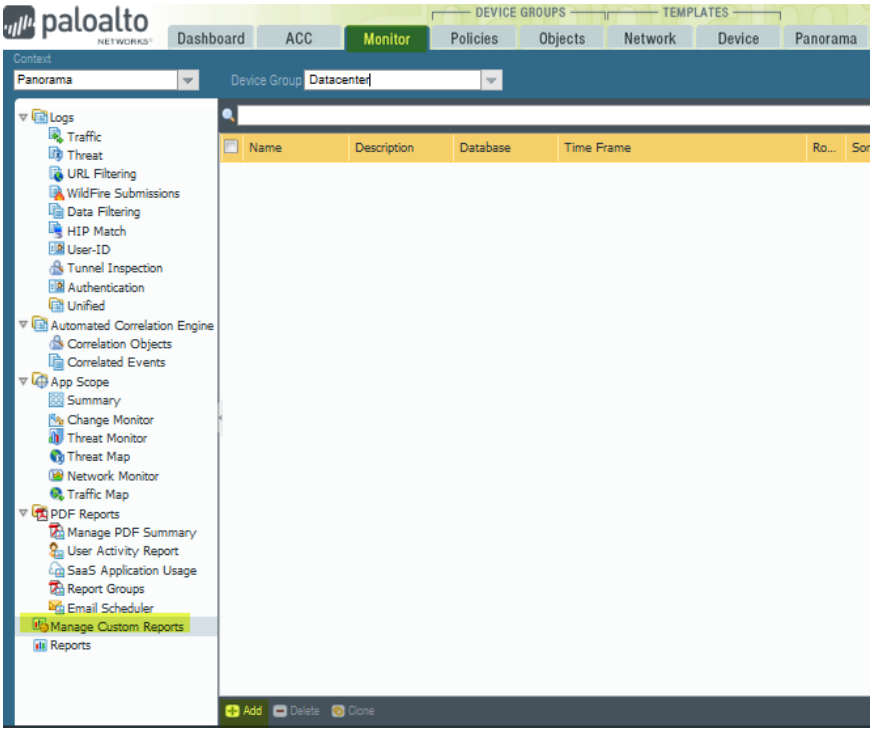
   - Connector - Choose the connector (and/or) to precede the expression you are adding.
   - Negate - Select the check box to interpret the query as a negation. If, for example, you choose to match entries in the last 24 hours and/or are originating from the untrust zone, the negate option causes a match on entries that are not in the past 24 hours and/or are not from the untrust zone.
   - Attribute - Choose a data element. The available options depend on the choice of database.
   - Operator - Choose the criterion to determine whether the attribute applies (such as equal). The available options depend on the choice of database.
   - Value - Specify the attribute value to match.

6. Run Now - Executes the report.

Generate Custom Reports

To create a custom report that the firewall generates immediately follow the steps below. This report will display *Unknown* outbound *URL categories* seen in URL logs in the last hour, sorted by *hit count* and grouped by *rule.*

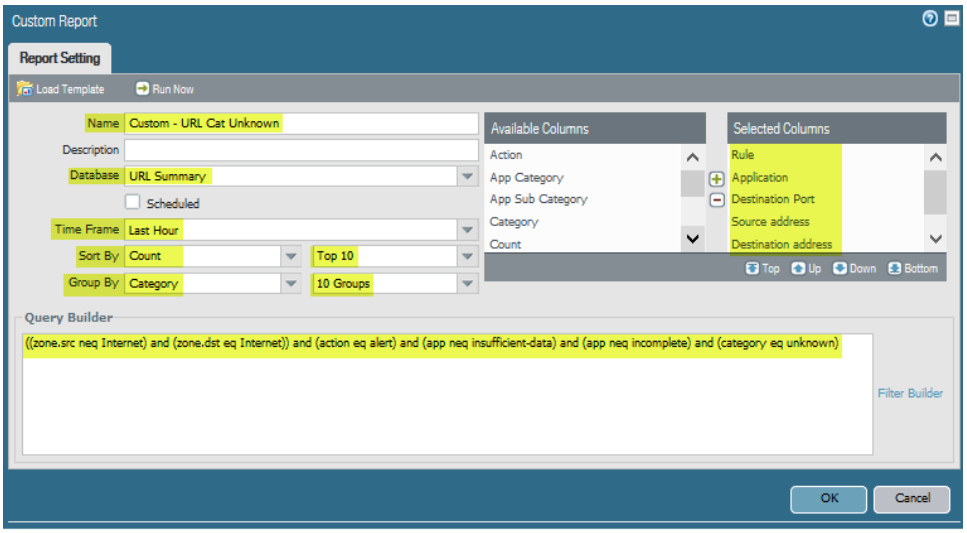
1. Navigate to **Monitor** > **Manage Custom Reports** > **Add**

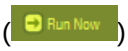


2. Enter a **Name** for the report: *Custom - URL Cat Unknown*

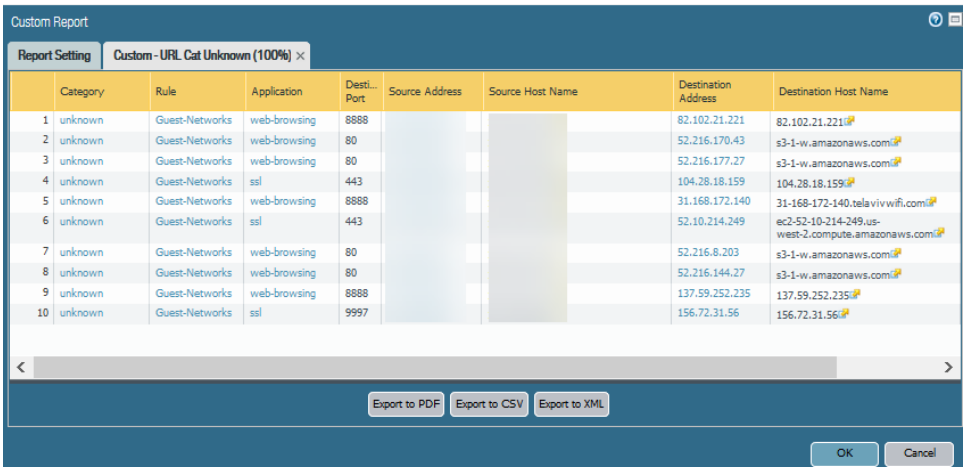
3. Select a Database: *URL Summary*
4. Time Frame – *Last Hour*
5. Sort By: Count – *Top 10*
6. Group By: Category – *10 Groups*
7. Columns:
    - Rule
    - Application
    - Destination Port
    - Source Address
    - Destination Address
    - Destination Country
8. Query - For this report we will build a query that looks into the URL logs with a *source zone* not equal to the *Internet* zone (untrust zone in this firewall), a *destination zone* equal to the *Internet* zone, *action* equal to *alert*, every application except *insufficient-data* and *incomplete*, and *URL category* equal to *unknown.*

    ((zone.src neq Internet) and (zone.dst eq Internet)) and (action eq alert) and (app neq insufficient-data) and (app neq incomplete) and (category eq unknown)



9. Click **Run Now** button to generate the report (

)
10. Review the results of the report



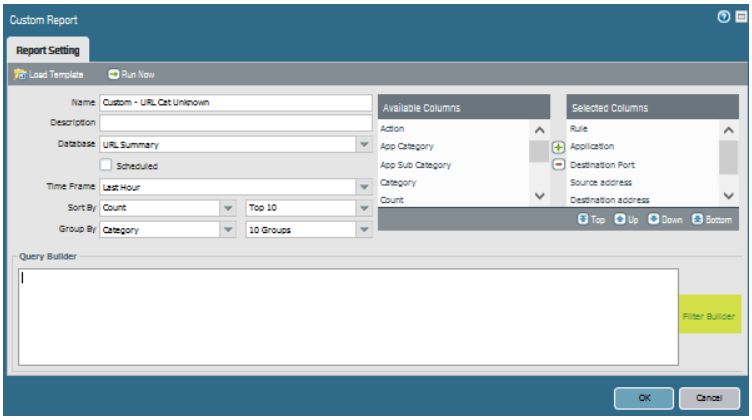
11. *Optional* – Export the report to PDF, CSV, or XML
12. Click **OK** to save the custom report

Using the Filter Builder to build queries

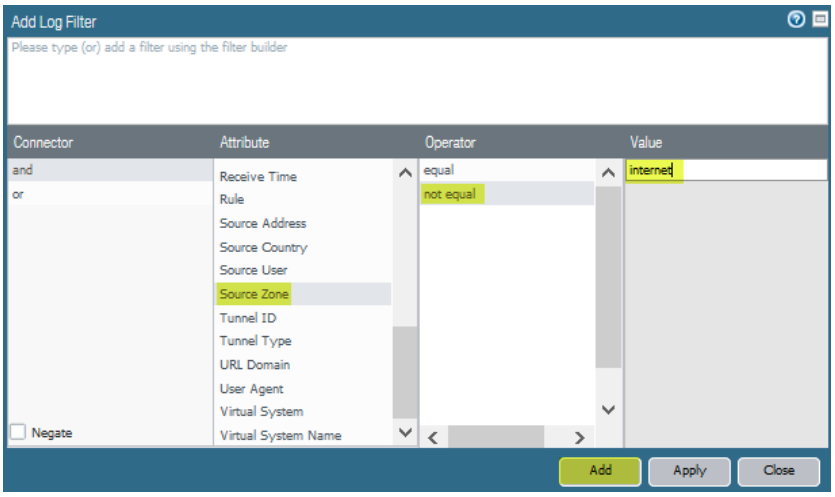
The filter builder lets you immediately choose if you want to add an *AND* or *OR* operated filter. You can then select the attribute you want to search for, select its own operator, and set the value.

Following the example in the previous report, we will use the Filter Builder to build a query used to filter URL logs for outbound Unknown categories.

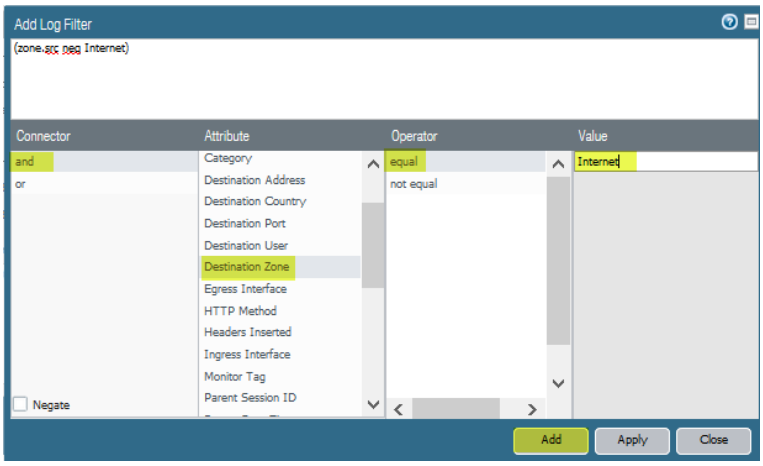
1. Click the **Filter Builder** link in the **Custom Report** menu.



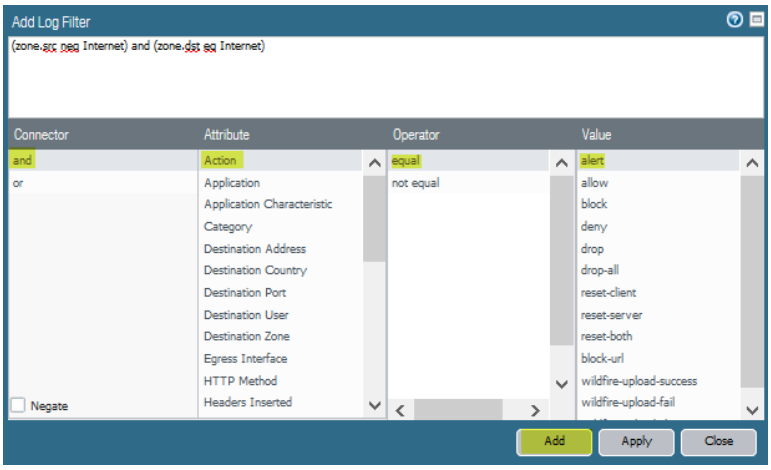
2. Create a *Source Zone not equal to Internet* (Untrust Zone) filter and click **Add.**



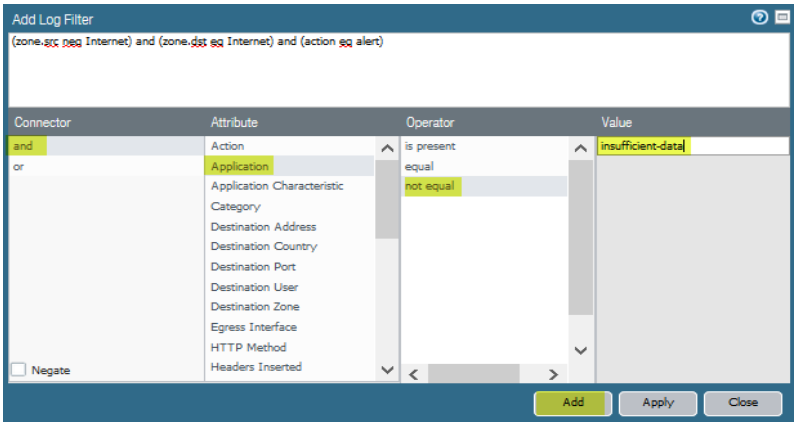
3. Add an *and* connector and create a *Destination Zone equal Internet* (Untrust Zone) filter and click **Add**.



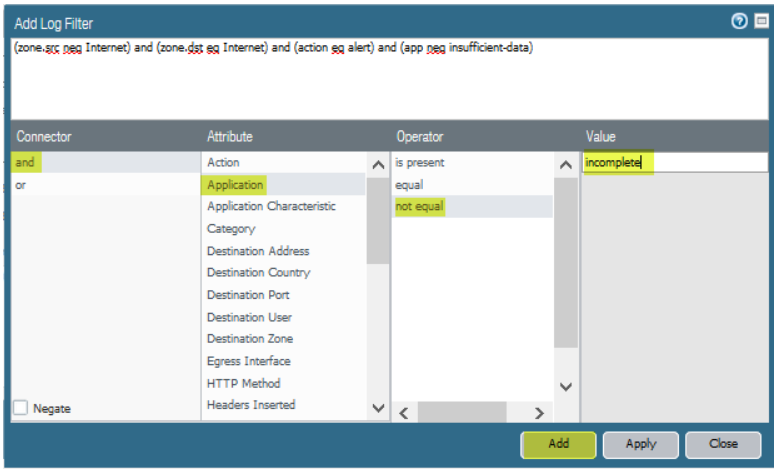
4. Add an *and* connector and an *Action equal Alert* filter. Click **OK.**



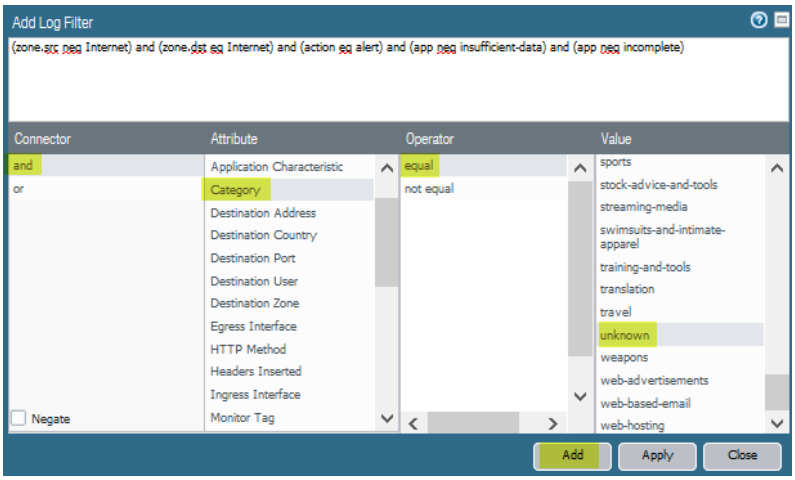
5. Add the next filter to exclude the *insufficient-data* application and click **Add**.



6. Add the next filter to exclude the *incomplete* application and click **Add**.



7. For the last filter for the query select the *unknown* URL Category and click **Add**.

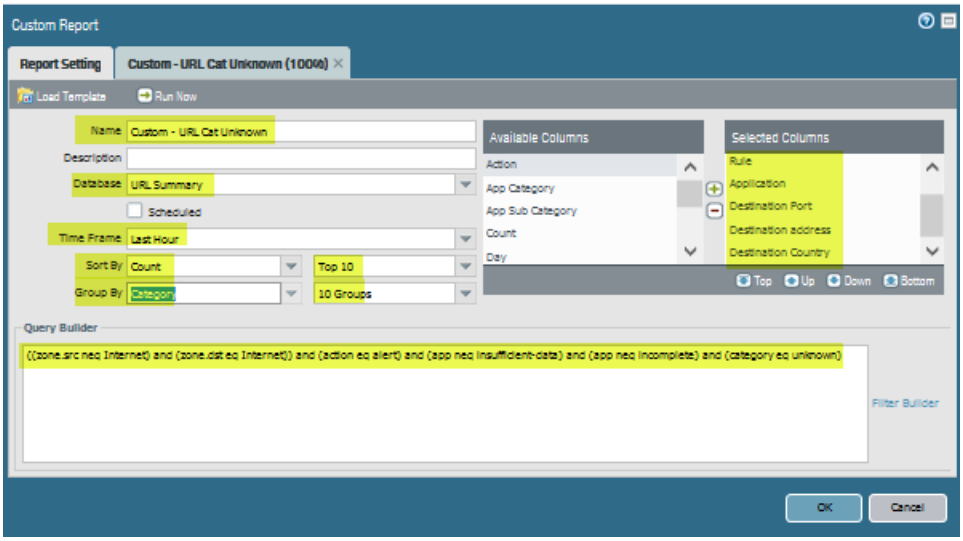


Analyzing a Custom Report

Unknown outbound URL category report

Once we have created a custom report configured settings to look into the URL filtering logs for outbound traffic with an unknown URL category, then we export the PDF file for review.

The following figure shows the Custom Report settings for this report.



The following figure shows the Outbound Unknown URL Category PDF report.

Custom - URL Cat Unknown

[redacted]: 2019/04/04 15:42:43 - 2019/04/04 16:42:42

Category	Rule	Application	Destination Port	Destination address	Destination Host Name	Destination Country
unknown	Guest-Networks	web-browsing	80	52.216.137.60	s3-1-w.amazonaws.com	United States
unknown	Guest-Networks	web-browsing	80	52.216.100.3	52.216.100.3	United States
unknown	Guest-Networks	web-browsing	80	52.216.10.59	s3-1-w.amazonaws.com	United States
unknown	Guest-Networks	web-browsing	80	52.216.104.155	s3-1-w.amazonaws.com	United States
unknown	Guest-Networks	web-browsing	8888	66.115.168.31	66.115.168.31	United States
unknown	Guest-Networks	web-browsing	80	52.216.234.43	52.216.234.43	United States
unknown	Guest-Networks	web-browsing	80	54.236.254.58	ec2-54-236-254-58.compute-1.amazonaws.com	United States
unknown	Guest-Networks	web-browsing	80	52.216.171.3	s3-1-w.amazonaws.com	United States
unknown	Guest-Networks	web-browsing	80	52.216.168.27	s3-1-w.amazonaws.com	United States
unknown	Guest-Networks	ssl	443	54.254.181.159	ec2-54-254-181-159.ap-southeast-1.compute.amazonaws.com	Singapore

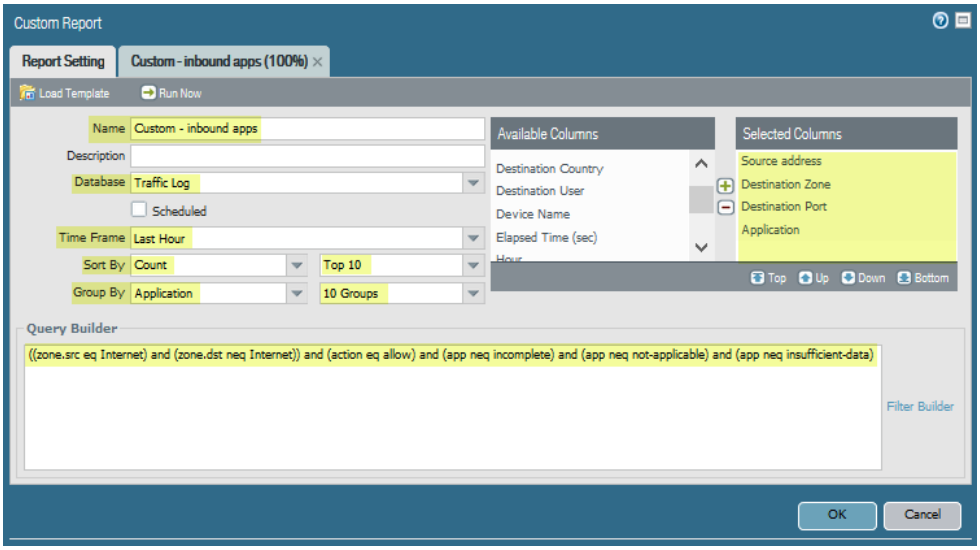
The report is used to evaluate outbound URL traffic classified as Unknown in the past hour. The report attributes (Rule, Application, Destination Port, Destination Address and Hostname, and Country) provide information useful to determine if the URL or domain should be allowed or denied.

Uncategorized URLs are a common risk and could be an indicator of compromise.

Identify Inbound Applications Report

Create this report to identify all inbound applications and determine which are valid and which need to be blocked.

The following figure shows the Custom Report settings for this report.



The following figure shows the Inbound Applications PDF report.

Custom - inbound apps

[redacted]: 2019/04/04 18:19:18 - 2019/04/04 19:19:17

Application	Source address	Source Host Name	Destination Zone	Destination Port
dns	45.42.32.20	vrnawi-sdns-001.epichosted.com	DMZ	53
dns	74.125.80.65	74.125.80.65	DMZ	53
ssl	73.11.138.22	c-73-11-138-22.hsd1.wa.comcast.net	DMZ	443
ssl	216.9.28.130	28-130.pool.cnw.net	DMZ	443
ssl	73.169.214.88	c-73-169-214-88.hsd1.wa.comcast.net	DMZ	443
ssl	97.41.149.26	26.sub-97-41-149.myvzw.com	DMZ	443
ssl	174.208.25.41	41.sub-174-208-25.myvzw.com	DMZ	443
ssl	71.231.122.82	c-71-231-122-82.hsd1.wa.comcast.net	DMZ	443
ssl	73.97.132.188	c-73-97-132-188.hsd1.wa.comcast.net	DMZ	443
ssl	67.183.165.231	c-67-183-165-231.hsd1.wa.comcast.net	DMZ	443

This report displays the top 10 inbound application in the past hour, source addresses, source hostnames, and the destination zones and ports. This information can be valuable to create rules to block or allow inbound traffic.

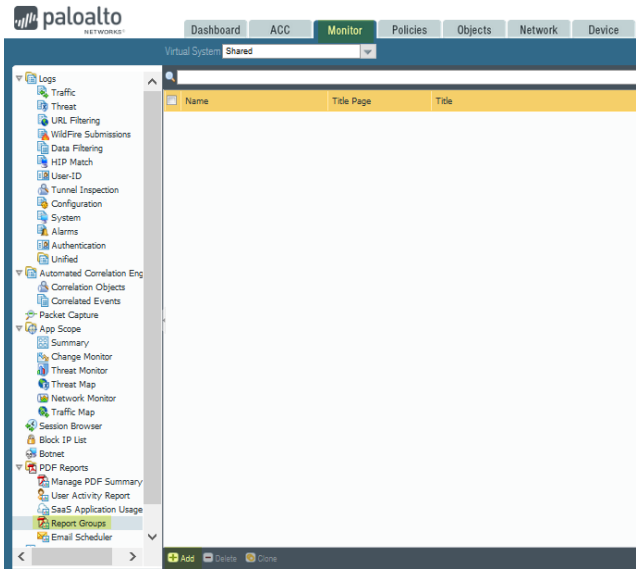
Report Groups

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

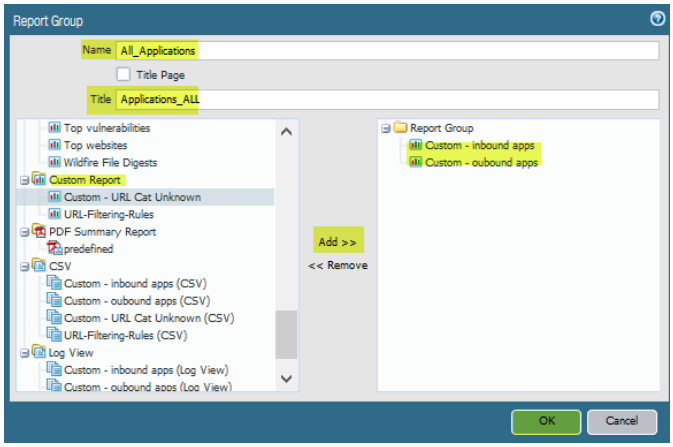
Configure Report Groups

1. Configure an Email server profile
    a. Select **Device** > **Server Profiles** > **Email**.
    b. Click **Add** and enter a Name for the profile.
    c. If the firewall has more than one virtual system (vsys), select the Location (vsys or Shared) where this profile is available.
    d. For each Simple Mail Transport Protocol (SMTP) server (email server), click **Add** and define the following information:
        - *Name*: Name to identify the SMTP server (1-31 characters). This field is just a label and doesn't have to be the hostname of an existing email server.
        - *Email Display Name*: The name to show in the From field of the email.
        - *From*: The email address from which the firewall sends emails.
        - *To*: The email address to which the firewall sends emails.
        - *Additional Recipient*: If you want to send emails to a second account, enter the address here. You can add only one additional recipient. For multiple recipients, add the email address of a distribution list.
        - *Email Gateway*: The IP address or hostname of the SMTP gateway to use for sending emails.
    e. Click **OK** to save the Email Server Profile.

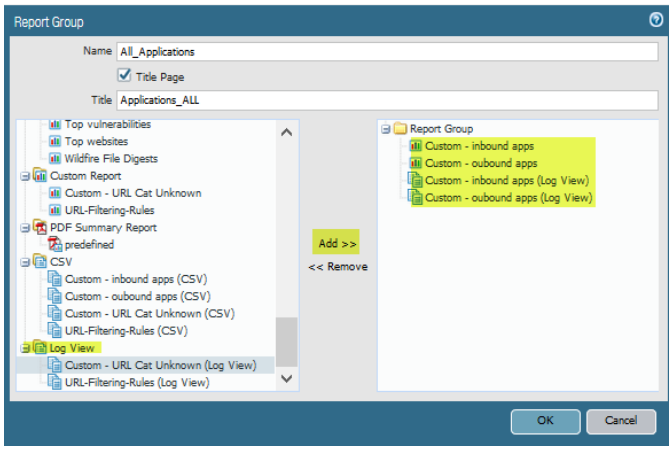
2. Define the Report Group.
    a. Select **Monitor** > **Report Group** > **Add**



    b. Enter a name for the report group and select **Custom Report** from the left column and click **Add** to move each report to the group in the right



c. (Optional) – Include the Log View Data when creating a report group by adding the custom reports under Log View. The report will include the custom report data and the log data that was used to create the custom report.

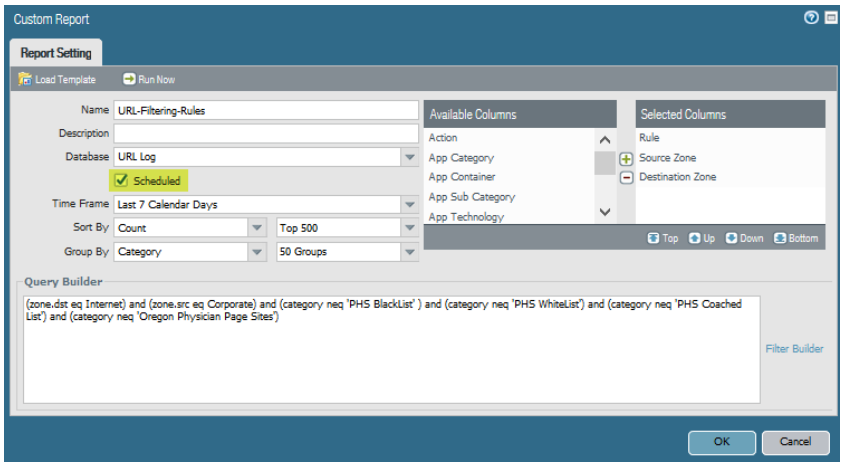


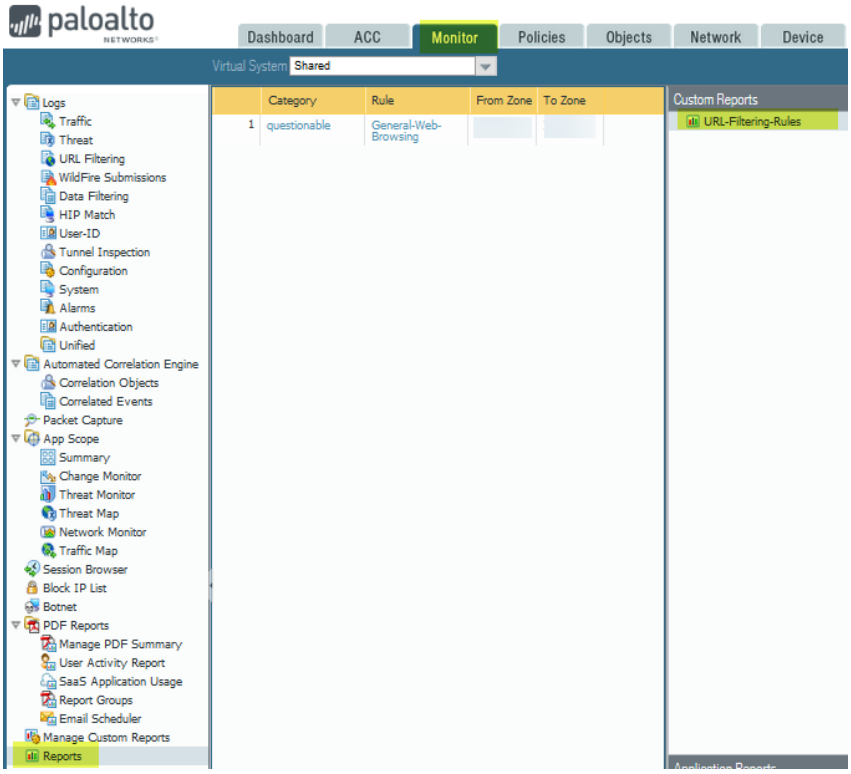
d. Click **OK** to save the settings.

Automate Report Creation and Delivery

Schedule Custom Reports

Custom reports can be scheduled to run each night by selecting the **Scheduled** checkbox, the report is then available for viewing in the **Reports** column on the left menu.



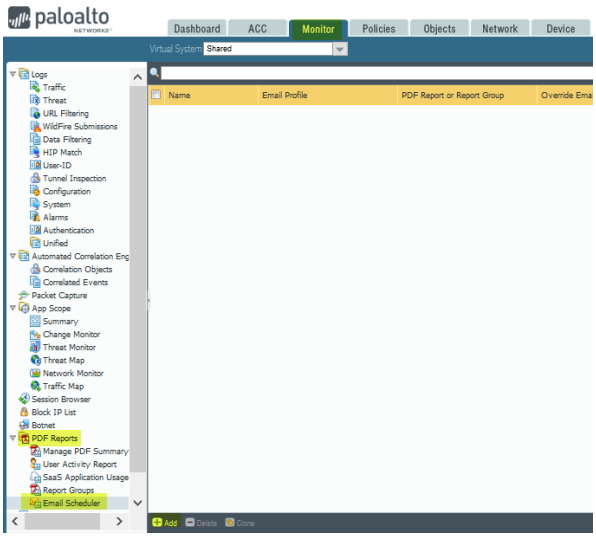


Schedule Reports for Email Delivery

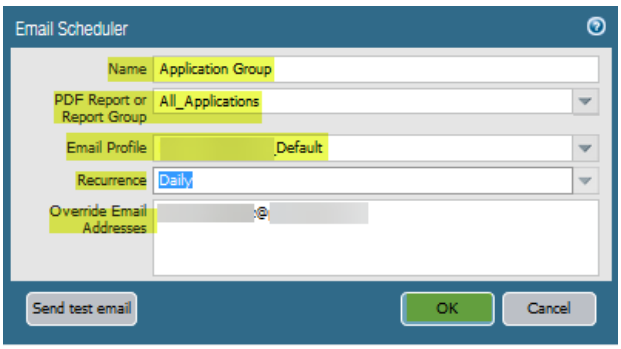
Reports can be scheduled for daily delivery or delivered weekly on a specified day. Scheduled reports are executed starting at 2:00 AM, and email delivery starts after all scheduled reports have been generated.

Following are the steps to configure email delivery:

1. Select **Monitor** > **PDF Reports** > **Email Scheduler** and click **Add**.



2. Enter a **Name** to identify the schedule.
3. Select the **Report Group**.
4. Select the **Email Profile** to use for delivering the reports.
5. Under **Recurrence** select the frequency at which to generate and send reports.
6. Optional – Use the **Override Email Addresses** option to send the report exclusively to the specified recipients.
7. Click **OK** and **Commit**.



Background Information

Visibility plays a key factor in stopping an attack while providing the necessary information to improve the security posture of an organization continuously. The ability to customize, analyze and automate delivery of reports enables security operations and management to make decisions that will help them stop and prevent security-related events.