Application Control Center

Log correlation and reporting

Powerful log filtering enables administrators to quickly investigate security incidents by correlating threats with applications and user identity. The ACC provides a comprehensive view of current and historical data – including network activity, application usage, users, and threats – in a highly visual, fully customizable, and easy-to-use interactive format. This visibility enables administrators to make informed policy decisions and respond quickly to potential security threats.

The ACC provides a tabbed view of network activity, threat activity, and blocked activity, and each tab includes pertinent widgets for better visualization of traffic patterns on the network (see Figure 2-12).

Figure 2-12

The ACC provides a highly visual, interactive, and customizable security management dashboard.

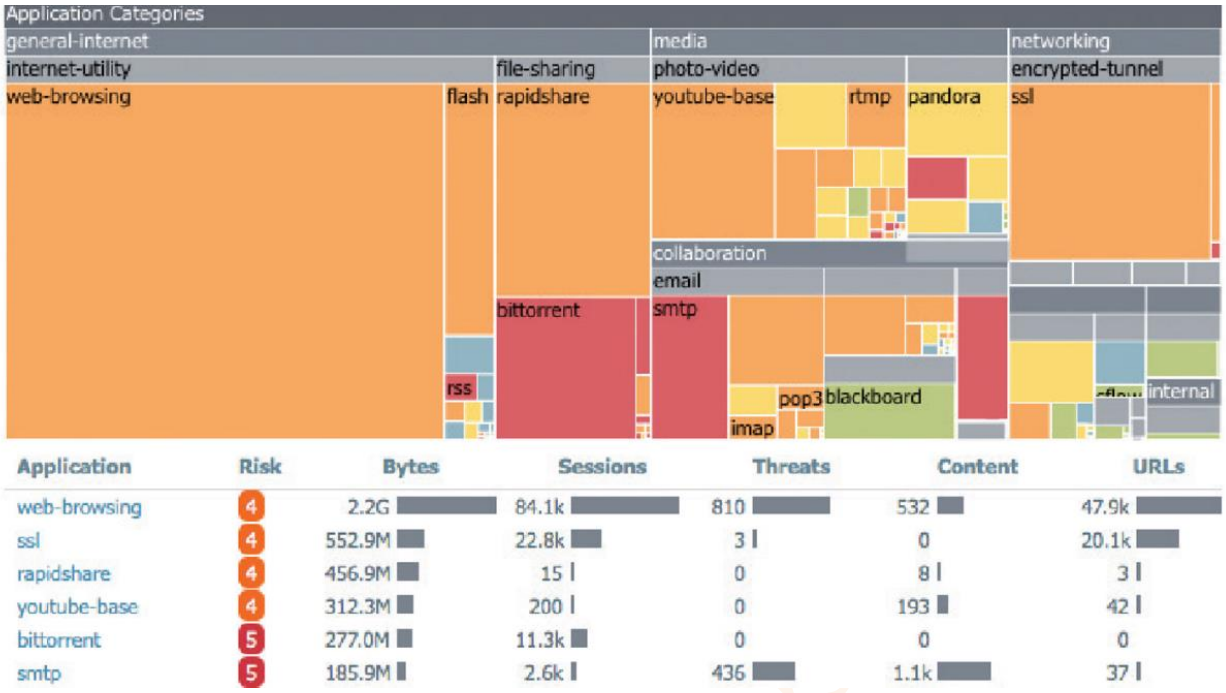
Figure 2-13 shows a core widget of the ACC, the Application Usage widget. In this case, the widget

shows application traffic in bytes. Applications (colored boxes) are grouped in application categories (gray bars). The size of each box indicates how much traffic a given application consumed during the selected time frame. The color of the box indicates the risk level of an application, with red being critical, orange medium, and blue the lowest risk. The tabular listing below the graph shows additional information, such as the number of sessions, threats detected, content or files included, and URLs accessed by these applications.

Figure 2-13

The ACC Application Usage widget displays application traffic by type, amount, risk, and category.

In Figure 2-14, an ACC widget shows source and destination by region, with a visual display of where



traffic is originating and going. The world maps are interactive and provide the ability to get more detail and information about traffic to or from individual countries.

Figure 2-14

Geolocation awareness in the ACC provides valuable information about source and destination of all application traffic.

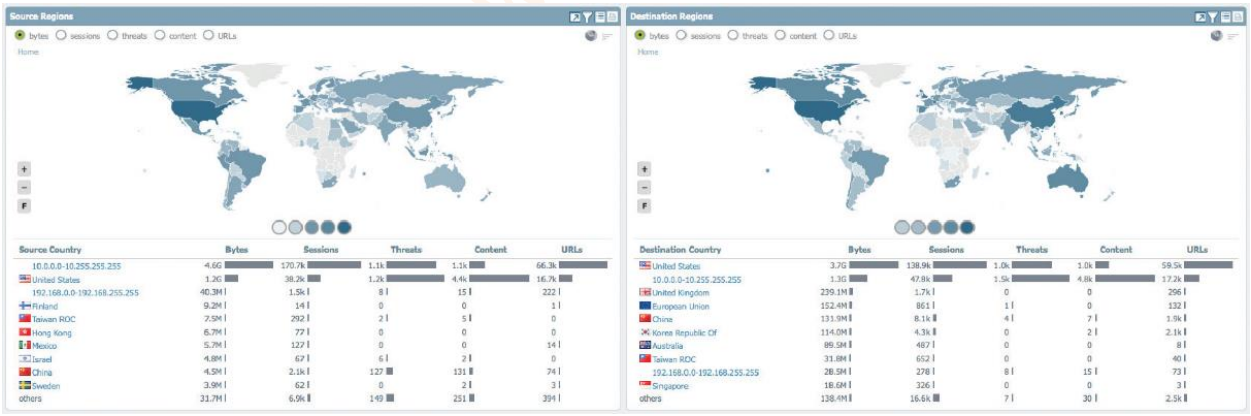
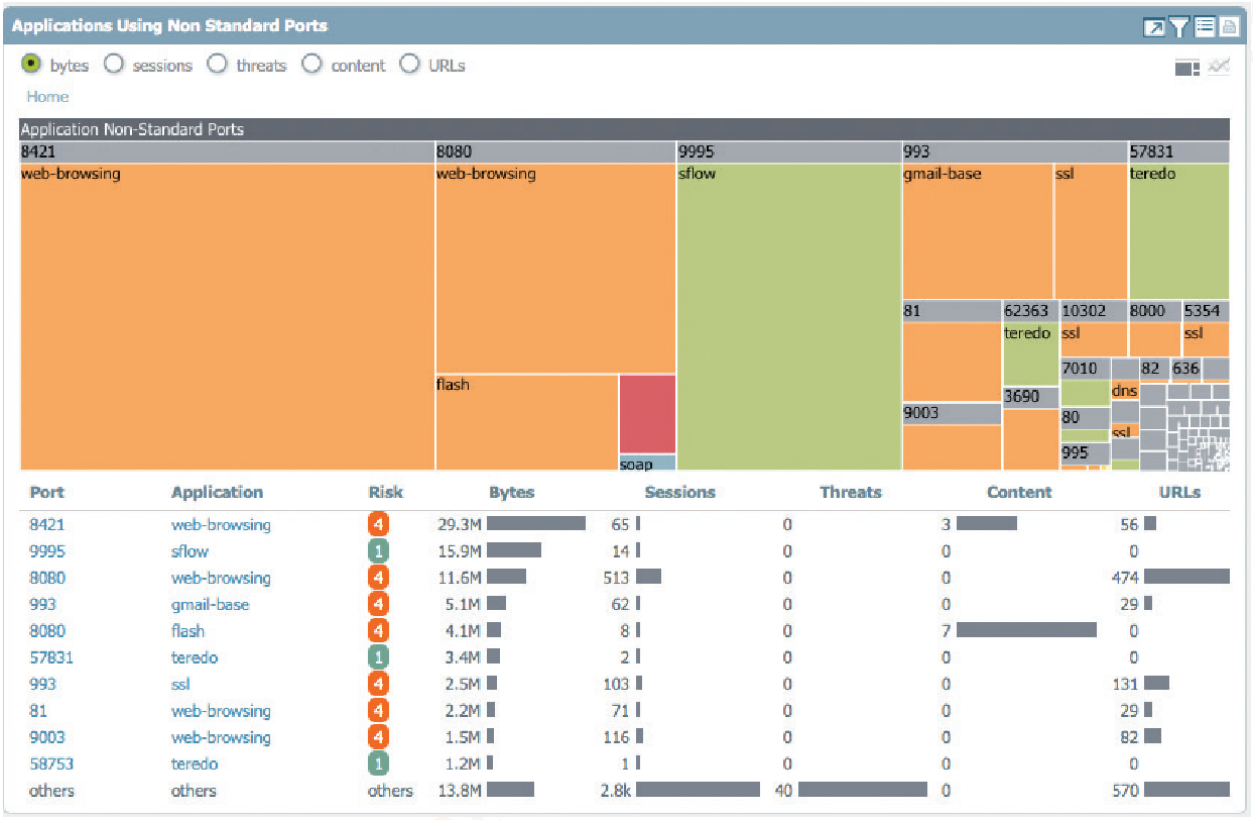


Figure 2-15 shows an ACC widget that demonstrates the power of application control in an next-generation firewall versus a traditional port-based firewall. This widget shows applications with port hopping capabilities using non-standard ports.

Figure 2-15

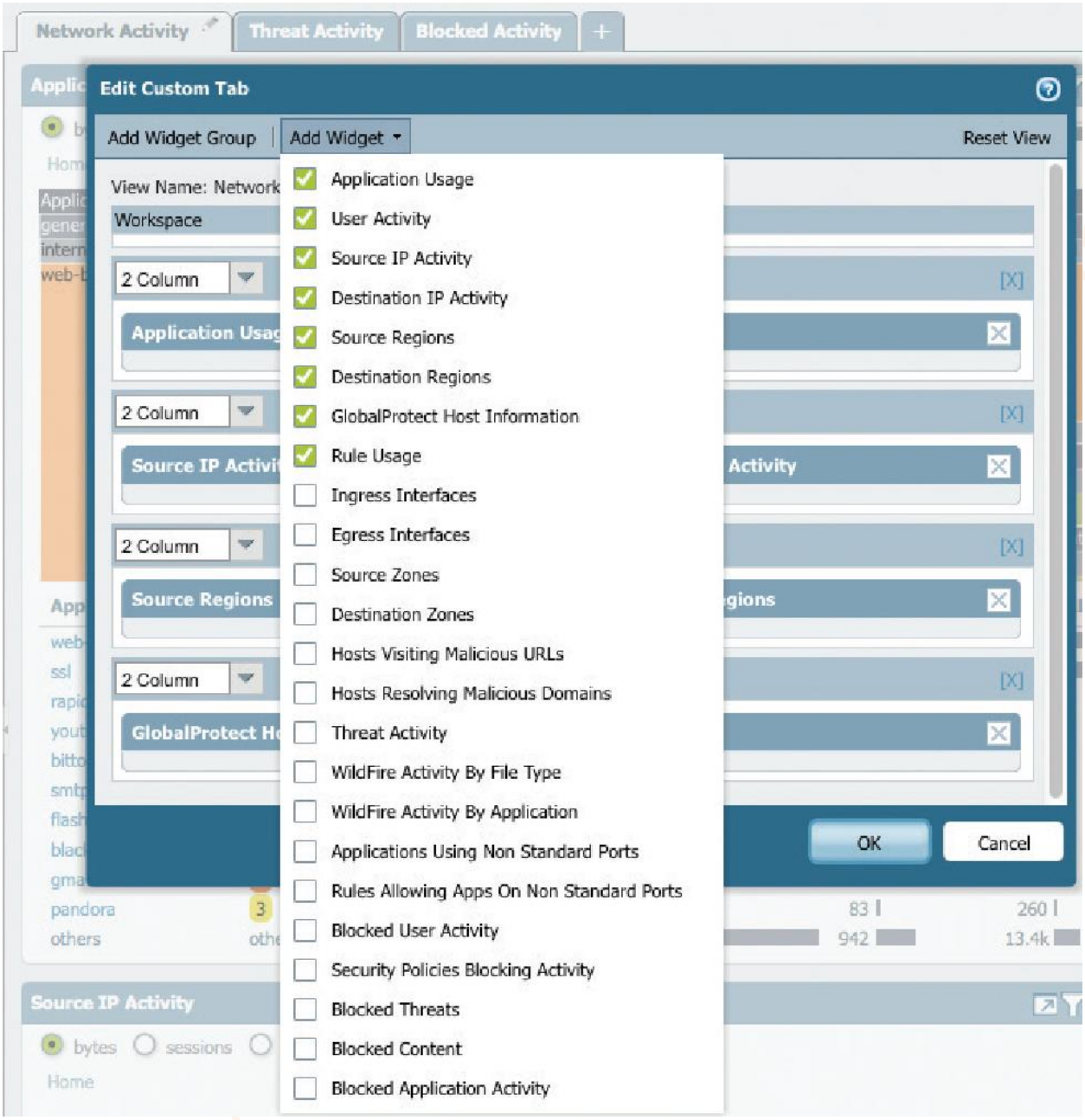
The ACC Applications Using Non Standard Ports widget highlights port hopping and showcases the importance of application versus port control.



Custom tabs can also be created that include widgets that enable administrators to view more specific information. With the ACC, every administrator can customize their own views by selecting predesigned widgets from a drop-down list and building their own user interface (see Figure 2-16).

Figure 2-16

A wide variety of widgets can be selected to customize tabs in the ACC.

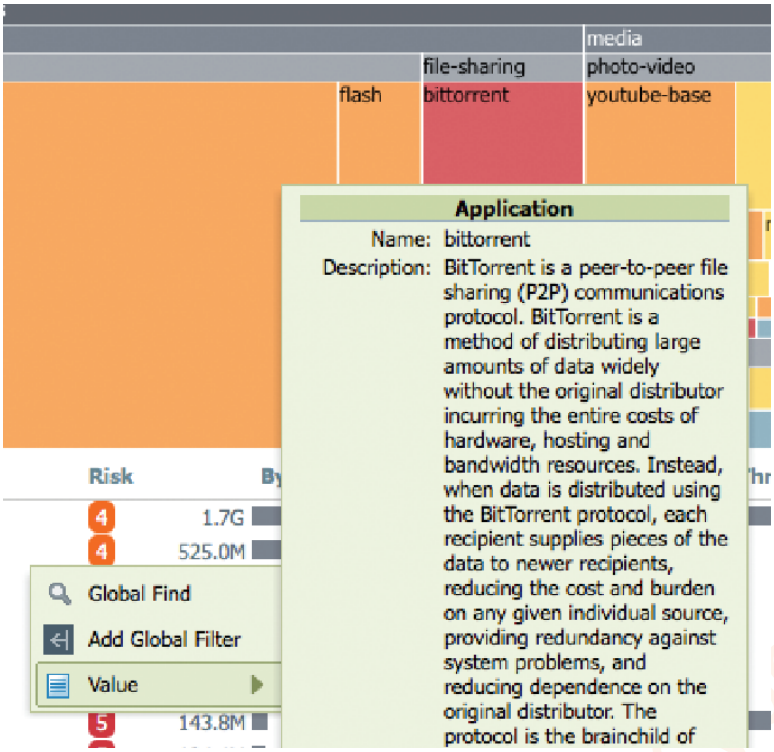


In addition to customizing existing tabs (**Network Activity**, **Threat Activity**, and **Blocked Activity**), administrators can create custom tabs to monitor certain employees, situations, or applications.

With the interactive capabilities of the ACC, you can learn more about applications, URL categories, risk levels, or threats to get a complete picture of network and threat activity (see Figure 2-17).

Figure 2-17

One-click, interactive capabilities provide additional information and the ability to apply any item as a global filter.

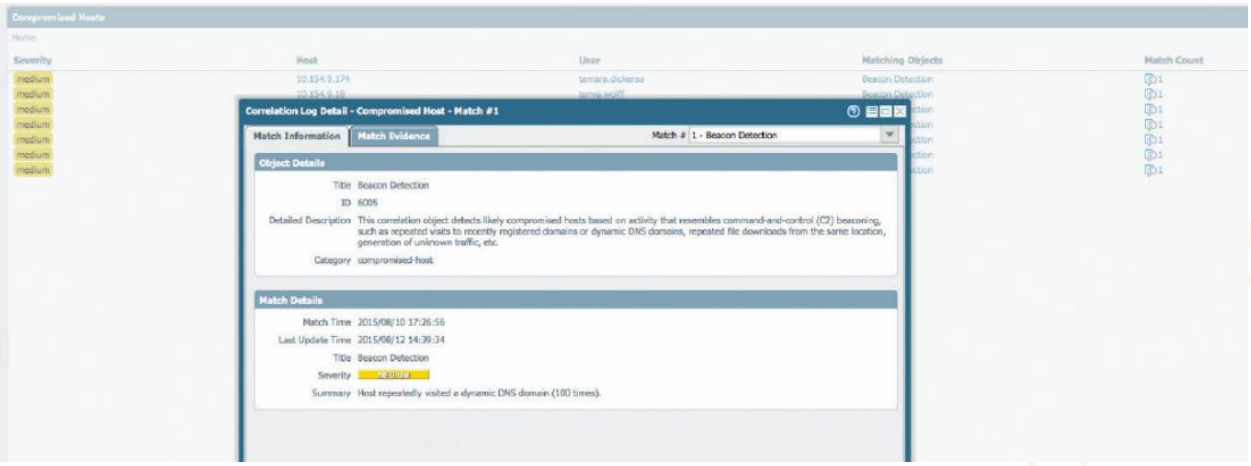


The automated correlation engine in the ACC is an analytics tool that surfaces critical threats that may be hidden in the network. The correlation engine reduces manual data mining and enables faster response times. It scrutinizes isolated events automatically across multiple logs, queries the data for specific patterns, and correlates network events to identify compromised hosts. And it includes correlation objects that are defined by the Palo Alto Networks Malware Research team. These objects identify suspicious traffic patterns, compromised hosts, and other events that indicate a malicious outcome. Some correlation objects can identify dynamic patterns that have been observed from malware samples in WildFire.

Correlation objects trigger correlation events when they match on traffic patterns and network artifacts that indicate a compromised host on your network. In the ACC, correlation triggers are clearly identified and highlighted to enable a fast response (see Figure 2-18).

Figure 2-18

The automated correlation engine automatically highlights compromised hosts in the ACC by correlating indicators of compromise (IoCs).



A log is an automatically generated, timestamped file that provides an audit trail for system events on the firewall or network traffic events that the firewall monitors. Log entries contain *artifacts*, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker. Each log type records information for a separate event type. For example, the firewall generates a Threat log to record traffic that matches a spyware, vulnerability, or virus signature or a DoS attack that matches the thresholds configured for a port scan or host sweep activity on the firewall.

The following logs can be viewed from the **Monitor** tab on Palo Alto Networks next-generation firewalls:

- **Traffic logs.** These logs display an entry for the start and end of each session. Each entry includes the following information: date and time; source and destination zones, addresses, and ports; application name; security rule applied to the traffic flow; rule action (“allow,” “deny,” or “drop”); ingress and egress interface; number of bytes; and session end reason.

- **Threat logs.** These logs display entries when traffic matches one of the Security Profiles attached to a security rule on the firewall. Each entry includes the following information: date and time; type of threat (such as virus or spyware); threat description or URL (**Name** column); source and destination zones, addresses, and ports; application name; alarm action (such as “allow” or “block”); and severity level.

- **URL Filtering logs.** These logs display entries for traffic that matches URL Filtering Profiles attached to security rules. For example, the firewall generates a log if a rule blocks access to specific websites and website categories or if you configured a rule to generate an alert when a user accesses a website.

- **WildFire Submissions logs.** The firewall forwards samples (files and emails links) to the WildFire cloud for analysis based on WildFire Analysis Profiles settings. The firewall generates WildFire Submissions log entries for each sample it forwards after WildFire completes static and dynamic analysis of the sample. WildFire Submissions log entries include the WildFire verdict for the submitted sample.

- **Data Filtering logs.** These logs display entries for the security rules that help prevent sensitive information such as credit card numbers from leaving the area that the firewall protects.

- **Correlation logs.** The firewall logs a correlated event when the patterns and thresholds defined in a correlation object match the traffic patterns on your network.

- **Config logs.** These logs display entries for changes to the firewall configuration. Each entry includes the date and time, the administrator username, the IP address from where the administrator made the change, the type of client (web, CLI, or Panorama), the type of command executed, the command status (succeeded or failed), the configuration path, and the values before and after the change.

- **System logs.** These logs display entries for each system event on the firewall. Each entry includes the date and time, event severity, and event description.

- **HIP Match logs.** The Prisma Access Host Information Profile (HIP) feature enables you to collect information about the security status of the end devices accessing your network (such as whether they have disk encryption enabled). The firewall can allow or deny access to a specific host based on adherence to the HIP-based security rules you define. HIP Match logs display traffic flows that match a HIP Object or HIP Profile that you configured for the rules.

- **Alarms logs.** An alarm is a firewall-generated message that indicates that the number of events of a particular type (for example, encryption and decryption failures) has exceeded the threshold configured for that event type.

- **Unified logs.** Unified logs are entries from the Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs displayed in a single view. The Unified log view enables you to investigate and filter the latest entries from different log types in one place, instead of searching through each log type separately.

The reporting capabilities on the Palo Alto Networks next-generation firewall enable you to monitor your network health, validate your policies, and focus your efforts on maintaining network security. The following report types are available:

- **Predefined reports** allow you to view a summary of the traffic on your network. Predefined reports are available in four categories: Applications, Traffic, Threat, and URL Filtering.
- **User or group activity reports** allow you to schedule or create an on-demand report on the application use and URL activity for a specific user or for a user group. The report includes the URL categories and an estimated browse-time calculation for individual users.
- **Custom reports** can be created and scheduled to show exactly the information you want to see by filtering on conditions and columns to include. You can also include query builders for more specific details in report data.
- **PDF summary reports** aggregate up to 18 predefined or custom reports and graphs from Threat, Application, Trend, Traffic, and URL Filtering categories into one PDF document.
- **Botnet reports** allow you to use behavior-based mechanisms to identify potential botnet-infected hosts in the network.
- **Report groups** combine custom and predefined reports into report groups and compile a single PDF document that is emailed to one or more recipients.

Reports can be generated on demand or on a recurring schedule, and they can be scheduled for email delivery.