

## Simplify Integration and Automation with Management and Security tools using RESTful APIs

Automating with Threat Detection and Anticipation

### Business Goals

- Reduce costs by eliminating multiple tools and tools conflicts
- Improve efficiency by leveraging existing tools and interoperability
- Create easy to use 'single pane of glass' management, monitoring, and visualization interfaces

### cPacket's Benefits

- Rich set of RESTful APIs for interoperability and automation
- Simple to use and easy to extract KPIs via APIs
- Extract and export KPIs to CSV, and combine with other tools to build high level actionable insights
- Integrated with Cisco Firepower; the combined value is greater than the sum of the individual value propositions

Most medium to large corporations use a variety of tools to achieve their network monitoring, management and troubleshooting objectives. Having multiple tools while attempting to solve current problems can also create new issues. A common goal facing corporations today is the ability to use multiple tools to build a single unified interface for cost effective visualization, information extraction, and management.

As IT complexity increases, so does the need to combine information from multiple monitoring tools to create higher level actionable insights. This becomes an urgent requirement as networks evolve to leverage SDN/NFV and 'intent based networking' paradigms. The integration of cPacket's network visibility solution and Cisco's Firepower security solution provides companies with valuable data and full visibility into network level insights for faster threat detection and an improved ROI.

## Application of REST

The web interface, and its underlying technology REST, have become de-facto standards for management, monitoring and visualization. RESTful APIs, due to use of standard protocols such as HTTP and statelessness, have become a popular choice for network operators to utilize when integrating and extracting information from multiple products.

cPacket has a rich set of RESTful APIs to access the various network KPIs, data sources and provisioning interfaces throughout the system. cClear, the central management and visualization device, provides a rich set of APIs that can be used for integration and data extraction.

The integration of cPacket's network performance monitoring (NPM) solution and Cisco Firepower is a good example of the REST API integration. Figure 1 shows the network topology of the integration use case. cVu network probes (1G-100G speed per port, up to 32 ports per device) and cStor (packet capture, storage and analysis) devices are deployed at critical monitoring points in the network and managed by a cClear device that collects, correlates and visualizes KPIs. The Sourcefire deployment has security sensors (Next Generation Intrusion Prevention System, NGIPS for short) deployed at critical points in the network and managed by the Firepower Management Console (FMC). When a security event is detected by the NGIPS, an alert is sent to the FMC. FMC provides the 'point' information about the event such as the type/priority of the event, timestamp when the event occurred, and the standard 5-tuple. However, to obtain detailed information for forensic analysis, the integration of cPacket's solution and the FMC can provide network behavior information and packet captures.

Once the integration is complete and if any security event occurs, it is flagged on the FMC. The FMC will show details of the event (seen in the blue box in Figure 2) as well as three additional options, as shown in the red box. The user can click on any of these three choices to obtain any necessary information needed for forensic analysis or for legal action. Clicking on these three links results in calling the corresponding REST API.

For example, when the user clicks the link that says 'Download PCAP', FMC will make a REST API call to cClear to obtain the raw packets. cClear will make REST API calls to the right set of cVus and cStors, and downloads the PCAPs in the context of this event.

By clicking on the link '*Search whether this offending IP combination is still in the network*', SecOps can cross-launch to cClear's cSearch window and automatically execute a REST API that performs a 'Google-like' search of the entire network. By using this search capability, SecOps can determine whether the bad actors are still lurking around in the network.

Furthermore, by clicking on the '*Cross-launch cClear to see other events in the window*', SecOps engineers can cross-launch to the cClear's dashboards to access the various packet, session, flow KPIs, and baseline information to understand the state of the network at the time of the event. Figure 2 below shows all three ways to interact with cPacket's cClear directly from the Firepower's FMC.

Because many security attacks have tell-tale signs of anomalous network behavior, by using these three options, NetOps and SecOps can potentially craft thresholds/alerts for certain types of traffic, protocols, and applications relevant to their environment and create early warning systems.

In summary, by using RESTful APIs and integrating cPacket's solution with Cisco Firepower, users benefit from the combined power of two related areas: network performance monitoring (NPM) and network security.

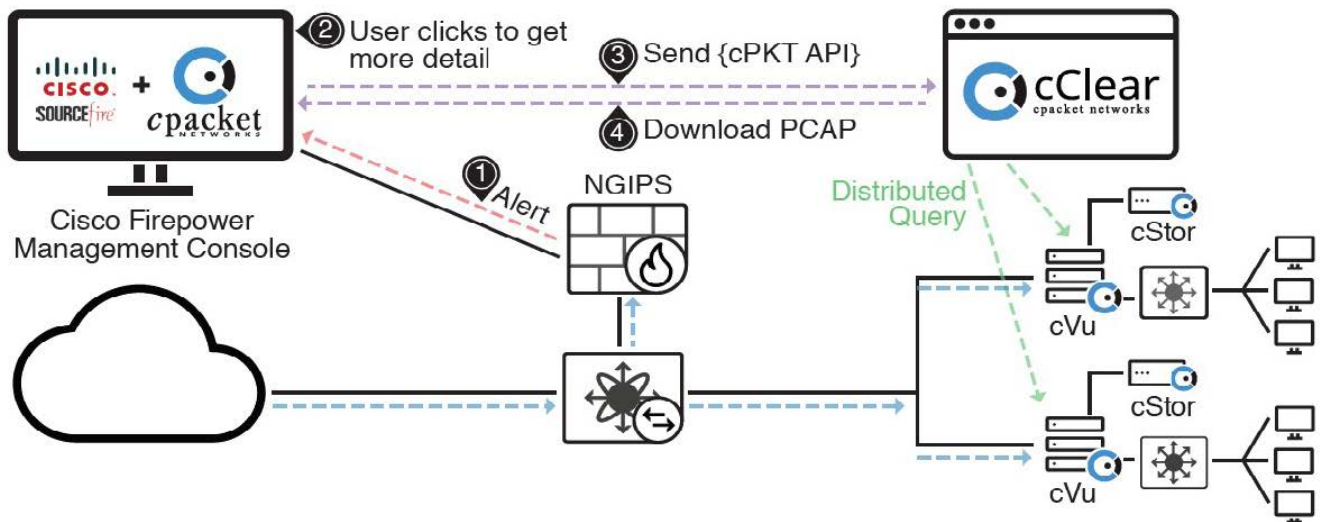
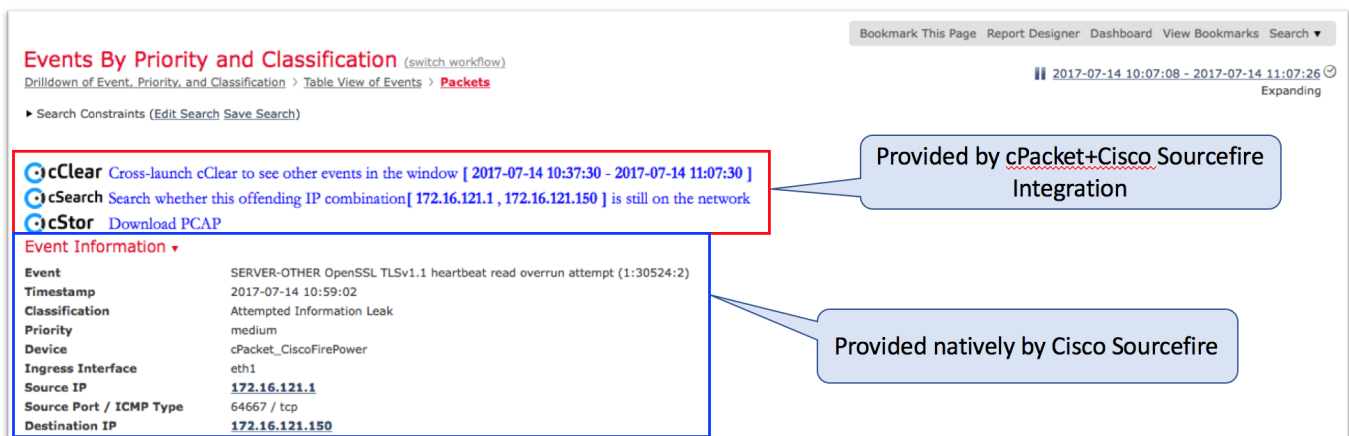


Figure 1: Integration of cPacket's NPM solution with Cisco Firepower using RESTful APIs



The screenshot shows the 'Events By Priority and Classification' page in the Cisco Firepower Management Console. The page displays a list of events, with one event highlighted in a red box. The event details are shown in a table below the list. Two callouts are present: one pointing to the event list and another pointing to the event details table.

| Event Information       |   |
|-------------------------|---|
| Event                   | SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt (1:30524:2) |
| Timestamp               | 2017-07-14 10:59:02   |
| Classification          | Attempted Information Leak  |
| Priority                | medium  |
| Device                  | cPacket_CiscoFirePower  |
| Ingress Interface       | eth1  |
| Source IP               | <b>172.16.121.1</b>   |
| Source Port / ICMP Type | 64667 / tcp   |
| Destination IP          | <b>172.16.121.150</b>   |

Figure 2: Result of the integration: cPacket's NPM augments Cisco Firepower's security analysis

## Benefits

cPacket's rich set of REST APIs provides users the flexibility to integrate with their favorite tools and create a single unified interface to interact with these tools. The API set allows access to valuable network performance data which can be seen in the cClear dashboard. This data can be exported to other time series databases, or data lakes, and be combined with other metrics from other devices. Additionally, this data can also be exported from other data sources to create high level insights and actions, resulting in more efficient network operations, reduced MTTR, and greater uptime.

## Unlock the Advantages with cPacket

cPacket's solutions offer unprecedented performance, deeper levels of insight, and real-time analytics to solve the most complex network challenges faced in today's enterprises. cPacket's advanced distributed intelligence enables network operators to proactively detect problems before they negatively impact end-users using predictive analytics. cPacket provides a unique algorithmic chip that delivers complete packet inspection immediately at the wire for accurate results.

cPacket Networks is committed to achieving quality standards in network performance monitoring and is trusted by network operators worldwide.

## Contact Us

To learn more about our products and solutions, please visit [www.cpacket.com](http://www.cpacket.com)