Use Case: Use cSearch to globally search the network

Verify network configuration changes

Business Goals

- Minimize mean time to resolution
- Reduce overall expenses using a network-wide search
- Improve efficiency of network configuration changes
- Create easy to use ‘single pane of glass’ management, monitoring and visualization interfaces

cPacket’s Benefits

- Network-wide Google-like search under all traffic conditions
- Search every byte in every packet or flow in real-time
- Test and verify network configuration changes in seconds
- Accessible from external devices using RESTful APIs

Network monitoring and troubleshooting are two essential tasks for NetOps and SecOps operating in medium and large-scale networks. The ability to have a complete and comprehensive view of the network is critical.

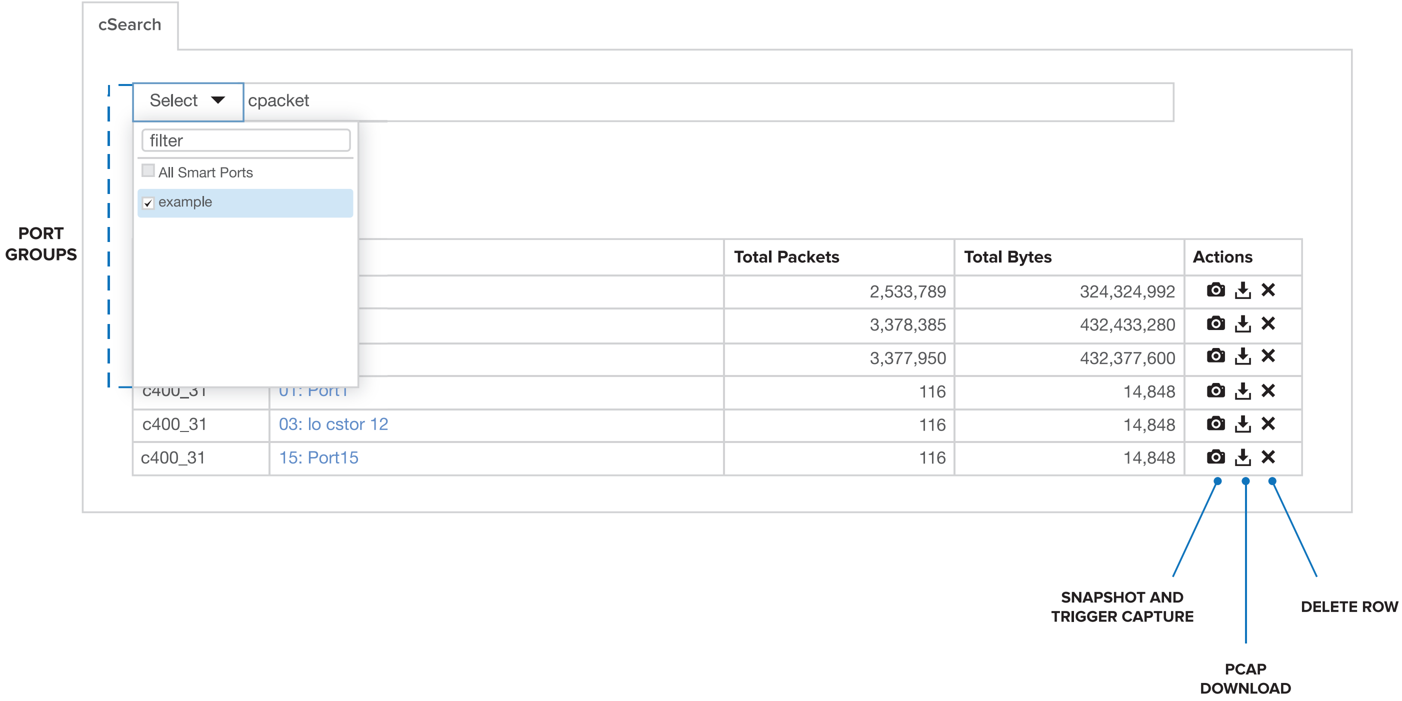
cPacket’s cSearch is a powerful tool that can be used to search the network for specific patterns as well as testing and verifying network level configuration changes. cSearch can identify an entire packet (payload and header), a specific portion of a packet at a specific offset, and/or a specific protocol/header value anywhere in the network. This pervasive search feature can be used to test and verify switch, router, and firewall configurations. Because cSearch is implemented in the hardware in the cPacket’s proprietary ASIC, it can deliver accurate search results regardless of link speed (1G to 100G), utilization or packet size mix.

In today’s challenging network environments, the need for reliability and accuracy is essential for organizations looking to improve efficiency while minimizing costs. Powered by cPacket’s patented algorithmic chip and cutting-edge technology, small to large sized companies around the world are using cSearch to optimize network performance and improve ROI.

What is cSearch?

cSearch is a Google-like search feature for the network. It is one of the most popular features among cPacket's customers who leverage its simplicity and comprehensive search capabilities to instantly run queries against the network to get the answers they need.

cSearch provides network engineers and operators the ability to search for any combination of header and payload patterns across the network, identify the segments with traffic patterns matching those profiles, and retrieve matching packets instantly. Essentially, the search pattern is free form text. Its scope can be the entire packet (payload and header), or a specific portion of a packet (specific offset in the packet), or specific protocol/header values. Using a simple search form, a query can be entered that will execute concurrently across all desired smart ports. The result is a sorted list of links on which the traffic profile exists, including the packet and byte counts matching the search pattern. Searches can be refreshed or saved as persistent searches for continuous monitoring. Packet captures can be triggered on any row of the search result by clicking on the 'camera' icon. Seen in Figure 1 below, raw packets (PCAPs) can be directly accessed by clicking on the download icon and analyzed in Wireshark.



		Total Packets	Total Bytes	Actions
		2,533,789	324,324,992	📷 ⤓ ✕
		3,378,385	432,433,280	📷 ⤓ ✕
		3,377,950	432,377,600	📷 ⤓ ✕
c400_31	01: Port1	116	14,848	📷 ⤓ ✕
c400_31	03: lo cstor 12	116	14,848	📷 ⤓ ✕
c400_31	15: Port15	116	14,848	📷 ⤓ ✕

Figure 1: cSearch page

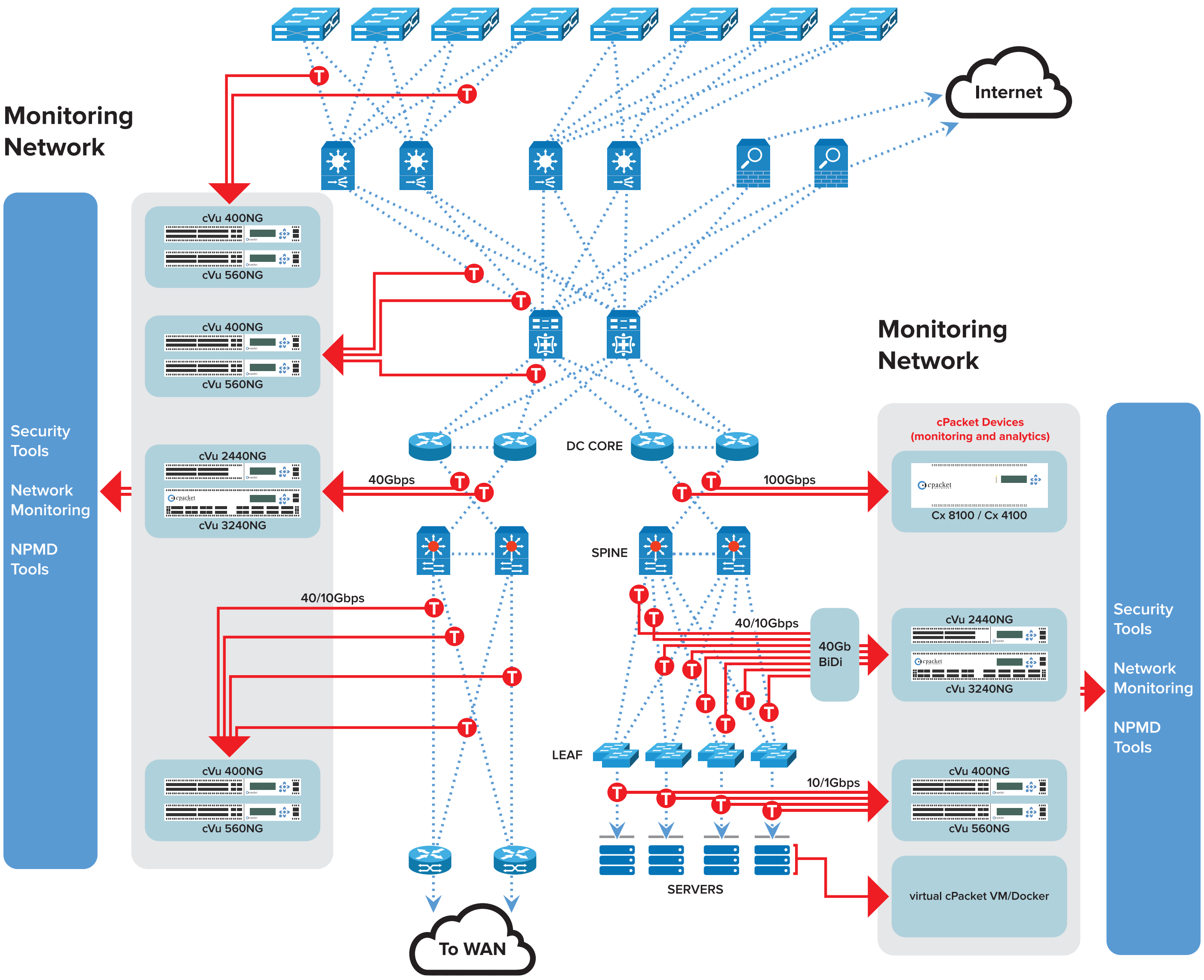


Figure 2: Monitoring network and Production network

Figure 2 shows the two different networks that exist in an organization. The production network runs the business. It consists of routers, switches, firewalls etc., that are actively moving packets in and out of the network. Production network feeds a monitoring network via SPANs and TAPs to packet brokers, which feeds the network traffic to specialty tools for monitoring and security. The purpose of a monitoring network is to observe the production network for performance, SLA, security and troubleshoot issues in the production network.

Figure 2 also shows a monitoring network topology deployed with cPacket's solution. It consists of cVu network sensors (1G-100G speed per port) and cStor devices (packet capture, storage and analysis) that are deployed at critical monitoring points in the network. They are managed by a cClear device that collects, correlates and visualizes KPIs. As seen in Figure 2 above, cPacket's solution plays a critical role in the network; it sees all the traffic that enters the monitoring network. cSearch can provide vital information about the production network. The following points describe several use cases for cSearch's feature, and how they can benefit SecOps and NetOps.

1. Determine whether packets with specific content are present anywhere in the network

Enter the pattern to be searched and click on the ‘search’ button. The result will include all links on the network matching the search criteria (see Figure 1 above).

2. Discover whether packets with specific content is present in a specific segment in the network

By selecting the port groups from the drop-down menu, the user can choose to narrow the search to a specific set of network segments.

3. Accurately determine the extent of propagation for a specific packet (i.e. the possibility of a worm or virus)

The goal of this search is to conclusively prove (or disprove) the existence of a specific packet (i.e. a packet containing a specific IP address, or a specific pattern in the payload) in a part of the network. This helps SecOps understand the extent of propagation (the spread of infection) in the network and proactively mitigate the issue(s).

4. Pinpoint where certain packets have NOT spread

Opposite of point #3 above, the links that do not show in the search results are the ones where the infection has not yet spread.

5. Identify packet flows and the paths they take in the network in real-time

Any of the above use cases can be configured to run once, or to be run endlessly. When the search run is perpetual, results will be periodically refreshed with new values of packet and byte counts. Furthermore, new rows of search results can appear. This feature can help identify network paths that specific packets take in real time.

6. Identify and watch the spread of infection

Using the infinite search feature, SecOps can visualize the ‘spread of the infection’ in real-time as new rows get added to the search results. This helps to quickly identify network segments that will be ‘infected’ and take any corrective action if necessary.

7. Test and verify network configuration changes

cSearch running in an infinite search loop can be employed to test and verify network configuration changes. Any changes to ACLs, time-based ACLs, firewall filters, flow rules, VRFs, routes and other router/switch configurations can be tested on the production network.

a) NetOps/SecOps can place cVu sensors at specific points in the network where the network configuration change will cause certain types of traffic to enter that part of the network. Optionally, by using a traffic generator, packets with a known signature can be injected into the production network.

b) Enter the search pattern that identifies the specific traffic and run the search in an endless loop.

c) Execute the network configuration change.

d) If the configuration change is correct, search results will include the cVu sensors placed in step a.).

e) By performing the steps above, many router, switch, and firewall configurations can be tested and verified.

The cSearch functionality can also be accessed from other devices via RESTful APIs. This has been leveraged in cPacket's integration with Cisco Sourcefire. When SecOps click the link '*Search whether this offending IP combination is still in the network*', the Sourcefire's FMC cross-launches the cClear's cSearch window. A time-stamp of that event and the 5-Tuple (source IP, source port, destination IP, destination port, protocol) as search parameters are automatically sent and the REST API is executed to search the entire network. The search results will notify the user whether the offending source IP-destination IP pair is attempting to compromise the network. The information received will enable SecOps to take immediate action, and deny access or redirect that traffic to a honey-pot for research and legal purposes.

Benefits

cPacket's cSearch is a powerful tool that optimizes the need for running similar searches on multiple downstream tools in a monitoring network. Because of cPacket's key position in the network, it can provide comprehensive network information and complete network-wide results to search queries. SecOps and NetOps can utilize these search results to make informed and accurate decisions. Furthermore, they can verify network configurations to improve network operations, reducing MTTR, and improve overall business objectives.

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.