cPacket

SOLUTION BRIEF

Distributed Denial of Service (DDoS):

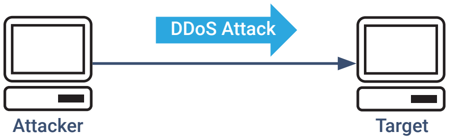
Deploying a Network Observability Service for Detection and Monitoring of Denial-of-Service Attacks

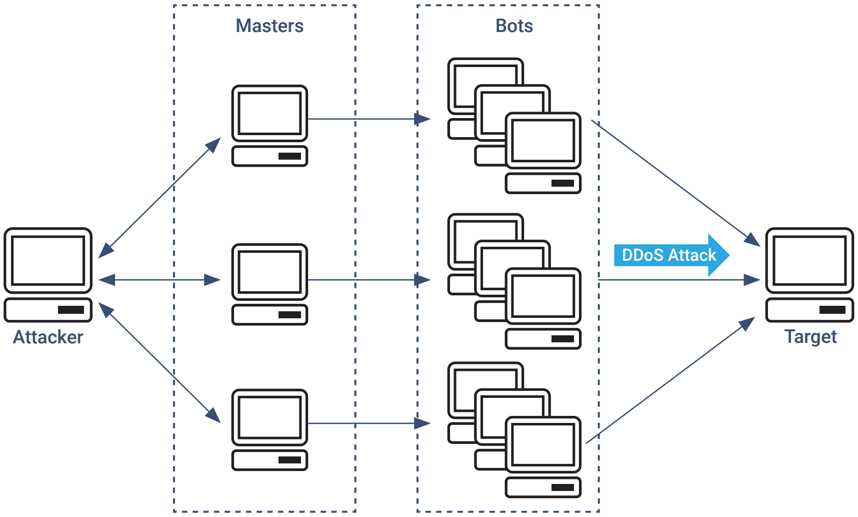
Today's complex hybrid infrastructure demands complete network observability enabled by packet capture, storage and analytics to support zero down time enterprises.

Online networks are under constant threat from malicious Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Accurately identifying the vector and type of DDoS attacks is crucial for security and network operations teams to take effective action, reduce network downtime, and provide valuable insights, accountability, and actionable steps. This is especially critical for large-scale, interconnected network systems and infrastructure.

Problem Statement

A Denial of Service (DoS) attack is a deliberate attempt to make your service unavailable to users, such as by flooding it with network traffic. To achieve this, attackers use a variety of techniques that consume large amounts of network bandwidth or tie up other system resources, disrupting access for legitimate users. In its simplest form, a lone attacker uses a single source to execute a DoS attack against a target, as shown in the next figure.





In a Distributed Denial of Service (DDoS) attack, an attacker uses multiple sources, (such as distributed groups of malware infected computers) to orchestrate an attack against a target. As illustrated in the following figure, a network of compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the target.

DDoS attacks are most common at layers 3, 4, 6, and 7 of the Open Systems Interconnection (OSI) model, which is described in the following table.

#	Layer	Unit	Description	Vector Examples
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	TLS abuse
5	Session	Data	Interhost communication	N/A
4	Transport	Segments	End-to-end connections and reliability	SYN floods, Malformed TCP flags
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	Data Link	Frames	Physical addressing	N/A
1	Physical	Bits	Media, signal, and binary transmission	N/A

Layer 3 and 4 attacks correspond to the Network and Transport layers of the OSI model. These layers are referred to collectively as infrastructure layer attacks.

It's worth noting that every public advertised IP today is under continuous "scanning" from malicious IPs. Attackers are continuously looking for vulnerabilities and continuously map webservers and/or probe for open ports and/or for unpatched applications. This phenomenon causes a continuous "noise" where public IPs see SYN packets without a corresponding SYNACK, and/or failed TLS handshakes.

That means that a DDoS detection mechanism needs to have the ability to distinguish between the baseline malicious activity and a DDoS in-progress; this detection is typically based on the quantity of the traffic involved.

Types of Attack

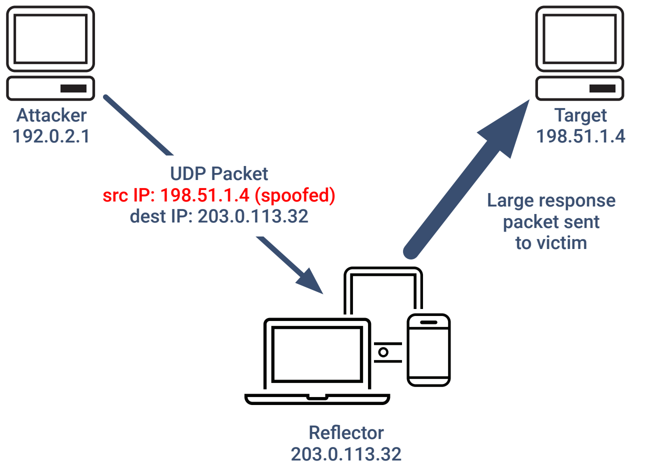
There are multiple DDoS attack types, each targets a different service or connectivity within the application service environment; each one works by utilizing existing services that are used for connectivity, management or operational service provision and generally these attacks intend to either overload network capacity or to over-extend server resources. Generally, these utilize 3rd party application services and servers; and either trick them into sending unsolicited data to the Target, or by initiating multiple concurrent sessions and not completing handshakes, or by purposefully failing these negotiated sessions resulting in increased resource usage on the servers. These DDoS attacks take the form of the following types.

UDP Reflection Attacks

UDP reflection attacks exploit the fact that UDP is a stateless protocol. Attackers can craft a valid UDP request packet listing the attack target's IP as the UDP source IP address. The attacker has now falsified (spoofed) the UDP request packet's source IP. An attacker then sends the UDP packet containing the spoofed source IP to an intermediate server. The server is tricked into sending its UDP response packets to the targeted victims IP rather than back to the attacker's IP address. The intermediate server is used because it generates a response that is several times larger than the request packet, effectively amplifying the amount of attack traffic sent to the target IP address. The amplification factor, which is the ratio of response size to request size, varies depending on which protocol the attacker uses: DNS, NTP, or SSDP.

For example, the amplification factor for DNS can be 28 to 54 times the original number of bytes.

So, if an attacker sends a request payload of 64 bytes to a DNS server, they can generate over 3400 bytes of unwanted traffic to an attack target. The diagram and table below illustrate the reflection tactic and amplification effect depending on the service type used for the amplification.



Protocol	Bandwidth Amplification Factor
Memcached	50000 (fixed in version 1.5.6)
NTP	556.9 (fixed in version 4.2.7p26)
CharGen	358.8
DNS	Up to 179
QOTD	140.3
Quake Network Protocol	63.9 (fixed in version 71)
BitTorrent	4.0 - 54.3 (fixed in libuTP since 2015)
CoAP	10 - 50
ARMS	33.5
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

SYN Flood Attacks

When a user connects to a TCP service, (like a web server) their client sends a SYN (synchronization) packet. The server returns a SYN-ACK packet in acknowledgement and finally the client responds with an ACK packet, which completes the expected three-way handshake. This typical handshake is a normally expected negotiation, expected by all TCP services.

In a SYN flood attack a malicious client sends a large number of SYN packets, but never sends the final ACK packets to complete the handshakes. The server is left waiting for a response to the half-open TCP connections and eventually runs out of capacity to accept new TCP connections. This can prevent new users from connecting to the server. SYN floods can reach up to hundreds of Gbps, but the attack is not about SYN traffic volume, but rather tying up available server connections resulting in no resources for legitimate connections.

TCP Middlebox Reflection

A relatively new attack vector was first disclosed in an academic whitepaper in August 2021, which explained how TCP non-compliance in both nation-state and commercially available firewalls, could result in these being tricked into becoming a TCP amplification vector. The amplification factor varies due to the different ways in which vendors have implemented this “feature”, but it can exceed Memcached UDP amplification, see table above.

Application Layer Attack

An attacker may target the application itself by using a layer 7 or application layer attack. In these attacks, like SYN flood infrastructure attacks, the attacker attempts to overload specific functions of an application to make the application unavailable or extremely unresponsive to legitimate users. Sometimes this can be achieved with very low request volumes that generate only a small volume of network traffic. This can make the attack difficult to detect and mitigate if the Network Operations team is only monitoring Network Bandwidth/Traffic. Examples of application layer attacks include HTTP floods, cache-busting attacks, and WordPress XML-RPC floods.

In an HTTP flood attack, an attacker sends HTTP requests that appear to be from a real user of the web application. Some HTTP floods target a specific resource, while more complex HTTP floods attempt to emulate human interaction with the application. This can increase the difficulty of using common mitigation techniques like request rate limiting.

Application layer attacks can also target domain name system (DNS) services. The most common of these attacks is a DNS query flood, in which an attacker uses many well-formed DNS queries to exhaust the resources of a DNS server. These attacks can also include a cache-busting component where the attacker randomizes the subdomain string to bypass the local DNS cache of any given resolver. As a result, the resolver can’t take advantage of cached domain queries and must instead repeatedly contact the authoritative DNS server, which amplifies the attack.

If a web application is delivered over TLS, an attacker can also choose to attack the TLS negotiation process. TLS is computationally expensive so an attacker can reduce a server’s availability by sending unintelligible data. In a variation of this attack, an attacker completes the TLS handshake but perpetually renegotiates the encryption method. Or an attacker can attempt to exhaust server resources by opening and closing many TLS sessions.

Each of these DDoS attacks use varying methods to overwhelm the local network services, resulting in troubleshooting problems for the Network Operations teams. Having the ability to view the network traffic and an overview of the utilized bandwidth is not sufficient to identify DDoS attacks, then mitigate and block these in real-time.

Feature Map

Distributed Denial of Service (DDoS) attacks pose a significant threat to infrastructure layers. Common mitigation strategies include overprovisioning capacity, deploying DDoS mitigation systems, or scrubbing traffic with specialized services. However, these techniques can be costly and may impact service latency. To balance these factors, many enterprises adopt a combined approach: detecting DDoS attacks and leveraging on-demand mitigation services as needed.

Effective detection and remediation require a robust network observation system with capabilities such as packet brokering, packet capture, and analytics. For comprehensive monitoring, traffic should be captured at full line rate both before and after firewalls or routers. Additionally, specific packet broker features are essential for accurate auditing, analytics, and source identification. Without these capabilities, effective detection, monitoring, and mitigation are challenging, and root cause analysis becomes nearly impossible.

The ability to capture and analyze traffic at full line rate while inspecting every packet and counting all packet types is crucial for mitigating DDoS attacks. By implementing these measures, organizations can better protect their infrastructure and minimize the impact of DDoS threats.

Feature	Description
SYN Counter	To count and monitor individual client connection requests to the server, enabling the identification of the total number of requests per client to each server and the detection of any imbalances between client requests and client acknowledgments.
SYNACK Counter	To count and monitor each server's response to a client connection request and track client acknowledgments. When used in combination with a SYN counter, the system can detect if a DDoS SYN attack is in progress.
DNS Request Counters	This counter monitors the volume of DNS requests sent by the network to the DNS server. By tracking the ratio of requests to responses, it can help detect signs of a DNS DDoS attack.
DNS Response Counters	This counter monitors responses from DNS servers to identify any discrepancies between the number of requests and responses, which could indicate a potential DNS DDoS attack, particularly those involving DNS UDP type reflection attacks.
TLS Client Hello Counter	The TLS Client Hello counter tracks and monitors transactions and connection requests at the application and TLS levels. This helps detect if a client is exploiting TLS renegotiation to launch DDoS attacks.
TLS Server Hello Counter	The TLS Server Hello Counter works in conjunction with the TLS Client Hello Counter to measure the frequency of client requests for encryption method updates, which can impact server performance.

cPacket Unique Proposition

cPacket's solution offers real-time, line-rate monitoring of every packet and byte, enabling rapid detection of DDoS attacks and accurate identification of potential attackers. This is achieved through low-latency alerts and a detection mechanism based on the following principles:

Packet Type Imbalance:

DDoS attacks often exhibit abnormal ratios of different packet types. For example, SYN flood attacks have a disproportionately high ratio of SYN packets to SYNACKs, while DNS amplification attacks have a high ratio of DNS requests to DNS responses.

Unexpected Packet Types:

DDoS attacks can be identified by the presence of IP fragments or illegal TCP flag combinations. These packets, when received from external sources on publicly advertised IPs, are strong indicators of an attack.

Null-Payload Sessions:

Layer 4 to 6 attacks often involve TCP sessions that are established, sometimes even with TLS handshakes, but ultimately fail to exchange any meaningful data. A large number of such sessions without data transfer is a key indicator of a DDoS attack in progress.

cPacket's Specific Features and Capabilities

To effectively detect and mitigate various DDoS attack types, cPacket's solution incorporates the following features:

- High-speed packet capture and analysis: Ensures real-time monitoring of network traffic for rapid detection of anomalous activity.
- Deep packet inspection: Provides detailed analysis of packet content, including headers, payloads, and protocol-specific information.
- Advanced anomaly detection algorithms: Leverages machine learning and statistical techniques to identify unusual patterns indicative of DDoS attacks.
- Real-time alerts and notifications: Provides immediate alerts to enable timely response and mitigation efforts.
- Integration with security tools: Seamlessly integrates with other security solutions for comprehensive threat management.
- Scalability: Can handle high-volume network traffic and adapt to changing network conditions.

By combining these features, cPacket's solution offers a powerful and effective approach to detecting and mitigating DDoS attacks, protecting networks and critical infrastructure from service disruption.

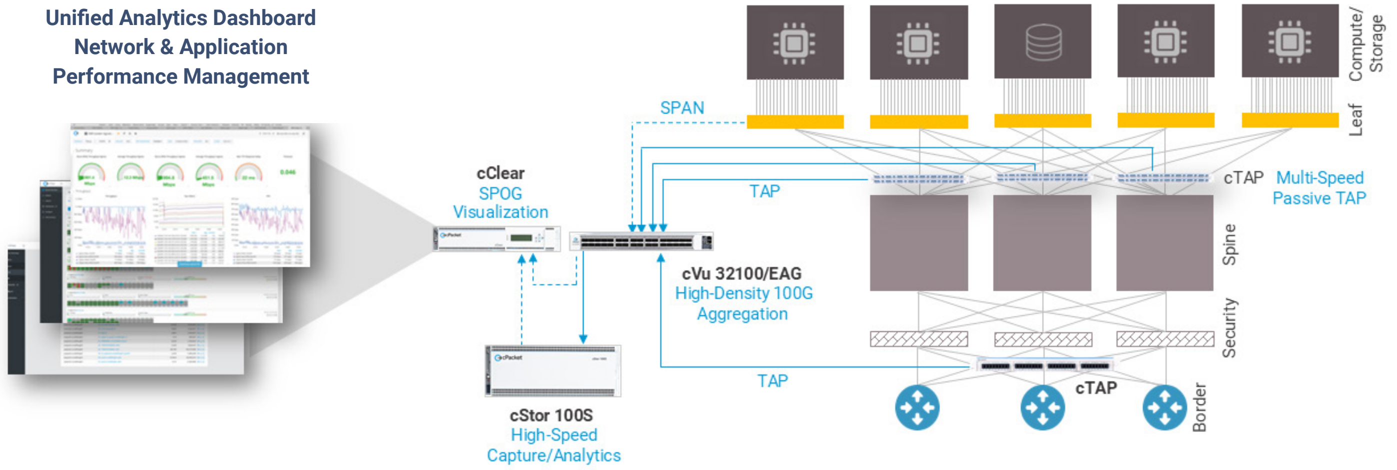
The table below lists cPacket's table of features and capabilities for DDoS Attack detection and mitigation.

Feature	Description
cBurst	This feature detects and monitors network traffic for small packet sizes and unusually high volumes of requests entering the network. These characteristics can be indicative of a DDoS attack vector. With dedicated hardware per port, it offers a reporting granularity of 1 millisecond, providing real-time insights into potential threats.
Timestamp	With 1 nanosecond timestamp accuracy, this feature enables the precise capture and analysis of large volumes of requests and all incoming packets. This high-resolution timestamping is also crucial for identifying and replaying traffic for in-depth post-analysis.
Dashboards	Standard dashboards are available for visualizing DDoS metrics and counters. These dashboards provide insights into various attack vectors and monitoring points, facilitating reporting, compliance, and auditing based on specific counter data and port information.
Alerts	Built-in standard dashboards are available for monitoring DDoS counters and generating alerts based on predefined thresholds. Additionally, a system-wide DDoS alert mechanism is in place to notify and alert administrators when threshold triggers are reached for each specific attack vector.
SYN Counter	A built-in counter is available to monitor SYN requests from clients to the server and trigger alarms when abnormal levels are detected. Additionally, the counter tracks source and destination IP and MAC addresses for logging and auditing purposes.
SYNACK Counter	Built-in counters monitor SYNACK responses from the server to the client and trigger alarms when abnormal patterns are detected. By analyzing the difference between SYN and SYNACK packets, the system can identify if a SYN flood attack is in progress or has occurred.
DNS Request Counters	A built-in counter is used to detect if DNS responses are being spoofed or sent without corresponding DNS requests. Additionally, the counter tracks source and destination IP and MAC addresses for logging and auditing purposes.
DNS Response Counters	Built-in counters are used to detect if DNS responses are being sent without corresponding requests, indicating that a UDP spoofed DDoS attack using DNS is in progress.
TLS Client Hello Counter	A built-in counter is used to monitor and correlate TLS requests from clients to the server or service to detect TLS handshake attacks. Additionally, the counter tracks source and destination IP and MAC addresses for logging and auditing purposes.
TLS Server Hello Counter	A built-in counter is used to monitor and correlate TLS responses from the server or service to detect TLS handshake attacks. These values are utilized by the DDoS alert system and dashboard for detection, reporting, and analysis.
Fragmentation Detection	A smart filter is capable of detecting if payloads are fragmented without a valid reason, which is often a byproduct of amplification attacks. Identifying high levels of IP fragments can be a strong indicator of DDoS activity.

All listed features are included by default and are fully supported on the cPacket Packet Broker, Packet Capture & Analytics platforms.

Deployment Architecture

To effectively deploy and monitor for DDoS attacks, the Packet Broker should be installed using a network tap between the internet/border router and the firewall. This tap should be placed on both ingress and egress interfaces to ensure both requests and responses can be monitored and counted for comprehensive oversight. The choice of Packet Broker is flexible, with both the cVu-AG and cVu-NG series being suitable options. The cVu-NG offers additional performance and edge-based measurement capabilities.



Solution Configuration

Prerequisites:

- A network tap or test access port (TAP) installed between the internet/border router and the firewall on both ingress and egress interfaces.
- A cPacket cVu-NG appliance and a cStor storage appliance.
- A cPacket cClear Appliance or Virtual machine.

Steps:

1. Physical Installation:

- Physically connect the cVu-NG, cStor and cClear appliances to the management network.
- Connect the TAP to the cVu-NG's capture ports.
- Connect the cVu-NG Aggregation port to the cStor Data Port/Ports.

2. Network Configuration:

- Configure the cVu-NG's network interface and assign an IP address.
- Assign IP addresses to the cVu-NG and cStor appliances.

3. cVu-NG Configuration:

- Configure the cVu-NG to capture traffic from the TAP ports.
- Define capture filters to focus on specific traffic types, such as SYN, ACK, DNS, or TCP packets.
- Configure the Aggregation port to connect traffic to the cStor.

4. cStor Configuration:

- Configure cStor as a storage backend for the cVu-NG.
- Set up storage policies and quotas to manage data retention and storage usage.

5. DDoS Detection Rules:

- Create rules within cClear to define criteria for identifying DDoS attacks. These rules can be based on factors such as:
  - Packet type imbalances (e.g., SYN/ACK ratios)
  - Unexpected packet types (e.g., IP fragments, illegal TCP flags)
  - Null-payload sessions
  - Traffic volume spikes
  - Source IP address analysis

6. Alerting and Notifications:

- Configure cClear to generate alerts when DDoS attacks are detected.
- Set up notification channels (e.g., email, SMS, SNMP) to alert administrators.
- Define alert thresholds and severity levels.

7. Testing and Validation:

- Conduct tests to verify that the solution can accurately detect and report DDoS attacks.
- Simulate various attack scenarios to assess the system's response time and accuracy.

8. Monitoring and Maintenance:

- Regularly monitor the deployment for performance, data integrity, and alert accuracy.
- Perform maintenance tasks such as software updates, backups, and troubleshooting.

Additional Considerations:

- Performance Optimization: Adjust capture filters and storage settings to optimize performance and minimize storage usage.
- Scalability: Ensure the cVu-NG and cStor appliances have sufficient capacity to handle the expected traffic volume.
- Security: Implement appropriate security measures to protect the solution and sensitive data.
- Integration with Other Tools: Consider integrating with other security tools, such as SIEMs or firewalls, for a comprehensive security posture.

By following these steps and considering the additional factors, organizations can effectively deploy cPacket cVu-NG and cStor with cClear to monitor for DDoS attacks and protect their networks from threats.

Solutions BOM

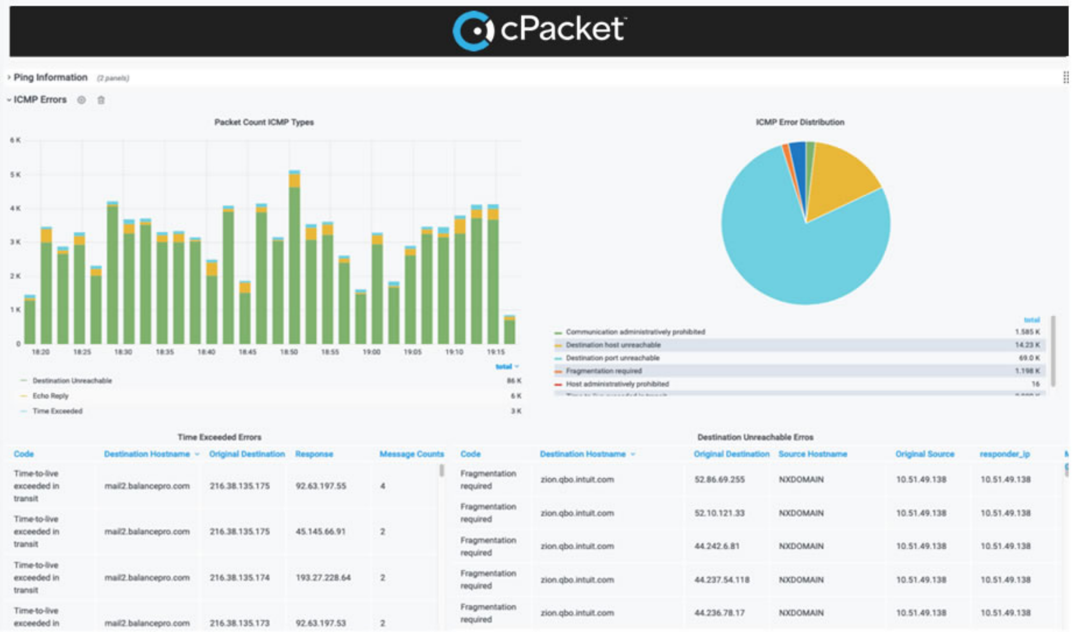
Example BoM for the building and operation of a DDoS solution with alarm generation and dashboard visualization at full line speed and 1mS resolution.

Platform	Description
cTap: Network Test Access Points	cPacket's cTAP passive network test access points (TAPs) provide a non-intrusive solution for monitoring network traffic at high speeds and densities. These TAPs are designed for enterprise networks operating at data rates ranging from 100 Mbps to 100 Gbps. By passively capturing network packets in data centres and other physical networks, cTAPs enable comprehensive monitoring without disrupting network performance or introducing security vulnerabilities. Available in both fixed and modular chassis, cTAPs can be tailored to meet current needs and scaled to accommodate future growth. Additionally, regeneration fiber TAPs are offered for tapping fiber optic networks, mitigating power reduction caused by splitting the optical signal.
cVu: Packet Broker	cPacket's cVu packet brokers are distinguished by their ability to perform advanced packet processing at line speed, utilizing dedicated hardware based on proprietary ASICs and FPGAs behind each port. Unlike competitors who charge extra for advanced features, cPacket offers a simple licensing model that unlocks all capabilities, resulting in a lower total cost of ownership (TCO) for observability and security solutions. By offloading pre-processing tasks to the packet broker, available security tool capacity can increase by up to 30%. cVu packet brokers are trusted by highly demanding environments in sectors such as financial services, healthcare, and high-performance computing.
cStor: Packet Capture and Analysis	Every business needs to understand how their network is performing. cStor is a valuable tool for troubleshooting application, server, and network problems. Organizations across all major industries rely on cStor, including financial institutions, market exchanges, hospitals and healthcare, government, manufacturing, retail, communications, education, and high-performance computing. Each industry has mission-critical applications that demand zero-downtime operation and compliance with regulations. Financial services companies, for example, rely on electronic trading systems where each transaction is critical. Healthcare providers depend on their electronic health records (EHR) systems to be up and running at all times, and must be able to transmit large X-ray images without delay. Hospitals are increasingly deploying thousands of cameras to improve responsiveness. All of these applications require high-performance, reliable networks with zero downtime.
cClear: Analytics Engine	cPacket cClear offers customizable dashboards that provide rich visualizations of network data, allowing for interactive exploration of traffic details and key performance indicators (KPIs). These dashboards leverage real-time and historical data from cPacket cVu packet data brokers and cStor packet capture and analytics observability nodes. By using cPacket cClear, IT teams can gain valuable insights into network behavior, troubleshoot issues effectively, enhance security, deliver exceptional end-user experiences, and meet compliance reporting requirements across multi-cloud and hybrid cloud environments. Users can view detailed network metrics, search network data in real-time, and utilize baselining techniques to proactively identify security threats. cPacket cClear integrates seamlessly with cPacket cVu packet data brokers and cStor capture and analytics observability nodes, providing the most accurate packet-data-based metadata for comprehensive network visibility. cPacket cClear simplifies network observability by correlating and presenting data in a user-friendly interface, making it easier for IT teams to understand and analyze network performance.

For more specific part numbering please refer to the **cPacket Quick Reference Guide** based on your Port speed, count and data retention requirements.

Results

DDoS Attack Dashboard



	total
Destination Unreachable	86 K
Echo Reply	6 K
Time Exceeded	3 K

	total
Communication administratively prohibited	1.585 K
Destination host unreachable	14.23 K
Destination port unreachable	69.0 K
Fragmentation required	1.198 K
Host administratively prohibited	16

Time Exceeded Errors

Code	Destination Hostname	Original Destination	Response	Message Counts
Time-to-live exceeded in transit	mail2.balancepro.com	216.38.135.175	92.63.197.55	4
Time-to-live exceeded in transit	mail2.balancepro.com	216.38.135.175	45.145.66.91	2
Time-to-live exceeded in transit	mail2.balancepro.com	216.38.135.174	193.27.228.64	2
Time-to-live exceeded in	mail2.balancepro.com	216.38.135.173	92.63.197.53	2

Destination Unreachable Erros

Code	Destination Hostname	Original Destination	Source Hostname	Original Source	responder_ip
Fragmentation required	zion.qbo.intuit.com	52.86.69.255	NXDOMAIN	10.51.49.138	10.51.49.138
Fragmentation required	zion.qbo.intuit.com	52.10.121.33	NXDOMAIN	10.51.49.138	10.51.49.138
Fragmentation required	zion.qbo.intuit.com	44.242.6.81	NXDOMAIN	10.51.49.138	10.51.49.138
Fragmentation required	zion.qbo.intuit.com	44.237.54.118	NXDOMAIN	10.51.49.138	10.51.49.138
Fragmentation required	zion.qbo.intuit.com	44.236.78.17	NXDOMAIN	10.51.49.138	10.51.49.138

Summary

DDoS attacks are increasingly sophisticated, leveraging techniques that closely resemble legitimate network traffic, making them difficult to identify and mitigate using traditional network observability tools. As a result, many organizations are forced to deploy separate security solutions alongside their observability platforms, leading to increased complexity and higher costs. These fragmented approaches can delay detection and response, leaving networks vulnerable to prolonged disruptions.

cPacket offers a comprehensive solution that minimizes the cost and expands the scope of DDoS monitoring, while providing standard packet brokering functions. Its edge-based monitoring and counting capabilities deliver precise, high-speed DDoS detection, while concurrently using its dedicated per-port ASIC architecture, for packet monitoring, categorization, and inspection at line rates up to 400Gbps. This approach provides visibility into every packet, from the network edge to the core, allow it to identify traffic imbalances and communication failures that signal DDoS attacks. These capabilities allow for early detection and accurate differentiation between malicious activity and normal network behavior.

With breadth across multiple detection points, cPacket solutions monitor all critical aspects of network traffic, including SYN/SYNACK imbalances, fragmented payloads, null-payload TCP sessions, and unexpected packet types. This depth of analysis provides a holistic view of network health, ensuring no anomaly goes unnoticed. Compared to competitors, cPacket's line-rate processing, SMART filtering, and rules-based counters enable faster, earlier, and more precise detection of DDoS threats, significantly reducing time-to-response and mitigating damage before it escalates.

cPacket's approach integrates real-time analytics, deep packet inspection, and historical data retention within its cStor and cClear platforms, ensuring organizations are equipped to detect, analyze, and respond to attacks with efficiency and precision. By combining advanced anomaly detection, seamless integration with security tools, and highly scalable architecture, cPacket delivers unmatched observability that not only safeguards against DDoS attacks but also ensures compliance and audit readiness.

Organizations across industries—from Enterprise to government agencies and financial institutions—can rely on cPacket to mitigate the financial and reputational risks of DDoS attacks. With industry-leading performance, cPacket solutions provide a proactive, edge-based advantage that sets them apart, offering security teams the tools they need to act decisively and protect critical infrastructure.

Find out more

For more information or a demonstration of the cPacket suite of network observability and security tools, please contact your local cPacket sales representative.

cPacket™

About cPacket Networks