

Cloud DDoS Network Analytics








Cloud DDoS Network Analytics

The Cloud DDoS Network Analytics service, a component of Cisco Secure Cloud DDoS Protection,¹ provides detailed, granular insights into network traffic, network services in use, and much more. The advanced network analytics service allows administrators to eliminate errors

when planning network deployments and stay ahead of DDoS threats through early detection of network abuse and intrusion. The service provides a graphical representation of data along with advanced filtering and investigation capabilities.

Key features

	Enhanced visibility <ul style="list-style-type: none">Provides deep insights into network behavior and performance with intuitive graphical representations
	Proactive monitoring <ul style="list-style-type: none">Detects anomalies and potential security threats early with comprehensive data visualization
	Customized analysis <ul style="list-style-type: none">Allows your analysis to be tailored to specific network segments or criteria using advanced filters
	Improved decision making <ul style="list-style-type: none">Enables more informed decision based on accurate and detailed network traffic analysis
	Scalability <ul style="list-style-type: none">Provides detailed insights into networks of all sizes, from small enterprises to large corporations

Graphical insights

Experience enriched data visualization with charts and graphs that offer intuitive insights into network activity over time based on various criteria including:

- **Assets:** view distribution and utilization of network assets
- **Sites:** monitor traffic patterns across your different geographical site locations
- **Top source countries:** identify countries with the highest traffic volume
- **Top protocols:** identify dominant network protocols in use
- **Top services:** analyze the usage of different network services
- **Top TCP flags:** monitor TCP flag usage for anomaly detection
- **Top packet sizes:** insights into packet size distributions
- **Top ASN:** identify organizations with the highest traffic by their the ASN

¹ Cisco Cloud DDoS Protection, Cloud Network Analytics, and other industry-leading security solutions are sold by Cisco through its global OEM partnership with Radware.

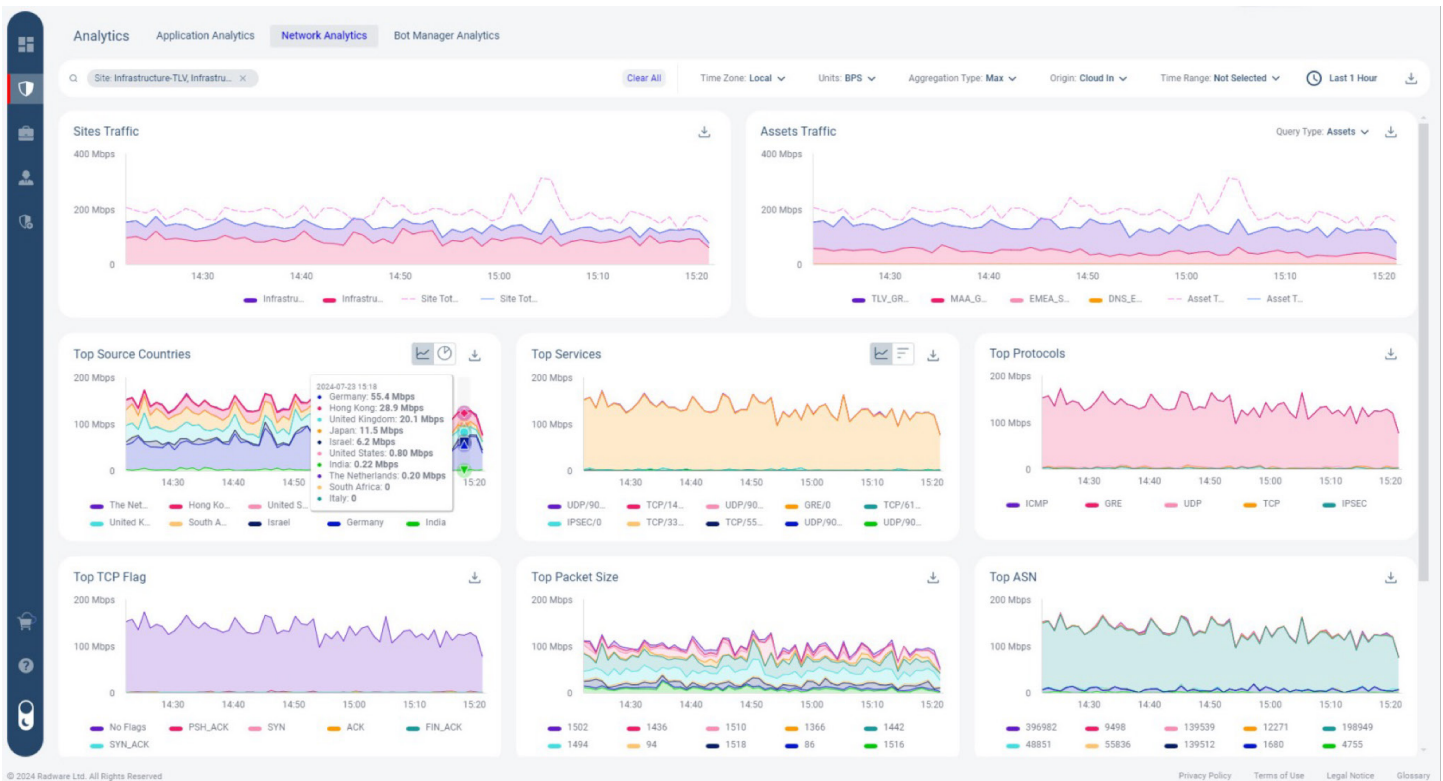


Figure 1. Graphical representation of data in the Cloud Network Analytics tab of the Radware¹ Unified Cloud portal

Advanced filtering

Users can perform deep investigations and network analysis with advanced filtering options, allowing you to slice and filter traffic by:

- **Assets & site:** filter based on specific network assets or segments
- **IP address:** drill down into traffic patterns based on IP addresses
- **Source countries and ASNs:** filter traffic originating from specific counties or ASNs
- **Protocols and ports:** focus on traffic using specific network protocols or ports
- **TCP flags:** filter traffic by TCP flag types (for example, SYN, ACK)
- **Packet sizes:** segment traffic by packet size for detailed analysis

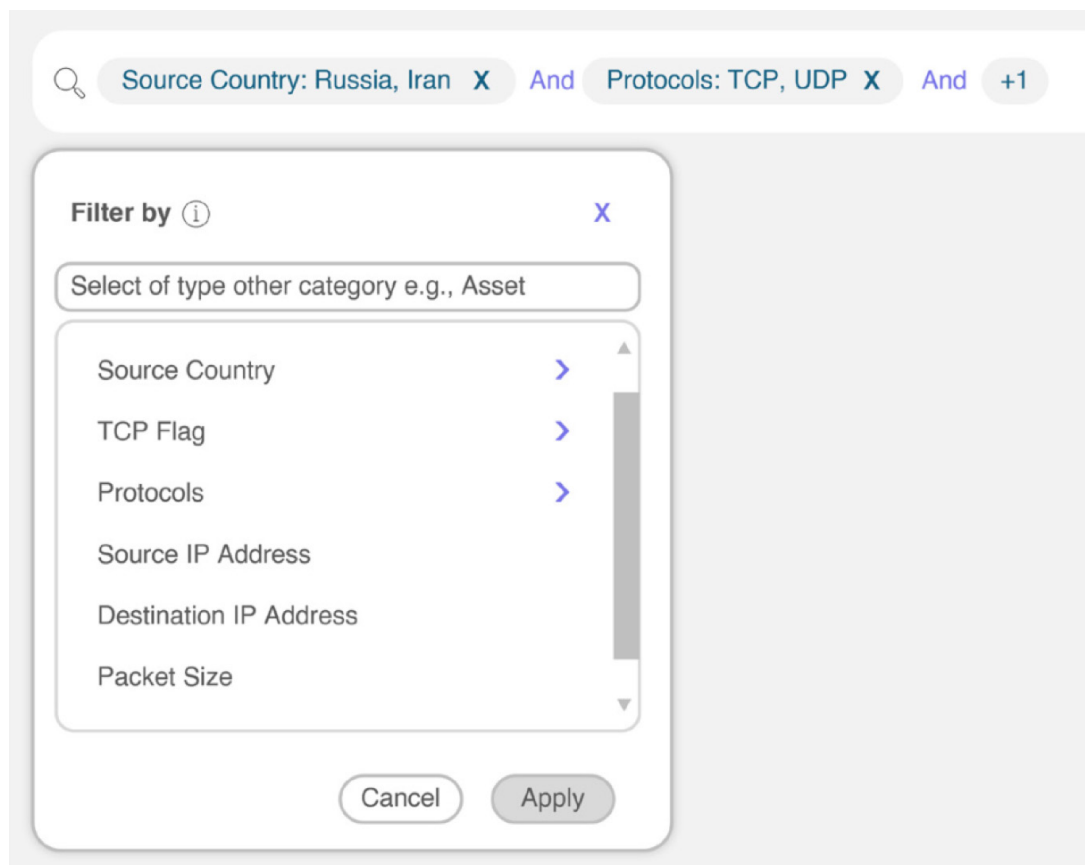


Figure 2. View of the Cloud Network Analytics advanced filtering selection tool

Deep investigation made simple

The Cloud DDoS Network Analytics service is designed to empower decision making with the tools needed to conduct thorough network traffic analysis, identify trends, detect anomalies, and enhance overall network

security. Whether analyzing specific assets, drilling down into geographical patterns, or examining detailed protocol interactions, Cloud DDoS Network Analytics puts powerful tools at your fingertips.