 **source\_address**: The IP address where the network traffic originates. This is crucial for identifying the source of data transfers and potential points of origin for attacks.

 **destination\_address**: The IP address where the network traffic is directed. Key for tracking the target of data transfers and assessing potential vulnerabilities at the destination.

 **source\_port**: The port number on the source IP used for initiating the connection. Helps identify the specific application or service that is generating the traffic.

 **destination\_port**: The port number on the destination IP receiving the connection. Indicates which service or application on the destination is being accessed, useful for understanding service interactions.

 **protocol**: The communication protocol used (e.g., TCP, UDP). Defines the method of data exchange and is vital for filtering and analyzing different types of network traffic.

 **app\_protocol**: The application-level protocol used (e.g., HTTP, FTP). Provides insight into the specific type of application traffic, important for application-layer analysis and security.

 **application\_name**: The name of the application generating the traffic. Identifies which software is involved, useful for tracking and monitoring application-specific behavior.

 **application\_category\_name**: The category or type of the application (e.g., web browser, email client). Helps classify traffic based on application type, aiding in high-level traffic analysis.

 **master\_application\_name**: The primary or parent application name, often used to group related applications. Provides context for understanding the broader application ecosystem.

 **tunnel\_source\_address**: The source IP address used in a tunneling protocol (e.g., VPN). Important for tracking traffic that is encapsulated or encrypted.

 **tunnel\_destination\_address**: The destination IP address used in a tunneling protocol. Helps identify the endpoint of tunneled traffic, critical for analyzing VPN or other encapsulated traffic.

 **source\_mac**: The MAC address of the source device. Used to uniquely identify the hardware initiating the traffic, essential for network identification and tracking.

 **destination\_mac**: The MAC address of the destination device. Helps in identifying the hardware receiving the traffic and can be used for network troubleshooting and monitoring.

 **tunnel\_value**: A value associated with the tunnel (e.g., tunnel ID). Provides additional context for traffic within a tunnel, useful for detailed network analysis.

 **package\_count**: The total number of packets exchanged in the traffic flow. Indicates the volume of data and helps in analyzing traffic patterns and performance.

 **login\_fail\_count**: The number of failed login attempts. Useful for detecting potential security incidents such as brute-force attacks.

 **login\_success**: The number of successful login attempts. Helps in tracking legitimate access and understanding user authentication patterns.

 **expiration\_id**: Identifier for session or data expiration. Useful for managing session lifecycles and ensuring proper handling of expired sessions.

 **drop\_eligible**: Indicator if a packet is eligible to be dropped. Important for traffic management and security measures, such as filtering out unwanted traffic.

 **priority**: Priority level assigned to the network traffic. Helps in managing and prioritizing critical traffic over less important traffic.

 **vlan\_identifier**: Identifier for the VLAN (Virtual LAN) associated with the traffic. Provides context on traffic segregation and helps in network management.

 **event\_time**: Timestamp of when the network event occurred. Essential for time-based analysis, including traffic patterns and attack timelines.

 **bidirectional\_first\_seen\_ms**: Timestamp when bidirectional traffic first appeared. Helps in tracking the start of traffic flows between two endpoints.

 **bidirectional\_last\_seen\_ms**: Timestamp when bidirectional traffic last appeared. Indicates the end of traffic flows and helps in understanding traffic duration.

 **bidirectional\_duration\_ms**: Duration of bidirectional traffic in milliseconds. Provides insights into the length of communication sessions between endpoints.

 **bidirectional\_bytes**: Total amount of data transferred bidirectionally in bytes. Measures the volume of traffic exchanged in both directions.

 **bidirectional\_max\_piat\_ms**: Maximum inter-arrival time between packets bidirectionally in milliseconds. Indicates the maximum delay between packet arrivals.

 **bidirectional\_max\_ps**: Maximum packet size in bidirectional traffic. Helps in understanding traffic patterns and identifying potential anomalies.

 **bidirectional\_mean\_piat\_ms**: Mean inter-arrival time between packets bidirectionally in milliseconds. Provides an average delay between packets in bidirectional traffic.

 **bidirectional\_mean\_ps**: Mean packet size in bidirectional traffic. Helps in understanding the typical size of packets exchanged.

 **bidirectional\_min\_piat\_ms**: Minimum inter-arrival time between packets bidirectionally in milliseconds. Indicates the shortest delay between packet arrivals.

 **bidirectional\_min\_ps**: Minimum packet size in bidirectional traffic. Identifies the smallest packet size exchanged.

 **bidirectional\_packets**: Total number of packets exchanged bidirectionally. Measures the amount of discrete data transfers in both directions.

 **bidirectional\_stddev\_piat\_ms**: Standard deviation of inter-arrival time between packets bidirectionally. Provides variability in packet arrival times.

 **bidirectional\_stddev\_ps**: Standard deviation of packet size bidirectionally. Measures variability in packet sizes.

 **bidirectional\_syn\_packets**: Number of SYN packets in bidirectional traffic. Helps identify connection initiation attempts and potential SYN flood attacks.

 **bidirectional\_cwr\_packets**: Number of CWR packets in bidirectional traffic. Indicates congestion window reduction packets, useful for detecting congestion control issues.

 **bidirectional\_ece\_packets**: Number of ECE packets in bidirectional traffic. Used to detect congestion experience notifications.

 **bidirectional\_urg\_packets**: Number of URG packets in bidirectional traffic. Indicates urgent data packets that require immediate processing.

 **bidirectional\_ack\_packets**: Number of ACK packets in bidirectional traffic. Helps in tracking acknowledgment of data packets.

 **bidirectional\_psh\_packets**: Number of PSH packets in bidirectional traffic. Indicates packets that should be pushed to the receiving application immediately.

 **bidirectional\_rst\_packets**: Number of RST packets in bidirectional traffic. Helps in identifying reset connections.

 **bidirectional\_fin\_packets**: Number of FIN packets in bidirectional traffic. Indicates the end of a connection.

 **src2dst\_first\_seen\_ms**: Timestamp when the source-to-destination traffic first appeared. Useful for tracking the start of traffic in one direction.

 **src2dst\_last\_seen\_ms**: Timestamp when the source-to-destination traffic last appeared. Indicates the end of traffic in one direction.

 **src2dst\_duration\_ms**: Duration of source-to-destination traffic in milliseconds. Provides insights into the length of communication in this direction.

 **src2dst\_packets**: Total number of packets from source to destination. Measures the discrete data transfers in this direction.

 **src2dst\_bytes**: Total amount of data transferred from source to destination in bytes. Measures the volume of traffic in this direction.

 **src2dst\_max\_piat\_ms**: Maximum inter-arrival time between packets from source to destination in milliseconds. Indicates the longest delay between packet arrivals.

 **src2dst\_max\_ps**: Maximum packet size from source to destination. Helps in identifying the largest packets in this direction.

 **src2dst\_mean\_piat\_ms**: Mean inter-arrival time between packets from source to destination in milliseconds. Provides an average delay between packets in this direction.

 **src2dst\_mean\_ps**: Mean packet size from source to destination. Provides an average size of packets in this direction.

 **src2dst\_min\_piat\_ms**: Minimum inter-arrival time between packets from source to destination in milliseconds. Indicates the shortest delay between packet arrivals.

 **src2dst\_min\_ps**: Minimum packet size from source to destination. Identifies the smallest packets in this direction.

 **src2dst\_stddev\_piat\_ms**: Standard deviation of inter-arrival time between packets from source to destination. Measures variability in packet arrival times.

 **src2dst\_stddev\_ps**: Standard deviation of packet size from source to destination. Measures variability in packet sizes.

 **src2dst\_syn\_packets**: Number of SYN packets in source-to-destination traffic. Helps identify connection initiation attempts in this direction.

 **src2dst\_cwr\_packets**: Number of CWR packets in source-to-destination traffic. Indicates congestion window reduction packets in this direction.

 **src2dst\_ece\_packets**: Number of ECE packets in source-to-destination traffic. Used to detect congestion experience notifications.

 **src2dst\_urg\_packets**: Number of URG packets in source-to-destination traffic. Indicates urgent data packets in this direction.

 **src2dst\_ack\_packets**: Number of ACK packets in source-to-destination traffic. Tracks acknowledgment of data packets in this direction.

 **src2dst\_psh\_packets**: Number of PSH packets in source-to-destination traffic. Indicates packets that should be pushed to the receiving application immediately in this direction.

 **src2dst\_rst\_packets**: Number of RST packets in source-to-destination traffic. Identifies reset connections in this direction.

 **src2dst\_fin\_packets**: Number of FIN packets in source-to-destination traffic.