|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Tên feature** | **Sự miêu tả** | **STT** | **Tên feature** | **Sự miêu tả** |
| 1 | ts | Dấu thời gian của sự kiện kết nối. | 12 | conn\_state | Trạng thái kết nối. |
| 2 | uid | Mã định danh duy nhất cho kết nối. | 13 | local\_orig | Chỉ ra kết nối có được coi là cục bộ hay không. |
| 3 | id\_orig\_h | Địa chỉ IP nguồn. | 14 | local\_resp | Chỉ ra kết nối có được coi là cục bộ hay không. |
| 4 | id\_orig\_p | Cổng nguồn. | 15 | missed\_bytes | Số lượng byte bị thiếu trong kết nối. |
| 5 | id\_resp\_h | Địa chỉ IP đích. | 16 | history | Lịch sử các trạng thái kết nối. |
| 6 | id\_resp\_p | Cảng đích. | 17 | orig\_pkts | Số lượng gói tin được gửi từ nguồn đến đích. |
| 7 | proto | Giao thức mạng được sử dụng (ví dụ: 'tcp'). | 18 | orig\_ip\_bytes | Số lượng byte IP được gửi từ nguồn đến đích. |
| 8 | service | Dịch vụ liên quan đến kết nối. | 19 | resp\_pkts | Số lượng gói tin được gửi từ đích đến nguồn. |
| 9 | duration | Thời gian kết nối. | 20 | resp\_ip\_bytes | Số lượng byte IP được gửi từ đích đến nguồn. |
| **STT** | **Tên feature** | **Sự miêu tả** | **STT** | **Tên feature** | **Sự miêu tả** |
| 10 | orig\_bytes | Số byte được gửi từ nguồn đến đích. | 21 | tunnel\_parents | Chỉ ra liệu kết nối này có phải là của đường hầm hay không. |
| 11 | resp\_bytes | Số byte được gửi từ đích đến nguồn. | 22 | label | Nhãn liên quan đến kết nối ('Benign' hoặc 'Malware'). |

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên đặc trưng** | **Ý nghĩa** |
| 1 | Destination Port | Cổng mạng mà gói tin hướng đến trên thiết bị đích |
| 2 | Flow Duration | Tổng thời gian (micro giây) của luồng kết nối |
| 3 | Total Fwd Packets | Số lượng gói được gửi từ nguồn đến đích |
| 4 | Total Backward Packets | Số lượng gói được gửi từ đích về nguồn |
| 5 | Total Length of Fwd Packets | Tổng kích thước (bytes) của gói gửi từ nguồn |
| 6 | Total Length of Bwd Packets | Tổng kích thước (bytes) của gói gửi từ đích |
| 7 | Fwd Packet Length Max | Gói lớn nhất gửi từ nguồn |
| 8 | Fwd Packet Length Min | Gói nhỏ nhất gửi từ nguồn |
| 9 | Fwd Packet Length Mean | Trung bình kích thước gói gửi từ nguồn |
| 10 | Fwd Packet Length Std | Đo độ phân tán kích thước gói |
| 11 | Bwd Packet Length Max | Gói lớn nhất gửi từ đích |
| 12 | Bwd Packet Length Min | Gói nhỏ nhất gửi từ đích |
| 13 | Bwd Packet Length Mean | Trung bình kích thước gói gửi từ đích |
| 14 | Bwd Packet Length Std | Mức độ phân tán kích thước phản hồi |
| 15 | Flow Bytes/s | Tốc độ truyền dữ liệu (byte/giây) |
| 16 | Flow Packets/s | Tốc độ gửi gói |
| 17 | Flow IAT Mean | Trung bình thời gian giữa hai gói liên tiếp |
| 18 | Flow IAT Std | Biến động thời gian giữa các gói |
| 19 | Flow IAT Max | Thời gian dài nhất giữa hai gói |
| 20 | Flow IAT Min | Thời gian ngắn nhất giữa hai gói |
| 21 | Fwd IAT Total | Tổng thời gian giữa các gói từ nguồn |
| 22 | Fwd IAT Mean | Trung bình thời gian giữa các gói từ nguồn |
| 23 | Fwd IAT Std | Biến động thời gian giữa các gói nguồn |
| 24 | Fwd IAT Max | Lớn nhất giữa 2 gói từ nguồn |
| **STT** | **Tên đặc trưng** | **Ý nghĩa** |
| 25 | Fwd IAT Min | Nhỏ nhất giữa 2 gói từ nguồn |
| 26 | Bwd IAT Total | Tổng thời gian giữa các gói từ đích |
| 27 | Bwd IAT Mean | Trung bình thời gian giữa các gói từ đích |
| 28 | Bwd IAT Std | Biến động thời gian giữa các gói từ đích |
| 29 | Bwd IAT Max | Lớn nhất giữa 2 gói từ đích |
| 30 | Bwd IAT Min | Nhỏ nhất giữa 2 gói từ đích |
| 31 | Fwd PSH Flags | Số lượng gói tin có cờ PSH |
| 32 | Bwd PSH Flags | Số lượng gói tin phản hồi có cờ PSH |
| 33 | Fwd URG Flags | Gói có cờ URG từ nguồn |
| 34 | Bwd URG Flags | Gói có cờ URG từ đích |
| 35 | Fwd Header Length | Tổng kích thước phần đầu gói (header) từ nguồn |
| 36 | Bwd Header Length | Tổng kích thước phần đầu từ đích |
| 37 | Fwd Packets/s | Tốc độ gửi gói từ nguồn |
| 38 | Bwd Packets/s | Tốc độ gửi gói từ đích |
| 39 | Packet Length Min | Gói nhỏ nhất trong luồng |
| 40 | Packet Length Max | Gói lớn nhất trong luồng |
| 41 | Packet Length Mean | Kích thước gói trung bình |
| 42 | Packet Length Std | Mức độ biến động kích thước |
| 43 | FIN Flag Count | Cờ kết thúc kết nối |
| 44 | SYN Flag Count | Cờ bắt đầu kết nối |
| 45 | RST Flag Count | Cờ thiết lập lại kết nối |
| 46 | PSH Flag Count | Đẩy dữ liệu đến ứng dụng |
| 47 | ACK Flag Count | Cờ xác nhận nhận dữ liệu |
| 48 | URG Flag Count | Cờ khẩn cấp |
| 49 | CWE Flag Count | Cờ bất thường trong giao tiếp |
| 50 | ECE Flag Count | ECN-capable flag (congestion control) |
| 51 | Down/Up Ratio | Dữ liệu tải xuống so với tải lên |
| 52 | Average Packet Size | Trung bình toàn bộ gói |
| 53 | Avg Fwd Segment Size | Mỗi TCP segment từ nguồn |
| 54 | Avg Bwd Segment Size | Mỗi TCP segment từ đích |
| 55 | Fwd Header Length.1 | Có thể bị trùng lặp với cột 35 |
| 56 | Fwd Avg Bytes/Bulk | Trung bình byte mỗi đợt truyền |
| 57 | Fwd Avg Packets/Bulk | Trung bình số gói mỗi đợt truyền |
| 58 | Fwd Avg Bulk Rate | Tốc độ dữ liệu theo đợt |
| 59 | Bwd Avg Bytes/Bulk | Trung bình byte mỗi đợt phản hồi |
| 60 | Bwd Avg Packets/Bulk | Trung bình gói trong đợt phản hồi |
| 61 | Bwd Avg Bulk Rate | Tốc độ phản hồi theo đợt |
| 62 | Subflow Fwd Packets | Gói chia nhỏ luồng từ nguồn |
| 63 | Subflow Fwd Bytes | Tổng byte trong subflow |
| 64 | Subflow Bwd Packets | Gói chia nhỏ luồng từ đích |
| 65 | Subflow Bwd Bytes | Tổng byte trong subflow |
| 66 | Init\_Win\_bytes\_forward | TCP Window size tại bắt đầu |
| 67 | Init\_Win\_bytes\_backward | TCP Window size tại bắt đầu |
| 68 | act\_data\_pkt\_fwd | Gói tin chứa payload từ nguồn |
| 69 | min\_seg\_size\_forward | Đoạn TCP nhỏ nhất |
| 70 | Active Mean | Trung bình thời gian giữa 2 gói hoạt động |
| 71 | Active Std | Biến động thời gian hoạt động |
| 72 | Active Max | Hoạt động lâu nhất giữa gói |
| 73 | Active Min | Khoảng hoạt động ngắn nhất |
| 74 | Idle Mean | Khoảng thời gian không hoạt động |
| 75 | Idle Std | Biến động thời gian rảnh |
| 76 | Idle Max | Khoảng nghỉ dài nhất |
| 77 | Idle Min | Khoảng nghỉ ngắn nhất |
| 78 | Label | Phân loại loại tấn công hoặc Benign |
| 79 | Protocol | Giao thức TCP, UDP |
| 80 | Timestamp | Thời điểm gói được ghi nhận |

| **STT** | **Tên đặc trưng** | **Ý nghĩa** | **STT** | **Tên đặc trưng** | **Ý nghĩa** |
| --- | --- | --- | --- | --- | --- |
| 1 | Destination Port | Cổng mạng gói tin đến trên thiết bị đích | 41 | Packet Length Mean | Kích thước gói trung bình |
| 2 | Flow Duration | Tổng thời gian (micro giây) của luồng kết nối | 42 | Packet Length Std | Mức độ biến động kích thước |
| 3 | Total Fwd Packets | Số lượng gói được gửi từ nguồn đến đích | 43 | FIN Flag Count | Cờ kết thúc kết nối |
| 4 | Total Backward Packets | Số lượng gói được gửi từ đích về nguồn | 44 | SYN Flag Count | Cờ bắt đầu kết nối |
| 5 | Total Length of Fwd Packets | Tổng kích thước (bytes) của gói gửi từ nguồn | 45 | RST Flag Count | Cờ thiết lập lại kết nối |
| 6 | Total Length of Bwd Packets | Tổng kích thước (bytes) của gói gửi từ đích | 46 | PSH Flag Count | Đẩy dữ liệu đến ứng dụng |
| 7 | Fwd Packet Length Max | Gói lớn nhất gửi từ nguồn | 47 | ACK Flag Count | Cờ xác nhận nhận dữ liệu |
| 8 | Fwd Packet Length Min | Gói nhỏ nhất gửi từ nguồn | 48 | URG Flag Count | Cờ khẩn cấp |
| 9 | Fwd Packet Length Mean | Trung bình kích thước gói gửi từ nguồn | 49 | CWE Flag Count | Cờ bất thường trong giao tiếp |
| 10 | Fwd Packet Length Std | Đo độ phân tán kích thước gói | 50 | ECE Flag Count | ECN-capable flag (congestion control) |
| 11 | Bwd Packet Length Max | Gói lớn nhất gửi từ đích | 51 | Down/Up Ratio | Dữ liệu tải xuống so với tải lên |
| 12 | Bwd Packet Length Min | Gói nhỏ nhất gửi từ đích | 52 | Average Packet Size | Trung bình toàn bộ gói |
| 13 | Bwd Packet Length Mean | Trung bình kích thước gói gửi từ đích | 53 | Avg Fwd Segment Size | Mỗi TCP segment từ nguồn |
| 14 | Bwd Packet Length Std | Mức độ phân tán kích thước phản hồi | 54 | Avg Bwd Segment Size | Mỗi TCP segment từ đích |
| 15 | Flow Bytes/s | Tốc độ truyền dữ liệu (byte/giây) | 55 | Fwd Header Length.1 | Có thể bị trùng lặp với cột 35 |
| 16 | Flow Packets/s | Tốc độ gửi gói | 56 | Fwd Avg Bytes/Bulk | Trung bình byte mỗi đợt truyền |
| 17 | Flow IAT Mean | Trung bình thời gian giữa hai gói liên tiếp | 57 | Fwd Avg Packets/Bulk | Trung bình số gói mỗi đợt truyền |
| 18 | Flow IAT Std | Biến động thời gian giữa các gói | 58 | Fwd Avg Bulk Rate | Tốc độ dữ liệu theo đợt |
| 19 | Flow IAT Max | Thời gian dài nhất giữa hai gói | 59 | Bwd Avg Bytes/Bulk | Trung bình byte mỗi đợt phản hồi |
| 20 | Flow IAT Min | Thời gian ngắn nhất giữa hai gói | 60 | Bwd Avg Packets/Bulk | Trung bình gói trong đợt phản hồi |
| 21 | Fwd IAT Total | Tổng thời gian giữa các gói từ nguồn | 61 | Bwd Avg Bulk Rate | Tốc độ phản hồi theo đợt |
| 22 | Fwd IAT Mean | Trung bình thời gian giữa các gói từ nguồn | 62 | Subflow Fwd Packets | Gói chia nhỏ luồng từ nguồn |
| 23 | Fwd IAT Std | Biến động thời gian giữa các gói nguồn | 63 | Subflow Fwd Bytes | Tổng byte trong subflow |
| 24 | Fwd IAT Max | Lớn nhất giữa 2 gói từ nguồn | 64 | Subflow Bwd Packets | Gói chia nhỏ luồng từ đích |
| 25 | Fwd IAT Min | Nhỏ nhất giữa 2 gói từ nguồn | 65 | Subflow Bwd Bytes | Tổng byte trong subflow |
| 26 | Bwd IAT Total | Tổng thời gian giữa các gói từ đích | 66 | Init\_Win\_bytes\_forward | TCP Window size tại bắt đầu |
| 27 | Bwd IAT Mean | Trung bình thời gian giữa các gói từ đích | 67 | Init\_Win\_bytes\_backward | TCP Window size tại bắt đầu |
| 28 | Bwd IAT Std | Biến động thời gian giữa các gói từ đích | 68 | act\_data\_pkt\_fwd | Gói tin chứa payload từ nguồn |
| 29 | Bwd IAT Max | Lớn nhất giữa 2 gói từ đích | 69 | min\_seg\_size\_forward | Đoạn TCP nhỏ nhất |
| 30 | Bwd IAT Min | Nhỏ nhất giữa 2 gói từ đích | 70 | Active Mean | Trung bình thời gian giữa 2 gói hoạt động |
| 31 | Fwd PSH Flags | Số lượng gói tin có cờ PSH | 71 | Active Std | Biến động thời gian hoạt động |
| 32 | Bwd PSH Flags | Số lượng gói tin phản hồi có cờ PSH | 72 | Active Max | Hoạt động lâu nhất giữa gói |
| 33 | Fwd URG Flags | Gói có cờ URG từ nguồn | 73 | Active Min | Khoảng hoạt động ngắn nhất |
| 34 | Bwd URG Flags | Gói có cờ URG từ đích | 74 | Idle Mean | Khoảng thời gian không hoạt động |
| 35 | Fwd Header Length | Tổng kích thước phần đầu gói (header) từ nguồn | 75 | Idle Std | Biến động thời gian rảnh |
| 36 | Bwd Header Length | Tổng kích thước phần đầu từ đích | 76 | Idle Max | Khoảng nghỉ dài nhất |
| 37 | Fwd Packets/s | Tốc độ gửi gói từ nguồn | 77 | Idle Min | Khoảng nghỉ ngắn nhất |
| 38 | Bwd Packets/s | Tốc độ gửi gói từ đích | 78 | Label | Phân loại loại tấn công hoặc Benign |
| 39 | Packet Length Min | Gói nhỏ nhất trong luồng | 79 | Protocol | Giao thức TCP, UDP |
| 40 | Packet Length Max | Gói lớn nhất trong luồng | 80 | Timestamp | Thời điểm gói được ghi nhận |