|  |  |  |  |
| --- | --- | --- | --- |
| Feature | Value | Interpretation | Predicted Label |
| Flow\_Duration | 15000 | Normal duration | Normal |
| Total\_Fwd\_Packets | 20 | Balanced number of packets | Normal |
| Flow\_Bytes\_s | 500 | Moderate bytes per second | Normal |
| Fwd\_IAT\_Mean | 100 | Reasonable average packet interval | Normal |
| Flow\_Duration | 100 | Very short flow duration | Anomaly |
| Total\_Fwd\_Packets | 1 | Very low packets | Anomaly |
| Flow\_Bytes\_s | 10000 | Extremely high bytes per second | Anomaly |
| Fwd\_IAT\_Mean | 1 | Very high frequency packets | Anomaly |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Feature | Typical Normal Value Range/Behavior | Typical Anomalous Value Behavior | Why It Matters for Anomaly Detection | | Flow\_Duration | Moderate to high values (e.g., 1000 ms to minutes) | Extremely low or very high values | Anomalies may have unusually short or very long flow durations | | Total\_Fwd\_Packets | Balanced packet counts in forward direction | Very low or very high packet counts | Too few or too many packets can indicate suspicious behavior | | Total\_Backward\_Packets | Balanced packet counts in backward direction | Very low or none, or extremely high | Absence or excess of response packets can indicate anomalies | | Fwd\_Packet\_Length\_Max | Normal max packet sizes (depends on protocol, e.g., 40-1500 bytes) | Very small or abnormally large packet sizes | Abnormal packet sizes can reflect malformed or malicious traffic | | Bwd\_Packet\_Length\_Max | Normal max packet sizes in backward packets | Very small or very large | Same as forward direction | | Flow\_Bytes\_s | Moderate bytes per second typical for flow | Extremely high or low byte rates | Sudden spikes or drops in traffic rates signal anomalies | | Flow\_Packets\_s | Typical packet rates consistent with normal flow | Very high packet rate or very low | Burst traffic or idle flows can be anomalous | | Fwd\_IAT\_Mean | Moderate average time between packets (milliseconds) | Very low (high frequency) or very high (delays) | Unusual timing between packets can indicate scanning or flooding | | Bwd\_IAT\_Mean | Similar to forward IAT mean | Very low or very high | Same reason as above | | Packet\_Length\_Variance | Normal variance indicating diversity in packet sizes | Very low (all packets same size) or very high variance | Too uniform or erratic packet sizes can be suspicious | | Average\_Packet\_Size | Average sizes consistent with normal communication | Very small or very large average packet sizes | Indicates abnormal payloads or malformed packets | |