WHAT IS CLAIMED IS:

1. A computer-implemented method for monitoring for anomalies in network traffic, the method comprising:

    for a data flow transmitted between a sender host and a receiver host:

        recording, on a first rolling basis, by the sender host, a first pre-defined amount of sent network traffic of the data flow;

        recording, on a second rolling basis, by the receiver host, a second pre-defined amount of received network traffic of the data flow, wherein the sender host and the receiver host are clock-synchronized;

    monitoring for an anomaly in the data flow based on time stamps of data packets in the network traffic;

    determining whether an anomaly is detected during the monitoring;

    responsive to determining that no anomaly is detected during the monitoring, overwriting the recorded sent network traffic and the recorded received network traffic with newly sent network traffic and newly received network traffic, respectively; and

    responsive to determining that an anomaly is detected during the monitoring, pausing the data flow, causing the sender host to store the recorded sent network traffic to a first buffer, and causing the receiver host to store the recorded received network traffic to a second buffer.

2. The computer-implemented method of claim 1, wherein the first pre-defined amount of sent network traffic and the second pre-defined amount of received network traffic are a same amount.

3. The computer-implemented method of claim 2, wherein the same amount is measured using either a pre-defined number of most recently transmitted or received packets, or packets received during a pre-defined amount of units of time prior to a current time.

4. The computer-implemented method of claim 1, wherein determining that an anomaly is detected during the monitoring comprises determining that a one-way delay of a data packet sent by the sender host to the receiver host exceeds a threshold amount of delay.

5. The computer-implemented method of claim 4, further comprising determining the one-way delay using a send time stamp applied by the sender host to data packets of the data flow as compared to a receive time stamp applied by the receiver host to the data packets, wherein the sender host and the receiver host are synchronized to a same reference clock, and wherein the send time stamp and the receive time stamp are based on the same reference clock.

6. The computer-implemented method of claim 1, wherein the sender host is located at either a kernel or a network interface card (NIC) of a sender device, and wherein the receiver host is located at either a kernel or a NIC of a receiver device.

7. The computer-implemented method of claim 6, wherein the sender device is a physical machine or a virtual machine, and wherein the receiver device is a physical machine or a virtual machine.

8. The computer-implemented method of claim 1, wherein the data flow includes data packets from a plurality of sender hosts, the plurality including the sender host, and wherein each of the plurality of sender hosts records the data packets it sends as part of the data flow.

9. The computer-implemented method of claim 8, wherein, responsive to determining that the anomaly is detected during the monitoring, causing each of the plurality of sender hosts to store their respective recorded data packets sent as part of the data flow to respective buffers.

10. The computer-implemented method of claim 9, further comprising, further responsive to determining that the anomaly is detected during the monitoring, retransmitting data packets associated with the anomaly from each sending host's respective buffer, and resuming the data flow.

11. The computer-implemented method of claim 10, wherein retransmitting the data packets comprises jittering a transmission time of two or more of the data packets at the sender

host to the receiver host, wherein jittering is done using one or more of predefined amounts of time or random amounts of time.

12. The computer-implemented method of claim 10, wherein retransmitting the data packets comprises re-transmitting all of the data packets from each sending host's respective buffer.

13. A non-transitory computer-readable medium comprising memory with instructions encoded thereon for monitoring for anomalies in network traffic, the instructions, when executed by one or more processors, comprising instructions to:

for a data flow transmitted between a sender host and a receiver host:

record, on a first rolling basis, by the sender host, a first pre-defined amount of sent network traffic of the data flow; and

record, on a second rolling basis, by the receiver host, a second pre-defined amount of received network traffic of the data flow, wherein the sender host and the receiver host are clock-synchronized;

monitor for an anomaly in the data flow based on time stamps of data packets in the network traffic;

determine whether an anomaly is detected during the monitoring;

responsive to determining that no anomaly is detected during the monitoring, overwrite the recorded sent network traffic and the recorded received network traffic with newly sent network traffic and newly received network traffic, respectively; and

responsive to determining that an anomaly is detected during the monitoring, pause the data flow, causing the sender host to store the recorded sent network traffic to a first buffer, and causing the receiver host to store the recorded received network traffic to a second buffer.

14. The non-transitory computer-readable medium of claim 13, wherein the first pre-defined amount of sent network traffic and the second pre-defined amount of received network traffic are a same amount.

15. The non-transitory computer-readable medium of claim 14, wherein the same amount is measured using either a pre-defined number of most recently transmitted or received packets, or packets received during a pre-defined amount of units of time prior to a current time.

16. The non-transitory computer-readable medium of claim 13, wherein determining that an anomaly is detected during the monitoring comprises determining that a one-way delay of a data packet sent by the sender host to the receiver host exceeds a threshold amount of delay.

17. The non-transitory computer-readable medium of claim 16, the instructions further comprising instructions to determine the one-way delay using a send time stamp applied by the sender host to data packets of the data flow as compared to a receive time stamp applied by the receiver host to the data packets, wherein the sender host and the receiver host are synchronized to a same reference clock, and wherein the send time stamp and the receive time stamp are based on the same reference clock.

18. The non-transitory computer-readable medium of claim 13, wherein the sender host is located at either a kernel or a network interface card (NIC) of a sender device, and wherein the receiver host is located at either a kernel or a NIC of a receiver device.

19. The non-transitory computer-readable medium of claim 18, wherein the sender device is a physical machine or a virtual machine, and wherein the receiver device is a physical machine or a virtual machine.

20. The non-transitory computer-readable medium of claim 13, wherein the data flow includes data packets from a plurality of sender hosts, the plurality including the sender host, and wherein each of the plurality of sender hosts records the data packets it sends as part of the data flow.

21. The non-transitory computer-readable medium of claim 13, wherein byte stamps are recorded for the data flow in persistent memory.