What is Claimed is:

1. A computer-implemented method for encrypting data for transmission, the method comprising:

causing a network interface controller (NIC) to encrypt first data to generate a first transmission control protocol (TCP) packet in accordance with a hardware-based transport layer security (TLS) offload mode;

computing a first re-transmission statistic in response to the first TCP packet failing to reach a first device over a first TCP connection; in response to the first re-transmission statistic meeting a first criterion, assigning the first TCP connection to a software-based TLS offload mode instead of the hardware-based TLS offload mode;

encrypting second data to generate a second TCP packet in accordance with the software-based TLS offload mode; and causing the NIC to transmit the second TCP packet to the first device over the first TCP connection.

2. The computer-implemented method of claim 1, wherein computing the first re-transmission statistic comprises computing at least one of a ratio or a percentage based on a total number of data bytes transmitted over the first TCP connection and a total number of data bytes re-transmitted over the first TCP connection.

3. The computer-implemented method of claim 1, wherein the first re-transmission statistic is computed based on a count of TCP packets used to transmit data over the first TCP connection.

4. The computer-implemented method of claim 1, wherein assigning the first TCP connection to the software-based TLS offload mode instead of the hardware-based TLS offload mode comprises comparing the first re-transmission statistic to a re-transmission threshold and determining that the hardware-based TLS offload mode is to be disabled for the first TCP connection.

5. The computer-implemented method of claim 1, further comprising initially assigning the first TCP connection to the hardware-based TLS offload mode.

6. The computer-implemented method of claim 1, further comprising causing the NIC to re-encrypt the first data to generate a third TCP packet in accordance with the hardware-based TLS offload mode in response to the first TCP packet failing to reach the first device over the first TCP connection.

7. The computer-implemented method of claim 1, wherein one or more TCP packets are transmitted in accordance with the hardware-based TLS offload mode that is assigned to a second TCP connection while the first TCP connection is assigned to the software-based TLS offload mode.

8. The computer-implemented method of claim 1, wherein assigning the first TCP connection to the software-based TLS offload mode instead of the hardware-based TLS offload mode comprises assigning a TLS session associated with a transmit side of the first TCP connection to the software-based TLS offload mode instead of the hardware-based TLS offload mode.

9. The computer-implemented method of claim 1, further comprising, prior to computing the first re-transmission statistic, updating at least one of a count of TCP packets used to transmit data over the first TCP connection or a total number of data bytes transmitted over the first TCP connection based on the first TCP packet.

10. The computer-implemented method of claim 1, further comprising, prior to using the NIC to encrypt first data to generate the first TCP packet, determining that a TLS session associated with a transmit side of the first TCP connection is assigned to the hardware-based TLS offload mode.

11. One or more non-transitory computer readable media including instructions that, when executed by one or more processors, cause the one or more processors to encrypt data for transmission by performing the steps of:

causing a network interface controller (NIC) to encrypt first data to generate a first transmission control protocol (TCP) packet in accordance with a hardware-based transport layer security (TLS) offload mode;

computing a first re-transmission statistic in response to the first TCP packet failing to reach a first device over a first TCP connection;

in response to the first re-transmission statistic meeting a first criterion, assigning the first TCP connection to a software-based TLS offload mode instead of the hardware-based TLS offload mode;

encrypting second data to generate a second TCP packet in accordance with the software-based TLS offload mode; and causing the NIC to transmit the second TCP packet to the first device over the first TCP connection.

12. The one or more non-transitory computer readable media of claim 11, wherein the first re-transmission statistic is computed based on a total number of data bytes transmitted over the first TCP connection.

13. The one or more non-transitory computer readable media of claim 11, wherein computing the first re-transmission statistic comprises computing a ratio or a percentage based on a first count of TCP packets used to transmit data over the first TCP connection and a second count of TCP packets used to re-transmit data over the first TCP connection.

14. The one or more non-transitory computer readable media of claim 11, wherein assigning the first TCP connection to the software-based TLS offload mode instead of the hardware-based TLS offload mode comprises comparing the first re-transmission statistic to a re-transmission threshold and determining that the hardware-based TLS offload mode is to be disabled for the first TCP connection.

15. The one or more non-transitory computer readable media of claim 11, further comprising initially assigning the first TCP connection to the hardware-based TLS offload mode.

16. The one or more non-transitory computer readable media of claim 11, further comprising causing the NIC to re-encrypt the first data to generate a third TCP packet in accordance with the hardware-based TLS offload mode in response to the first TCP packet failing to reach the first device over the first TCP connection.

17. The one or more non-transitory computer readable media of claim 11, wherein one or more TCP packets are transmitted in accordance with the hardware-based

TLS offload mode that is assigned to a second TCP connection while the first TCP connection is assigned to the software-based TLS offload mode.

18. The one or more non-transitory computer readable media of claim 11, further comprising, prior to computing the first re-transmission statistic, updating at least one of a count of TCP packets used to re-transmit data over the first TCP connection or a total number of data bytes re-transmitted over the first TCP connection to reflect a re-transmission of encrypted data to the first device over the first TCP connection.

19. The one or more non-transitory computer readable media of claim 11, further comprising, prior to using the NIC to encrypt first data to generate the first TCP packet, determining that a TLS session associated with a transmit side of the first TCP connection is assigned to the hardware-based TLS offload mode.

20. A system comprising: one or more memories storing instructions; and one or more processors coupled to the one or more memories that, when executing the instructions, perform the steps of:

causing a network interface controller (NIC) to encrypt first data to generate a first transmission control protocol (TCP) packet in accordance with a hardware-based transport layer security (TLS) offload mode;

computing a first re-transmission statistic in response to the first TCP packet failing to reach a first device over a first TCP connection in response to the first re-transmission statistic meeting a first criterion, assigning the first TCP connection to a software-based TLS offload mode instead of the hardware-based TLS offload mode;

encrypting second data to generate a second TCP packet in accordance with the software-based TLS offload mode; and causing the NIC to transmit the second TCP packet to the first device over the first TCP connection.