

WHAT IS CLAIMED IS:

1. A computer-implemented method for providing secure communications, comprising:

receiving, by a hypervisor, a request for a secure connection between a guest operating system and a computing device, the guest operating system being one of one or more guest operating systems supported by the hypervisor, a physical machine comprises the hypervisor and the one or more guest operating systems;

establishing, by the hypervisor on behalf of the guest operating system, in response to the request, the secure connection to the computing device using a secure protocol and a set of cryptographic credentials associated with the guest operating system, the hypervisor acting as a local endpoint of the secure connection using the set of cryptographic credentials;

managing, by the hypervisor, secure communications between the guest operating system and the computing device using the secure protocol and the set of cryptographic credentials; and

sending, by the hypervisor, one or more unsecured messages to the guest operating system in response to managing the secure communications between the guest operating system and the computing device.

2. The computer-implemented method of claim 1, wherein managing the secure communications between the guest operating system and the computing device further comprises:

receiving, by the hypervisor, the set of cryptographic credentials associated with the guest operating system from a certificate store;

encrypting, by the hypervisor, on behalf of the guest operating system using the secure protocol and the set of cryptographic credentials, one or more outgoing messages from the guest operating system to the computing device, the one or more outgoing messages becoming one or more outgoing encrypted messages; and

sending, by the hypervisor, the one or more outgoing encrypted messages to the computing device using the secure protocol.

3. The computer-implemented method of claim 1, wherein managing the secure communications between the guest operating system and the computing device further comprises:

receiving, by the hypervisor, the set of cryptographic credentials associated with the guest operating system from a certificate store;

receiving, by the hypervisor, one or more incoming encrypted messages from the computing device; and

decrypting, by the hypervisor on behalf of the guest operating system using the secure protocol and the set of cryptographic credentials, the one or more incoming encrypted messages from the computing device becoming one or more decrypted messages, wherein the one or more unsecured messages includes the one or more decrypted messages.

4. A computer system for providing a secure connection, comprising:

one or more processors;

one or more memories; and

a data plane including a support system, wherein the support system includes instructions stored in the one or more memories, the instructions executable by the one or more processors to cause the computer system to at least:

receive a set of cryptographic credentials associated with a guest operating system, the guest operating system being one of one or more guest operating systems supported by the support system, a physical machine comprises the support system and the one or more guest operating systems;

establish on behalf of the guest operating system a secure connection to a computing device using a secure protocol and the set of cryptographic credentials, the support system acting as a local endpoint of the secure connection using the set of cryptographic credentials;

manage secure communications between the guest operating system and the computing device using the secure protocol and the set of cryptographic credentials; and

send one or more messages to the guest operating system in response to managing the secure communications between the guest operating system and the computing device.

5. The system of claim 4, wherein the support system is a network interface card.

6. The system of claim 4, wherein the support system includes further instructions executable by the one or more processors to cause the computer system to at least:

capture an outgoing unsecured message from the guest operating system;

examine routing information of the outgoing unsecured message;

encrypt the outgoing unsecured message into an outgoing encrypted message based at least in part on the examination; and

direct the outgoing encrypted message toward the computing device.

7. The system of claim 4, wherein the support system includes further instructions executable by the one or more processors to cause the computer system to at least:

capture an incoming secured message directed to the guest operating system;

examine routing information of the incoming secured message;

decrypt the incoming secured message into an incoming decrypted message based at least in part on the examination; and

send the incoming decrypted message to the guest operating system.

8. The system of claim 4, wherein a control plane and the data plane reside within a same trust boundary.

9. The system of claim 4, wherein the support system includes further instructions executable by the one or more processors to cause the computer system to at least:

store the set of cryptographic credentials on behalf of the guest operating system.

10. The system of claim 4, wherein a control plane includes further instructions executable by the one or more processors to cause the computer system to at least:

receive a user request for the secure connection between the guest operating system and the computing device, the request including a set of user-specified configuration options.

11. The system of claim 10, wherein the set of user-specified configuration options includes at least one of an indication as to whether to continuously use secure communication, a set of ports to use for secure communication, an indication as to whether to automatically detect secure communication, an indication to use a particular IP address for secure communications, or an indication to use a virtual Ethernet adaptor for secure communications.

12. The system of claim 10, wherein the control plane includes further instructions executable by the one or more processors to cause the computer system to at least:

in response to the request for the secure connection, create a public and private key pair on behalf of the guest operating system;

request the set of cryptographic credentials for the guest operating system from a certificate authority using the public and private key pair;

receive the set of cryptographic credentials;

store the set of cryptographic credentials; and

provide the set of cryptographic credentials to the hypervisor.

13. A non-transitory computer-readable storage medium having stored thereon computer-executable instructions that, when executed with one or more processors, cause a computer system to perform operations comprising, at least:

obtaining, by a hypervisor, a set of cryptographic credentials associated with a guest operating system, the guest operating system being one of one or more guest operating systems supported by the hypervisor, a physical machine comprises the hypervisor and the one or more guest operating systems;

negotiating, by the hypervisor on behalf of the guest operating system, a secure connection between the hypervisor and a computing device using a secure protocol and the set of cryptographic credentials;

managing, by the hypervisor, secure communications between the guest operating system and the computing device using the secure protocol and the set of cryptographic credentials; and

sending one or more messages to the guest operating system in response to managing the secure communications between the guest operating system and the computing device.

14. The non-transitory computer-readable storage medium of claim 13, having stored thereon further computer-executable instructions that, when executed with the one or more processors, cause the one or more processors to perform operations comprising, at least:

storing, by the hypervisor, the set of cryptographic credentials associated with a guest operating system on behalf of the guest operating system.

15. The non-transitory computer-readable storage medium of claim 13, having stored thereon further computer-executable instructions that, when executed with the one or more processors, cause the one or more processors to perform operations comprising, at least:

updating the secure protocol by the hypervisor, wherein updating occurs independent of the guest operating system.

16. The non-transitory computer-readable storage medium of claim 13, having stored thereon further computer-executable instructions that, when executed

with the one or more processors, cause the one or more processors to perform operations comprising, at least:

receiving user input including configuration options, wherein the user input includes an indication that the user desires to enable secure socket layer communications.

17. The non-transitory computer-readable storage medium of claim 16, wherein the user input includes at least one of an indication as to whether to continuously use secure communication, a set of ports to use for secure communication, an indication as to whether to automatically detect secure communication, an indication to use a particular IP address for secure communications, or an indication to use a virtual Ethernet adaptor for secure communications.

18. The non-transitory computer-readable storage medium of claim 16, having stored thereon further computer-executable instructions that, when executed with the one or more processors, cause the one or more processors to perform operations comprising, at least:

determining, from the user input, a channel to use for the secure communications; and

restricting a message of the secure communications when the message is provided to the hypervisor using a different channel.

19. The non-transitory computer-readable storage medium of claim 16, having stored thereon further computer-executable instructions that, when executed with the one or more processors, cause the one or more processors to perform operations comprising, at least:

determining that the secure communication is complete;

terminating the secure connection using the secure protocol and the set of cryptographic credentials; and

deleting the set of cryptographic credentials from the hypervisor.

20. The non-transitory computer-readable storage medium of claim 16, wherein the user input is received using an application programming interface, and

wherein the user input is provided in response to an offer to add secure communication to the hypervisor in exchange for value.