

WHAT IS CLAIMED IS:

1. A computer-implemented method for providing secure communications, comprising:
under the control of one or more computer systems configured with executable instructions,
receiving, by a support system of a host system, a request for a secure connection with a device to a guest operating system on the host system, the host system having the support system and configured to host at least one guest operating system;
receiving, by the support system, a set of credentials associated with the guest operating system;
using, by the support system, the set of credentials on behalf of the guest operating system to establish a secure connection with the device, the support system acting as an endpoint of the secure connection in place of the guest operating system; and
sending, by the support system over the secure connection, one or more communications between the guest operating system and the device, the support system processing the one or more communications to enable the secure connection.

2. The computer-implemented method of claim 1, the method further including:
receiving, by the support system of the host system, a request for a second secure connection with a second device to a second guest operating system on the host system;
retrieving, by the support system, a second set of credentials associated with the second guest operating system;
using, by the support system, the second set of credentials on behalf of the second guest operating system to establish a second secure connection with the second device, the support system acting as an endpoint of the second secure connection in place of the second guest operating system; and
sending, by the support system over the second secure connection, one or more second communications between the second guest operating system and the second device.

3. The computer-implemented method of claim 1, wherein using the set of credentials further includes storing the set of credentials by the support system on behalf of the guest operating system, the set of credentials unreadable to the guest operating system.

1 4. The computer-implemented method of claim 1, wherein the support
2 system is a hypervisor, is a hardware security module attached to the host system, embedded
3 within a network interface card attached to the host system, or a separate processor within the
4 host system.

1 5. The computer-implemented method of claim 1, wherein sending one or
2 more communications further includes encrypting the one or more communications using a
3 secure protocol.

1 6. The computer-implemented method of claim 5, wherein the secure
2 protocol is transport layer security.

1 7. The computer-implemented method of claim 1, further comprising:
2 receiving a request to add a secure connection service to the guest operating
3 system on the host system, service using the support system to manage secure connections on
4 behalf of the guest operating system;
5 requesting the set of credentials associated with the guest operating system; and
6 storing, by the support system, the set of credentials.

1 8. The computer-implemented method of claim 7, further comprising:
2 charging a fee in exchange for adding the secure connection service to the guest
3 operating system.

1 9. The computer-implemented method of claim 1, wherein the support
2 system encrypts at least some of the communication over the secure connection.

1 10. A computer system for enabling a secure connection, comprising:
2 one or more processors; and
3 memory, including instructions executable by the one or more processors to cause
4 the computer system to at least:
5 receive, by a support system having a set of guest systems, a secure
6 communication directed to a guest system from the set of guest systems;
7 select, by the support system, the guest system from the set of guest
8 systems to which the secure communication is directed; and

9 provide, by the host system using a set of credentials that represent an
10 identity of the selected guest operating system, a decrypted message to the selected guest
11 operating system, the decrypted message prepared from the secure communication, the
12 credentials unavailable to the selected guest system.

1 11. The system of claim 10, the system further including a hardware security
2 module, the hardware security module in communication with the one or more processors, the
3 hardware security module providing encryption and decryption services to at least one of the one
4 or more processors, the hardware security module accessible to the support system to decrypt the
5 message.

1 12. The system of claim 10, wherein the support system is a network device,
2 the support system placed between the one or more guest systems and a network from which the
3 secure communication is received.

1 13. The system of claim 10, wherein providing a decrypted message further
2 includes:

3 receiving the secure communication through a first channel of communication,
4 the receipt through the first channel causing the support system to decrypt the secure
5 communication, wherein the support system is configured to decrypt communications received
6 through the first channel; and

7 passing through one or more communications received through a second channel
8 of communication to the guest system, wherein the support system is configured to pass through
9 communications received through a second channel.

1 14. The system of claim 10, wherein providing a decrypted message further
2 includes altering the decrypted message to indicate the decrypted message was previously
3 encrypted.

1 15. The system of claim 10, wherein the set of credentials include a private
2 key assigned to the guest operating system.

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;

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 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;

a data plane including a support system, wherein the support system includes instructions stored in the one or more memories, the one or more processors 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;

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 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 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 the 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 the 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;

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;

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:

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

restrict 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:

determine that the secure communication is complete;

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

deleting the set of 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.

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;

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 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;

a data plane including a support system, wherein the support system includes instructions stored in the one or more memories, the one or more processors 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;

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 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 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 the 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 the 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;

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;

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:

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

restrict 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:

determine that the secure communication is complete;

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

deleting the set of 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.