WHAT IS CLAIMED

1. A computer-implemented method, comprising:

obtaining, on a first network, a first request for a hardware security module from a plurality of hardware security modules managed by a computing resource service provider;

causing, based at least in part on parameters included in the first request, the computing resource service provider to connect the hardware security module of the plurality of hardware security modules to a second network; and

routing a second request at the first network to the hardware security module of the second network.

2. The computer-implemented method of claim 1, wherein the first network is an on-premise network associated with a customer of the computing resource service provider implementing the second network.

3. The computer-implemented method of claim 1, wherein the second network, as a result of identifying the hardware security module, implements a virtual network to associate with the hardware security module.

4. The computer-implemented method of claim 3, further comprising:

generating, by a device on the first network, a cryptographic request;

submitting the cryptographic request to cause the second network to route, via the virtual network, the cryptographic request to the identified hardware security module; and

routing a result of the cryptographic request to the device.

5. The computer-implemented method of claim 1, wherein information included in the request includes a credential associated with the hardware security module.

6. The computer-implemented method of claim 1, further comprising presenting the hardware security module on the first network as a local device of the first network.

7. A system, comprising:

memory to store instructions that, if executed by one or more processors of the system, cause the system to:

obtain, outside of a network, a first request for a hardware security module from a plurality of hardware security modules managed by a computing resource service provider;

cause, based at least in part on parameters included in the first request, the hardware security module of the plurality of hardware security modules to be added inside of the network; and

route a second request to the hardware security module.

8. The system of claim 7, wherein the instructions, if executed, further cause the system to:

cause inside of the network to add a virtual network to associate with the selected hardware security module;

associate the virtual network with a network interface outside of the network; and

route cryptographic requests to the selected hardware security module via the network interface.

9. The system of claim 7, wherein the request is an application programming interface (API) call to an API provided via inside of the network.

10. The system of claim 7, wherein the hardware security module is selected from a plurality of hardware security modules inside of the network.

11. The system of claim 7, wherein the second request is associated with a cryptographic operation to be performed by the security module outside of the network.

12. The system of claim 7, wherein the hardware security module stores, in a manner inaccessible to any other device inside of the network, cryptographic information on behalf of a device outside of the network.

13. A non-transitory computer-readable storage medium having instructions that, if executed by one or more processors of a computer system, cause the computer system to:

obtain, on a first network, a first request for a hardware security module from a plurality of hardware security modules managed by a computing resource service provider;

cause, based at least in part on parameters included in the first request, the computing resource service provider to identify the hardware security module of the plurality of hardware security modules to connect to a second network; and

route a second request at the first network to the hardware security module of the second network.

14. The non-transitory computer-readable storage medium of claim 13, wherein the instructions, if executed, further cause the computer system to cause generation of a network interface that enables the first network to connect to the hardware security module.

15. The non-transitory computer-readable storage medium of claim 13, wherein the first network is a physical network remote from the second network.

16. The non-transitory computer-readable storage medium of claim 13, wherein the second network identifies the hardware security module for exclusive use by the first network.

17. The non-transitory computer-readable storage medium of claim 13, wherein the second network is hosted by a computing resource provider and managed by a device associated with the first network.

18. The non-transitory computer-readable storage medium of claim 17, wherein the second network includes a network address designated by the device.

19. The non-transitory computer-readable storage medium of claim 13, wherein the second request is routed to the hardware security module via network address translation between a first network address on the first network and a second network address of the hardware security module.

20. The non-transitory computer-readable storage medium of claim 13, wherein the first request is a web service call to an interface of a computing resource service provider implementing the second network.