

CLAIMS:

1. A computer-implemented method, comprising:
 - under the control of one or more computer systems configured with executable instructions,
 - receiving, from a customer device remotely connected to a computing resource provider, a request to add a hardware security module hosted by the computing resource provider to a customer network that is hosted by the computing resource provider and remotely managed by the customer device;
 - as a result of receiving the request, selecting a hardware security module from a plurality of available hardware security modules local to the computing resource provider;
 - creating, in the customer network, a network interface to another network in communication with the selected hardware security module allocated to the customer device; and
 - configuring the network interface and other network such that requests through the customer network addressed to the network interface are provided to the selected hardware security module.
2. The computer-implemented method of claim 1, wherein:
 - the customer network comprises one or more devices having assigned corresponding network addresses defined by the customer device; and
 - the customer network is connected to an on-premise network hosted by the customer by a virtual private network connection.
3. The computer-implemented method of claim 1 or 2, wherein the network interface has a network address in a set of network addresses defined by the customer device.
4. The computer-implemented method of any of claims 1 to 3, further comprising:

receiving, from the customer device, a communication addressed to a network address of the interface; and

translating the network address of the communication to an address of the selected hardware security module that is utilized by the computing resource provider for routing network traffic to the hardware security module.

5. The computer-implemented method of any of claims 1 to 4, further comprising:
using a first administrative account of the hardware security module to create a second administrative account with device administration rights; and
providing a credential for the second administrative account to enable the customer device to change the credential, thereby revoking access to the second account from the computing resource provider.

6. The computer-implemented method of claims 1 to 5, further comprising:
creating, in the customer network, a second network interface to second network in communication with a second selected hardware security module allocated to the customer device; and
configuring the second network interface and other network such that requests through the customer network addressed to the second network interface are provided to the second selected hardware security module.

7. A computer-implemented method, comprising:
under the control of one or more computer systems configured with executable instructions,
receiving, from an entity remote from the one or more computer systems, a request to add a device to a network;
selecting, from a set of available devices hosted by and local to the one or more computer systems and usable to fulfill the request, a device;
allocating the selected device to exclusive use by the entity; and

reconfiguring a set of computing resources of the one or more computing systems such that that the network includes a network interface to another network connecting the network interface and the device and such that network traffic addressed to the network interface is forwarded over the other network to the selected device.

8. The computer-implemented method of claim 7, wherein the device is a hardware security module.

9. The computer-implemented method of claim 7 or 8, wherein:
the entity is a customer device remotely connected to a computing resource provider associated with the one or more computer systems; and
the network is hosted by the computing resource provider and managed by the customer device.

10. The computer-implemented method of any of claims 7 to 9, wherein the network comprises devices having network addresses defined by the entity.

11. The computer-implemented method of any of claims 7 to 10, wherein:
the network is hosted by an organization different from the entity; and
the network interface has an network address that is a private network address of the entity.

12. The computer-implemented method of any of claims 7 to 11, wherein the request is an application programming interface call to having parameters for fulfilling the request.

13. A system, comprising:
a set of computing resources that implements a network;
a web server configured to receive requests; and
a management subsystem configured to:

receive a request via the web server to add a security module hosted by and local to the system, to the network having a corresponding set of network addresses, the request originating from an entity remote to the system; and

as a result of receiving the request, configure at least a subset of the set of computing resources such that one or more devices in the network can communicate with the security module by addressing communications to the security module with a network address from the set of network addresses.

14. The system of claim 13, wherein configuring the subset of the set of computing resources includes:

adding a network interface to the network such that the network interface has the network address; and

connecting the network interface to the security module over another network implemented by the set of computing resources.

15. The system of claim 14, wherein the network and the other network are virtual local area networks.

16. The system of any of claims 13 to 15, wherein the security module is a hardware security module.

17. The system of any of claims 13 to 16, wherein:

the set of computing resources is hosted by a computing resource provider; and

the request is a Web services call from a customer device associated with the computing resource provider.

18. The system of any of claims 13 to 17, wherein:

the set of computing resources is hosted by a computing resource provider; and

at a time after configuring the set of computing resources, the security module stores, in a manner inaccessible to the computing resource provider, cryptographic information for a customer of the computing resource provider.

19. One or more non-transitory computer-readable storage media having collectively stored thereon instructions that, when executed by one or more processors of a computer system, cause the computer system to:

receive a remote request to add a security module to a network, the network being hosted on behalf a third-party entity and having a corresponding set of network addresses, the security module being local to and hosted on behalf of the third-party entity; and

as a result of receiving the request, cause reconfiguration of computing resources of a set of computing resources so that the communications to the security module are addressable using a network address from the corresponding set of network addresses.

20. One or more non-transitory computer-readable storage media of claim 19, wherein causing reconfiguration of the computing resources includes causing a network interface to a network connecting the network to the security module to become part of the network.

21. One or more non-transitory computer-readable storage media of claim 19 or 20, wherein the security module is a hardware security module.

22. One or more non-transitory computer-readable storage media of any of claims 19 to 21, wherein causing reconfiguration of the computing resources includes causing allocation of the security module to exclusive use by the third-party entity.

23. One or more non-transitory computer-readable storage media of any of claims 19 to 22, wherein:

the security module has a network address outside of the set of network addresses; and

causing reconfiguration of the computing resources includes connecting the network to a network address translation device that translates network addresses to enable communications between the network and the security module.

24. One or more non-transitory computer-readable storage media of any of claims 19 to 23, wherein the corresponding set of network addresses are private Internet protocol addresses.

25. A computer-implemented method, comprising:

receiving, by a computing resource provider, a request identifying a customer account to add a hardware security module to a virtual network of the computing resource service provider;

in response to the request:

selecting a hardware security module from a plurality of hardware security modules available to the computing resource provider;

configuring the hardware security module to be made available on a customer-defined subset of the virtual network for processing cryptographic requests; and

routing cryptographic requests initiated by a customer network associated with the customer account to the hardware security module for processing, via the customer-defined subset of the virtual network, such that cryptographic information used by the hardware security module to process the cryptographic requests is inaccessible to the computing resource service provider.

26. The computer-implemented method of claim 25, wherein:

the customer network is an on-premise network associated with the customer account; and

the customer-defined subset of the virtual network comprises one or more devices of the computing resource service provider having corresponding network addresses defined by the customer account.

27. The computer-implemented method of claim 25, wherein the customer network is connected to the virtual network via a virtual private network connection.
28. The computer-implemented method of claim 25, further comprising:
receiving, by the virtual network from a device on the customer network, a cryptographic request; and
routing the cryptographic request to the customer-defined subset so as to be processed by the hardware security module.
29. The computer-implemented method of claim 25, further comprising:
using a first administrative account of the hardware security module to create a second administrative account with device administration rights;
providing a credential for the second administrative account to enable a controlling entity to change the credential so as to revoke access to the second account from the computing resource provider.
30. The computer-implemented method of claim 25, further comprising presenting the hardware security module as a device on the customer network.
31. A system, comprising:
a set of computing resources that implements a network;
a web server that receives requests from one or more other networks remotely connected to the system; and
a management subsystem that at least:
receives a request forwarded by the web server to add a security module to the network having a corresponding set of network addresses available to the one or more other networks; and
based at least in part on the request, configures at least a subset of the set of computing resources such that:

one or more devices associated with the one or more other networks become capable of communicating with the security module by addressing communications to the security module with a network address from the set of network addresses, and cryptographic information used by the security module to process the communications is inaccessible to the set of computing resources.

32. The system of claim 31, wherein configuring the subset of the set of computing resources includes:

adding a network interface to the network such that the network interface has the network address; and

connecting the network interface to the security module.

33. The system of claim 32, wherein the network is a virtual local area network.

34. The system of claim 31, wherein the security module is a hardware security module.

35. The system of claim 31, wherein:

the set of computing resources is hosted by a computing resource provider; and

the request is a webservice call from the one or more other networks.

36. The system of claim 31, wherein:

the set of computing resources is hosted by a computing resource provider;

at a time after configuring the set of computing resources, the security module stores, in a manner inaccessible to the computing resource provider, cryptographic information for a device associated with the one or more other networks.

37. One or more non-transitory computer-readable storage media having collectively stored thereon instructions that, when executed by one or more processors of a computer system, cause the computer system to:

receive, from a first network, a request to add a security module to a second network, the second network being hosted on behalf of the first network, and having a corresponding set of network addresses;

based at least in part on the request, configure at least a set of computing resources of the computer system that implements the second network such that:

the communications to the security module are directed to a first network address from the corresponding set of network addresses and associated with the security module, and

cryptographic information used by the security module to process the communications is inaccessible to the set of computing resources.

38. The one or more non-transitory computer-readable storage media of claim 37, wherein causing reconfiguration of the computing resources includes generating a network interface that connects the second network to the security module.

39. The one or more non-transitory computer-readable storage media of claim 37, wherein the security module is a hardware security module.

40. The one or more non-transitory computer-readable storage media of claim 37, wherein causing reconfiguration of the computing resources includes causing allocation of the security module to exclusive use by the first network and the second network.

41. The one or more non-transitory computer-readable storage media of claim 37, wherein:
the first network is an on-premise network associated with a customer of a computing resource provider; and
the second network is hosted by the computing resource provider and managed by the customer.

42. The one or more non-transitory computer-readable storage media of claim 37, wherein the second network comprises devices having network addresses defined by the customer via the first network.

43. The one or more non-transitory computer-readable storage media of claim 37, wherein:
the security module has a network address outside of the set of network addresses; and
causing reconfiguration of the computing resources includes connecting the first network to a network address translation device associated with the second network that translates network addresses to enable communications between the first network and the security module.

44. The one or more non-transitory computer-readable storage media of claim 37, wherein the request is an application programming interface call.