Claims

WHAT IS CLAIMED IS:

1. A computer-implemented method for authenticating a connection, comprising:

under control of one or more computer systems configured with executable instructions,

establishing a dedicated physical network connection between a computing resource service provider network device connected to a computer resource service provider network and a customer network device connected to a customer network separate from the computer resource service provider network-device;

transmitting, from the computing resource service provider network device to the customer network device, through the dedicated physical network connection, a request for a customer to provide cryptographic authentication information for authenticating the customer network device;

receiving, at the computing resource service provider network device and from the customer network device, the cryptographic authentication information;

forwarding, from the computing resource service provider network device, the cryptographic authentication information to an authentication service that is operable to authenticate the cryptographic authentication information via verification based at least in part on a secret key of the customer; and

as a result of the authentication service successfully authenticating the cryptographic authentication information, configuring the computing resource service provider network device to route network traffic received from the customer network device through the dedicated physical network connection to one or more services of a computing resource service provider on the computer resource service provider network, the one or more services being different from the authentication service.

2. The computer-implemented method of claim 1, wherein the secret key is a private key from a public-private cryptographic key pair.

3. The computer-implemented method of claim 1, further comprising provisioning a network interface for the customer on the computing resource service provider

network device as a result of the authentication service successfully authenticating the cryptographic authentication information.

4. The computer-implemented method of claim 1, wherein the dedicated physical network connection is established based at least in part on a physical connection in a colocation center remote to the customer, the physical connection comprising one or more cables connected from a set of customer ports of the customer network device to a set of computing resource service provider ports of the computing resource service provider network device.

5. The computer-implemented method of claim 1, wherein:

the method further comprises receiving additional cryptographic authentication information from the customer network device one or more times over an amount of time; and

continued routing of the network traffic from the customer network device to the one or more services is contingent on successfully authenticating the additional cryptographic authentication information.

6. The computer-implemented method of claim 1, wherein the method is performed in accordance with an authentication protocol used by the customer network device and the computing resource service provider network device.

7. The computer-implemented method of claim 1, further comprising receiving, prior to transmitting the request to provide cryptographic authentication information, through a communications channel that lacks the computing resource service provider network device, the secret key of the customer.

8. A network device, comprising:

one or more communications ports configured to receive one or more signals from outside of the network device through physical network connections with other network devices, including a communications port that is connected to a provider network that includes one or more services including an authentication service and one or more services, the communications port configured to establish a dedicated physical network connection with a customer network device outside of the provider network;

one or more processors that are operatively coupled with the one or more communications ports; and

memory including instructions executable by the one or more processors that when executed by the one or more processors cause the one or more processors to:

forward cryptographic authentication information received over the dedicated physical network connection from the customer network device connected to at least one of the one or more communications ports to the authentication service that is operable to authenticate the cryptographic authentication information;

receive reconfiguration information, from the authentication service as a result of the authentication service having successfully authenticated the cryptographic authentication information, to enable the network device to forward data received through the dedicated physical network connection from the customer network device to the one or more services on the provider network; and

reconfigure the network device to forward data received through the communications port over the dedicated physical network connection from the customer network device to at least one of the one or more services on the provider network in accordance with the reconfiguration information.

9. The network device of claim 8, wherein the cryptographic authentication information received from the customer network device is generated based at least in part on a secret key of a customer.

10. The network device of claim 9, wherein the secret key is a private key from a public-private cryptographic key pair.

11. The network device of claim 8, wherein the instructions further cause the one or more processors to transmit the cryptographic authentication information, verifiable by the customer network device, from the authentication service to the customer network device.

12. The network device of claim 8, wherein the instructions further cause the one or more processors to forward additional cryptographic authentication information received from the customer network device to the authentication service one or more times over time.

13. The network device of claim 8, wherein the signals are received through one or more fiber-optic cables connected from the customer network device to the one or more communications ports.

14. The network device of claim 8, wherein the instructions further cause the one or more processors to provision a network interface for processing data from the customer network device, based at least in part on the reconfiguration information.

15. One or more non-transitory computer-readable storage media having collectively stored thereon instructions that, as a result of execution by one or more processors, cause operations to be performed, the operations comprising:

establishing a dedicated physical network connection between a computing resource service provider network device connected to a computer resource service provider network and a customer network device connected to a customer network separate from the computer resource service provider network device;

transmitting, from the computing resource service provider network device to the customer network device, through the dedicated physical network connection, a request for a customer to provide cryptographic authentication information for authenticating the customer network device;

receiving, at the computing resource service provider network device and from the customer network device, the cryptographic authentication information;

forwarding, from the computing resource service provider network device, the cryptographic authentication information to an authentication service that is operable to authenticate the cryptographic authentication information via verification based at least in part on a secret key of the customer; and

as a result of the authentication service successfully authenticating the cryptographic authentication information, configuring the computing resource service provider network device to route network traffic received from the customer network device through the dedicated physical network connection to one or more services of a computing resource service provider on the computer resource service provider network, the one or more services being different from the authentication service.

16. The one or more non-transitory computer-readable storage media of claim 15, wherein the secret key is a private key from a public-private cryptographic key pair.

17. The one or more non-transitory computer-readable storage media of claim 15, wherein the operations further comprise provisioning a network interface for the customer on the computing resource service provider network device as a result of the authentication service successfully authenticating the cryptographic authentication information.

18. The one or more non-transitory computer-readable storage media of claim 15, wherein the dedicated physical network connection is established based at least in part on a physical connection in a colocation center remote to the customer, the physical connection comprising one or more cables connected from a set of customer ports of the customer network device to a set of computing resource service provider ports of the computing resource service provider network device.

19. The one or more non-transitory computer-readable storage media of claim 15, wherein:

the operations further comprise receiving additional cryptographic authentication information from the customer network device one or more times over an amount of time; and

continued routing of the network traffic from the customer network device to the one or more services is contingent on successfully authenticating the additional cryptographic authentication information.

20. The one or more non-transitory computer-readable storage media of claim 15, wherein the operations are performed in accordance with an authentication protocol used by the customer network device and the computing resource service provider network device.

21. The one or more non-transitory computer-readable storage media of claim 15, wherein the operations further comprise receiving, prior to transmitting the request to provide cryptographic authentication information, through a communications channel that lacks the computing resource service provider network device, the secret key of the customer.

22. The one or more non-transitory computer-readable storage media of claim 15, wherein the operations further comprise:

receiving additional cryptographic authentication information from the customer network device; and

after receiving the additional cryptographic authentication information and as a result of failing to authenticate using the additional cryptographic authentication information, denying additional network traffic received from the customer network device through the dedicated physical network connection to the one or more services of a computing resource service provider on the computer resource service provider network.

23. The one or more non-transitory computer-readable storage media of claim 22, wherein denying the additional network traffic comprises transmitting, to the computing resource service provider network device over the dedicated physical network connection, reconfiguration information for denying transmission of the network traffic over the dedicated physical network connection from the customer network device to the one or more services of the computing resource service provider on the computer resource service provider network.

24. The one or more non-transitory computer-readable storage media of claim 15, wherein the operations further comprise:

obtaining second cryptographic authentication information different than the cryptographic authentication information and verifiable by the customer network device to authenticate the computing resource service provider; and

transmitting the second cryptographic authentication information to the computing resource service provider network device to the customer network device.

25. The one or more non-transitory computer-readable storage media of claim 15, wherein the dedicated physical network connection between the computing resource service provider network device and the customer network device is established in response to generation of a letter of authority, the letter of authority generated in response to a request from the customer to establish the dedicated physical network connection.