CLAIMS

~~What is claimed is:~~

1. A computing device comprising:

processing circuitry coupled to a memory, the processing circuitry and memory configured to implement:

a network function;

an external virtual domain for the network function, the external virtual domain connected to a public network and managed by a provider for the computing device; and

a virtual domain for the network function, the virtual domain separate from the external virtual domain, configured with a secure tunnel interface, connected to a customer network, and managed by a customer of the provider for the computing device,

wherein the external virtual domain implements a route-based virtual private network to forward encrypted network traffic, received from the public network via a secure tunnel, to the secure tunnel interface configured in the virtual domain, and

wherein the virtual domain is configured to decrypt the encrypted network traffic to generate network traffic and forward the network traffic to the customer network.

2. The computing device of claim 1,

wherein the virtual domain comprises a first virtual domain and the customer network comprises a first customer network,

wherein the processing circuitry and memory are further configured to implement:

a second virtual domain for the network function, the second virtual domain separate from the first virtual domain and the external virtual domain, and connected to a second customer network,

wherein the first virtual domain and the second virtual domain are configured with a virtual domain connection, and routing information or firewall rules, to cause the first virtual domain to forward selected network traffic, received from the customer network, to the second virtual domain for forwarding to the second customer network.

3. The computing device of claim 2, wherein the second customer network is a cloud service provider network.

4. The computing device of any of claims 2–3,

wherein the secure tunnel interface is a first secure tunnel interface,

wherein the second virtual domain is configured with a second secure tunnel interface,

wherein the external virtual domain implements the route-based virtual private network to forward other encrypted network traffic, received from the public network via a different secure tunnel, to the second secure tunnel interface in the second virtual domain, and

wherein the second virtual domain is configured to decrypt the other encrypted network traffic to generate other network traffic and forward the other network traffic to the second customer network.

5. The computing device of any of claims 1–4,

wherein the computing device is configured to limit, to the provider, authorization to configure the external virtual domain,

wherein the computing device is configured to allow the customer to configure the virtual domain.

6. The computing device of any of claims 1–5, wherein the network function is a virtualized network function.

7. The computing device of any of claims 1–6,

wherein the route-based virtual private network comprises a route that maps a prefix to the secure tunnel interface and applies the route to forward the encrypted network traffic to the secure tunnel interface configured in the virtual domain.

8. The computing device of any of claims 1–7, wherein the external virtual domain implements a virtual private network gateway.

9. The computing device of any of claims 1–8, wherein the virtual domain is configured to apply the network function to the network traffic prior to forwarding the network traffic to the customer network.

10. The computing device of any of claims 1–9,

wherein the virtual domain comprises one of a virtual routing and forwarding instance or a firewall domain that stores routing information received from the customer network, and

wherein the virtual domain is configured to apply the routing information to the network traffic to forward the network traffic to the customer network.

11. The computing device of any of claims 1–10,

wherein the customer network is connected to the virtual domain via a cloud exchange fabric, and

wherein the public network is connected to the external virtual domain via the cloud exchange fabric.

12. A method comprising:

receiving, by a computing device, configuration data defining:

an external virtual domain for a network function, the external virtual domain connected to a public network and managed by a provider for the computing device;

a virtual domain for the network function, the virtual domain separate from the external virtual domain, configured with a secure tunnel interface, connected to a customer network, and managed by a customer of the provider for the computing device;

forwarding, by the external virtual domain implementing a route-based virtual private network, encrypted network traffic, received from the public network via a secure tunnel, to the secure tunnel interface configured in the virtual domain;

decrypting, by the virtual domain, the encrypted network traffic to generate network traffic; and

forwarding, by the virtual domain, the network traffic to the customer network.

13. The method of claim 12, wherein the route-based virtual private network comprises a route that maps a prefix to the secure tunnel interface and applies the route to forward the encrypted network traffic to the secure tunnel interface configured in the virtual domain.

14. A computing device comprising:

processing circuitry coupled to a memory, the processing circuitry and memory configured to implement:

a network function;

a first virtual domain for the network function, the first virtual domain connected to a first customer network and managed by a first customer of a provider for the computing device;

a second virtual domain for the network function, the second virtual domain separate from the first virtual domain, connected to a second customer network, and managed by a second customer of ~~a~~the provider for the computing device; and

a virtual domain connection enabling network traffic forwarding from the first virtual domain to the second virtual domain, the virtual domain connection configured by the provider for the computing device.

15. The computing device of claim 14,

wherein the virtual domain connection comprises a first virtual domain connection, and

wherein the processing circuitry and memory are further configured to implement:

an external virtual domain for the network function, the external virtual domain connected to a public network, managed by the~~a~~ provider for the computing device, and separate from the first virtual domain and the second virtual domain; and

a second virtual domain connection enabling network traffic forwarding from the external virtual domain to the second virtual domain, the second virtual domain connection configured by the provider for the computing device.

16. The computing device of any of claims 14–15, wherein the second virtual domain is configured to apply the network function to second received network traffic prior to forwarding the second received network traffic to the second customer network.

17. The computing device of any of claims 14–16, wherein the first virtual domain is configured to apply the network function to received network traffic prior to forwarding the received network traffic to the second virtual domain.

18. The computing device of any of claims 14–17, wherein the network function is a virtualized network function.

19. The computing device of any of claims 14–18,

wherein the computing device is configured to limit, to the provider, authorization to configure the virtual domain connection, and

wherein the computing device is configured to allow the first customer to configure the first virtual domain.

20. The computing device of any of claims 14–18, wherein the external virtual domain implements a virtual private network gateway.~~network function is a virtualized network function.~~