WHAT IS CLAIMED IS:

1. A system, comprising:

a configuration manager of a provider network, wherein the configuration manager is implemented via one or more computers comprising one or more respective hardware processors and memory;

a virtualization management component (VMC) of an instance host comprising one or more hardware processors and memory, wherein a first compute instance of a first isolated virtual network (IVN) established on behalf of a client is instantiated at the instance host, and wherein the first compute instance has a private network address selected by the client; and

a tunneling intermediary comprising one or more hardware processors and memory;

wherein the configuration manager is configured to store a first metadata entry representing a designation of a first private alias endpoint (PAE) as a routing target for packets originating at the first IVN and directed to a particular service, wherein the packets are to be delivered to the particular service without indicating a publicly-advertised network address as a source address;

wherein the VMC is configured to transmit to the tunneling intermediary, based at least part on an examination of the first metadata entry, a first encapsulation packet derived from a baseline packet intercepted at the VMC, wherein the baseline packet is generated at the first compute instance and directed to a publicly-advertised network address of the particular service; and

wherein the tunneling intermediary is configured to:

generate, in accordance with a tunneling protocol, a second encapsulation packet from the first encapsulation packet, wherein the second encapsulation packet includes a header component indicating the first IVN as a source IVN; and

transmit the second encapsulation packet to a first node of one or more nodes of the particular service, wherein the first node is configured to (a) determine, from the second encapsulation packet, an identifier of the first

IVN and the private network address, and (b) initiate one or more operations to fulfill a service request indicated in the baseline packet.

2. The system as recited in claim 1, wherein the second encapsulation packet is formatted in accordance with IPv6 (version 6 of the Internet Protocol), and wherein the baseline packet is formatted in accordance with IPv4 (version 4 of the Internet Protocol).

3. The system as recited in claim 1, wherein the particular service supports a plurality of operation types on a plurality of objects, wherein one or more of (a) the first node of the particular service or (b) the VMC are configured to:

initiate a determination, prior to an initiation of the one or more operations, of whether the service request is in compliance with a first access control policy assigned to the first PAE, wherein the first access control policy indicates, with respect to requests submitted using the first PAE as a routing target, one or more of: (a) a permitted operation type of the plurality of operation types, (b) a prohibited operation type of the plurality of operation types, (c) a time interval during which a particular operation type of the plurality of operation types is permitted, or (d) a particular object of the plurality of objects on which a particular operation type of the plurality of operation types is permitted.

4. The system as recited in claim 1, wherein the configuration manager is further configured to:

designate a second PAE as a routing target for additional packets originating at the first IVN, wherein the additional packets is to be delivered to a different service.

5. The system as recited in claim 1, wherein the configuration manager is further configured to:

assign, at the request of the client, the private network address to a second compute instance established at a second IVN of the client;

establish a second PAE to be used for routing traffic originating at the second IVN and directed to the particular service;

and wherein the first node of the service is configured to:

determine, based on an examination of a particular encapsulation header generated by the tunneling intermediary, whether a particular baseline packet extracted at the first node was generated at the first compute instance or at the second compute instance.

6. A method, comprising:

determining, at a tunneling intermediary of a provider network, that a first private alias endpoint (PAE) has been designated as a routing target for traffic originating at a first isolated virtual network (IVN) established within the provider network on behalf of a client, wherein the traffic is to be delivered to a particular publicly-accessible service implemented in the provider network;

receiving, at the tunneling intermediary, a baseline packet directed from a first compute instance of the first IVN to a publicly-advertised network address of the particular publicly-accessible service for which the first PAE is designated as the routing target; generating, at the tunneling intermediary, an encapsulation packet comprising (a) contents of the baseline packet and (b) an indication of the first IVN as a source IVN; and

transmitting, from the tunneling intermediary to a first node of the particular service without traversing network links outside the provider network, the encapsulation packet.

7. The method as recited in claim 6, wherein the encapsulation packet is formatted in accordance with IPv6 (version 6 of the Internet Protocol), and wherein the baseline packet is formatted in accordance with IPv4 (version 4 of the Internet Protocol).

8. The method as recited in claim 6, wherein the particular service supports a plurality of operation types on a plurality of objects, further comprising:

receiving, at a configuration manager of the first IVN from the client, a request to apply a first access control policy to the first PAE, wherein the first access control policy indicates, with respect to requests submitted using the first PAE as a routing

target, one or more of: (a) a permitted operation type of the plurality of operation types, (b) a prohibited operation type of the plurality of operation types, (c) a time interval during which a particular operation type of the plurality of operation types is permitted, or (d) a particular object of the plurality of objects on which a particular operation type of the plurality of operation types is permitted; and

verifying, prior to executing a first operation in accordance with a particular request indicated in the baseline packet, that the first operation is permitted by the first access control policy.

9. The method as recited in claim 6, further comprising:

designating a second PAE as a routing target for additional traffic originating at the first IVN, wherein the additional traffic is to be delivered to a different service.

10. The method as recited in claim 6, wherein the first compute instance has a particular private IP address assigned to it at the request of the client, further comprising:

establishing a second IVN on behalf of the client, wherein the second IVN includes a second compute instance;

assigning, at the request of the client, the particular private IP address to the second compute instance;

establishing a second PAE to be used for routing traffic originating at the second IVN and directed to the particular service;

determining, at a particular node of the particular service based on examination of an encapsulation header generated by the tunneling intermediary, whether a particular baseline packet received at the particular node was generated at the first compute instance to which the particular private IP address was assigned, or at the second compute instance to which the particular private IP address was assigned.

11. The method as recited in claim 6, wherein the encapsulation packet is formatted in accordance with a proprietary tunneling protocol implemented at the provider network.

12. The method as recited in claim 6, wherein the encapsulation packet comprises a header including a representation of an identifier of the first PAE.

13. The method as recited in claim 6, further comprising:

receiving, at a configuration manager of the provider network via a programmatic interface, a request from the client to generate the first PAE; and

storing, by the configuration manager in response to the request, a metadata entry representing the first PAE.

14. The method as recited in claim 6, further comprising:

receiving, at a configuration manager of the provider network via a programmatic interface, a request to register a different service for access using a PAE; and

adding, by the configuration manager in response to the request, the different service to a collection of services from which a particular service can be selected by the client for association with a particular PAE.

15. The method as recited in claim 14, wherein the different service is implemented by a different client of the provider network using a set of resources of the provider network, further comprising:

establishing one or more front-end nodes for the different service, including a particular front-end node configured to extract contents of encapsulation packets derived from baseline packets directed to the different service.

16. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors implements a tunneling intermediary of a provider network, wherein the tunneling intermediary is configured to:

identifying a first private alias endpoint (PAE) designated as a routing target for traffic directed to a particular service implemented in the provider network from a first isolated virtual network (IVN) established at a provider network on behalf of a client;

receive a baseline packet generated at a first compute instance of the first IVN, wherein the baseline packet indicates a public IP (Internet Protocol) address of the particular service for which the first PAE is designated as the routing target as its destination address;

generate, in accordance with a selected tunneling protocol, an encapsulation packet comprising (a) at least a portion of contents of the baseline packet and (b) a header component indicating the first IVN as a source IVN; and

transmit the encapsulation packet to a first node of the particular service without traversing network links outside the provider network.

17. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the encapsulation packet is formatted in accordance with IPv6 (version 6 of the Internet Protocol), and wherein the baseline packet is formatted in accordance with IPv4 (version 4 of the Internet Protocol).

18. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the tunneling intermediary is further configured to:

receive, in accordance with a designation of a second PAE as a routing target for traffic directed to a different service from a first IVN, a representation of a second baseline packet generated at a second compute instance of the first IVN, wherein the second baseline packet indicates a public IP address of the different service as its destination address;

generate, in accordance with the selected tunneling protocol, a second encapsulation packet comprising (a) at least a portion of contents of the second baseline packet and (b) a header component indicating the first IVN as a source IVN; and

transmit the second encapsulation packet to a different node of the different service.

19. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the first encapsulation packet includes an indication of a private IP address of the first compute instance, wherein the tunneling intermediary is further configured to:

receive, in accordance with a designation of a second PAE as a routing target for traffic directed to the particular service from a second IVN established on behalf of the client, a representation of a second baseline packet generated at a second compute instance of the second IVN, wherein the second baseline packet indicates the public IP address of the particular service as its destination address;

generate, in accordance with the selected tunneling protocol, a second encapsulation packet comprising (a) at least a portion of contents of the second baseline packet (b) a header component indicating the second IVN as a source IVN and (c) an indication of the private IP address; and

transmit the second encapsulation packet to the first node of the particular service, wherein the first node of the particular service is configured to determine, based on an examination of the second encapsulation packet, whether the second baseline packet was generated at the first compute instance or the second compute instance.

20. The non-transitory computer-accessible storage medium as recited in claim 16, wherein the encapsulation packet comprises a header including a representation of an identifier of the first PAE.