CLAIMS

1. A method comprising:

causing a first encapsulation tunnel to be established between a tunnel aggregator device and a first customer routing device;

receiving, at the tunnel aggregator device and from a first managed security router of a provider network, a first plurality of packets addressed to a first customer endpoint;

encapsulating, by the tunnel aggregator device, the first plurality of packets;

providing the encapsulated first plurality of packets to the first customer routing device using the first encapsulation tunnel;

receiving, at the tunnel aggregator device and from a second managed security router of the provider network, a second plurality of packets addressed to the first customer endpoint;

encapsulating, by the tunnel aggregator device, the second plurality of packets; and

providing the encapsulated second plurality of packets to the first customer routing device using the first encapsulation tunnel.

2. The method of claim 1, wherein:

the first plurality of packets are received at the tunnel aggregator device over a clean return virtual routing and forwarding system of the provider network in unencapsulated form; and/or

the first plurality of packets and the second plurality of packets are received at the tunnel aggregator device through a premise edge router co-located with the tunnel aggregator device.

3. The method of claim 1 or 2, wherein:

the tunnel aggregator device is logically closer to the first customer routing device than either of the first managed security router or the second managed security router; and/or

the method further comprising:

causing a second encapsulation tunnel to be established between the tunnel aggregator device and a second customer routing device;

receiving, at the tunnel aggregator device and from the first managed security router of the provider network, a third plurality of packets addressed to a second customer endpoint;

encapsulating, by the tunnel aggregator device, the third plurality of packets; and

providing the encapsulated third plurality of packets to the second customer routing device using the second encapsulation tunnel.

4. The method of any preceding claim, wherein the tunnel aggregator device uses either:

Generic Routing Encapsulation (GRE) to provide the first plurality of packets and the second plurality of packets to the first customer endpoint; or

Internet Protocol Security (IPsec) to provide the first plurality of packets and the second plurality of packets to the first customer endpoint.

5. A method comprising:

receiving, at a first managed security router of a provider network, a first plurality of packets addressed to a first customer endpoint;

providing the first plurality of packets to one or more threat mitigation devices;

receiving, at the first managed security router and from the one or more threat mitigation devices, a first plurality of filtered packets associated with the first plurality of packets; and

providing, based on a configuration of the first managed security router, the first plurality of filtered packets to a first tunnel aggregator device for transmission to the first customer endpoint.

6. The method of claim 5, further comprising:

receiving, at the first managed security router, customer packet routing instructions, wherein the configuration of the first managed security router is at least partially based on the customer packet routing instructions.

7. The method of claim 6, wherein the customer packet routing instructions includes an indication that the first plurality of filtered packets should be provided to the first customer endpoint via an encapsulation tunnel.

8. The method of claim 6 or 7, further comprising selecting the first tunnel aggregator device from a plurality of tunnel aggregator devices, wherein the first tunnel aggregator device is selected by the first managed security router based at least partially on the customer packet routing instructions.

9. The method of any one of claims 5 to 8, wherein the first plurality of filtered packets is provided to a provider edge router over a clean return virtual routing and forwarding system of the provider network in unencapsulated form.

10. The method of any one of claims 5 to 9, further comprising selecting the first tunnel aggregator device from a plurality of tunnel aggregator devices, wherein the first tunnel aggregator device is selected from a plurality of tunnel aggregator devices based on the first tunnel aggregator device being logically closer to the first customer endpoint.

11. A system, comprising:

at least one processor; and

memory, operatively connected to the at least one processor and storing instructions that, when executed by the at least one processor, cause the system to perform a method comprising:

causing a first encapsulation tunnel to be established between a tunnel aggregator device and a first customer routing device;

receiving, at a tunnel aggregator device and from a first managed security router of a provider network, a first plurality of packets addressed to a first customer endpoint;

encapsulating, by the tunnel aggregator device, the first plurality of packets;

providing the encapsulated first plurality of packets to the first customer routing device;

receiving, at the tunnel aggregator device and from a second managed security router of the provider network, a second plurality of packets addressed to the first customer endpoint;

encapsulating, by the tunnel aggregator device, the second plurality of packets; and

providing the encapsulated second plurality of packets to the first customer routing device using the first encapsulation tunnel.

12. The system of claim 11, wherein the first plurality of packets and the second plurality of packets are received at the tunnel aggregator device over a clean return virtual routing and forwarding system of the provider network in unencapsulated form.

13. The system of claim 11 or 12, wherein:

the tunnel aggregator device is logically closer to the first customer routing device than either of the first managed security router or the second managed security router; and/or

the system further comprising:

causing a second encapsulation tunnel to be established between the tunnel aggregator device and a second customer routing device;

receiving, at the tunnel aggregator device and from the first managed security router of the provider network, a third plurality of packets addressed to a second customer endpoint;

encapsulating, by the tunnel aggregator device, the third plurality of packets; and

providing the encapsulated third plurality of packets to the second customer endpoint.

14. The system of any one of claims 11 to 13, wherein:

the first plurality of packets and the second plurality of packets are received at the tunnel aggregator device through a premise router co-located with the tunnel aggregator device; and/or

the tunnel aggregator device uses Generic Routing Encapsulation (GRE) to provide the first plurality of packets and the second plurality of packets to the first customer endpoint.

15. The system of any one of claims 11 to 14, wherein a configuration of the first managed security router is at least partially based on customer packet routing instructions.