

CLAIMS

What is claimed is:

1. An exchange comprising:
 - a first virtual network for switching mixed traffic from one or more networks to one or more Distributed Denial of Service (DDoS) scrubbing centers, wherein the mixed traffic includes dirty traffic that represents DDoS traffic and clean traffic that represents non-DDoS traffic; and
 - a second virtual network for switching the clean traffic from the one or more DDoS scrubbing centers to the one or more networks,
 - wherein the exchange is configured to receive the mixed traffic from the one or more networks and switch, using the first virtual network, the mixed traffic to a selected DDoS scrubbing center of the one or more DDoS scrubbing centers, and
 - wherein the exchange is configured to receive the clean traffic from the selected DDoS scrubbing center and switch, using the second virtual network, the clean traffic to the one or more networks.
2. The exchange of claim 1,
 - wherein the first virtual network is a dirty virtual local area network (VLAN) for switching the mixed traffic, and
 - wherein the second virtual network is a clean VLAN for switching the clean traffic.
3. The exchange of claim 2,
 - wherein the dirty VLAN is associated with a first set of ports of the exchange for receiving the mixed traffic from the one or more networks and sending the mixed traffic to the one or more DDoS scrubbing centers, and
 - wherein the clean VLAN is associated with a second set of ports of the exchange for receiving clean traffic from the one or more DDoS scrubbing centers and sending the clean traffic to the one or more networks.

4. The exchange of claim 1, further comprising:
 - a policy unit configured to instruct one or more provider edge devices of the one or more DDoS scrubbing centers to advertise, to the one or more networks, a first route advertisement specifying the one or more provider edge devices as a next hop for a path on the first virtual network to reach a destination of the mixed traffic,
 - the policy unit further configured to instruct a gateway device of the one or more networks to advertise, to the one or more DDoS scrubbing centers, a second route advertisement to advertise the gateway device as a next hop for a path on the second virtual network to reach a destination of the clean traffic.
5. The exchange of claim 4, further comprising:
 - one or more network devices of the exchange configured to:
 - receive, from the one or more provider edge devices, the first route advertisement;
 - in response to receiving the first route advertisement, associate the first virtual network with a first set of ports of the one or more network devices of the exchange for receiving the mixed traffic from the one or more networks and sending the mixed traffic to the one or more DDoS scrubbing centers via the one or more provider edge devices;
 - send, to the gateway device, the first route advertisement using the first virtual network;
 - receive, from the gateway device, the second route advertisement;
 - in response to receiving the second route advertisement, associate the second virtual network with a second set of ports of the one or more network devices of the exchange for receiving the clean traffic from the one or more DDoS scrubbing centers and sending the clean traffic to the one or more networks via the gateway device; and
 - send, to the one or more provider edge devices, the second route advertisement using the second virtual network.

6. The exchange of claim 5, wherein the network device of the exchange is further configured to:

- receive the mixed traffic from the one or more networks;
- switch, using the first virtual network, the mixed traffic from the one or more networks to the selected DDoS scrubbing center;
- receive the clean traffic from the selected DDoS scrubbing center; and
- switch, using the second virtual network, the clean traffic from the selected DDoS scrubbing center to the one or more networks.

7. A method comprising:

- configuring, by a policy unit for an exchange, the exchange to implement a first virtual network for switching mixed traffic from one or more networks to one or more Distributed Denial of Service (DDoS) scrubbing centers, wherein the mixed traffic includes dirty traffic that represents DDoS traffic and clean traffic that represents non-DDoS traffic; and

- configuring, by the policy unit, the exchange to implement a second virtual network for switching the clean traffic from the one or more DDoS scrubbing centers to the one or more networks.

8. The method of claim 7,

- wherein the first virtual network is a dirty virtual local area network (VLAN) for switching the mixed traffic, and

- wherein the second virtual network is a clean VLAN for switching the clean traffic.

9. The method of claim 8,
wherein configuring the exchange to implement the first virtual network further comprises associating the dirty VLAN with a first set of ports of the exchange for switching the mixed traffic from the one or more networks to the one or more DDoS scrubbing centers, and
wherein configuring the network device of the exchange to implement the second virtual network further comprises associating the clean VLAN with a second set of ports of the exchange for switching the clean traffic from the one or more DDoS scrubbing centers to the one or more networks.
10. The method of claim 7, further comprising:
instructing, by the policy unit, one or more provider edge devices of the one or more DDoS scrubbing centers to advertise, to the one or more networks, a first route advertisement specifying the one or more provider edge devices as a next hop for a path on the first virtual network to reach a destination of the mixed traffic; and
instructing, by the policy unit, a gateway device of the one or more networks to advertise, to the one or more DDoS scrubbing centers, a second route advertisement specifying the gateway device as a next hop for a path on the second virtual network to reach a destination of the clean traffic.

11. The method of claim 10, further comprising:
- receiving, by the exchange and from the one or more DDoS scrubbing centers, the first route advertisement;
 - in response to receiving the first route advertisement, associating, by the exchange, the first virtual network with a first set of ports of the exchange for receiving the mixed traffic from the one or more networks and sending the mixed traffic to the one or more DDoS scrubbing centers via the one or more provider edge devices;
 - sending, by the exchange and to the one or more networks, the first route advertisement using the first virtual network;
 - receiving, by the network device of the exchange and from the one or more networks, the second route advertisement;
 - in response to receiving the second route advertisement, associating, by the network device of the exchange, the second virtual network with a second set of ports of the exchange for receiving the clean traffic from the one or more DDoS scrubbing centers and sending the clean traffic to the one or more networks via the gateway device; and
 - sending, by the exchange and to the one or more DDoS scrubbing centers, the second route advertisement using the second virtual network.
12. The method of claim 7, further comprising:
- receiving, by the exchange, the mixed traffic from the one or more networks;
 - switching, by the exchange and using the first virtual network, the mixed traffic from the one or more networks to a selected DDoS scrubbing center of the one or more DDoS scrubbing centers;
 - receiving, by the exchange, the clean traffic from the selected DDoS scrubbing center; and
 - switching, by the exchange and using the second virtual network, the clean traffic from the selected DDoS scrubbing center to the one or more networks.

13. A system comprising:
 - one or more networks connected to an exchange via a gateway device;
 - one or more Distributed Denial of Service (DDoS) scrubbing centers connected to the exchange via one or more provider edge devices;
 - the exchange; and
 - a policy unit for the exchange, wherein the policy unit is configured to:
 - configure the exchange to implement a first virtual network for switching mixed traffic from the one or more networks to a selected DDoS scrubbing center of the one or more DDoS scrubbing centers, wherein the mixed traffic includes dirty traffic that represents DDoS traffic and clean traffic that represents non-DDoS traffic; and
 - configure the exchange to implement a second virtual network for switching the clean traffic from the one or more DDoS scrubbing centers to the one or more networks.
14. The system of claim 13, wherein the exchange is configured to:
 - receive the mixed traffic from the one or more networks;
 - switch, in response to receiving the mixed traffic, using the first virtual network, the mixed traffic to the selected DDoS scrubbing center;
 - receive the clean traffic from the selected DDoS scrubbing center; and
 - switch, in response to receiving the clean traffic, using the second virtual network, the clean traffic to the one or more networks.

15. The system of claim 13,
wherein the first virtual network is a dirty virtual local area network (VLAN) for switching the mixed traffic, and
wherein the second virtual network is a clean VLAN for switching the clean traffic.
16. The system of claim 15, wherein the exchange is further configured to:
associate the dirty VLAN with a first set of ports of the exchange for receiving the mixed traffic from the one or more networks to send the mixed traffic to the one or more DDoS scrubbing centers, and
associate the clean VLAN with a second set of ports of the exchange for receiving clean traffic from the one or more DDoS scrubbing centers to send the clean traffic to the one or more networks.
17. The system of claim 13, wherein the policy unit is further configured to:
instruct the one or more provider edge devices of the one or more DDoS scrubbing centers to advertise, to the one or more networks, a first route advertisement specifying the one or more provider edge devices as a next hop for a path on the first virtual network to reach a destination of the mixed traffic; and
instruct the gateway device of the one or more networks to advertise, to the one or more DDoS scrubbing centers, a second route advertisement specifying the gateway device as a next hop for a path on the second virtual network to reach a destination of the clean traffic.

18. The system of claim 17, wherein the network device of the exchange is further configured to:

- receive, from the one or more DDoS scrubbing centers, the first route advertisement;

- in response to receiving the first route advertisement, associate the first virtual network with a first set of ports of the exchange for receiving the mixed traffic from the one or more networks and sending the mixed traffic to the one or more DDoS scrubbing centers via the one or more provider edge devices;

- send, to the one or more networks, the first route using the first virtual network;

- receive, from the one or more networks, the second route advertisement;

- in response to receiving the second route advertisement, associate the second virtual network with a second set of ports of the exchange for receiving the clean traffic from the one or more DDoS scrubbing centers and sending the clean traffic to the one or more networks via the gateway device; and

- send, to the one or more DDoS scrubbing centers, the second route using the second virtual network.

19. The system of claim 17, wherein the gateway device comprises:

- a dirty virtual routing and forwarding (VRF) instance associated with the first route advertisement for routing the mixed traffic from the one or more networks to the one or more DDoS scrubbing centers via the exchange; and

- a clean VRF instance associated with the second route advertisement for routing the clean traffic from the one or more DDoS scrubbing centers via the exchange to the one or more networks.

20. The system of claim 19, wherein the gateway device is configured to:

- receive the mixed traffic from the one or more networks;

- send, in response to receiving the mixed traffic, the mixed traffic including a virtual local area network (VLAN) identifier or VLAN tag associated with the first virtual network,

- receive, from the network device of the exchange, the clean traffic including a VLAN identifier or VLAN tag associated with the second virtual network; and

- send the clean traffic to the one or more networks.