Integrate Cisco Secure Threat Defense Virtual with Megaport - Solution Brief

First Published: 2024-05-12

Deploy the Threat Defense Virtual on Megaport

This guide brief provides information on deploying the Cisco Secure Threat Defense Virtual on Megaport.

Overview

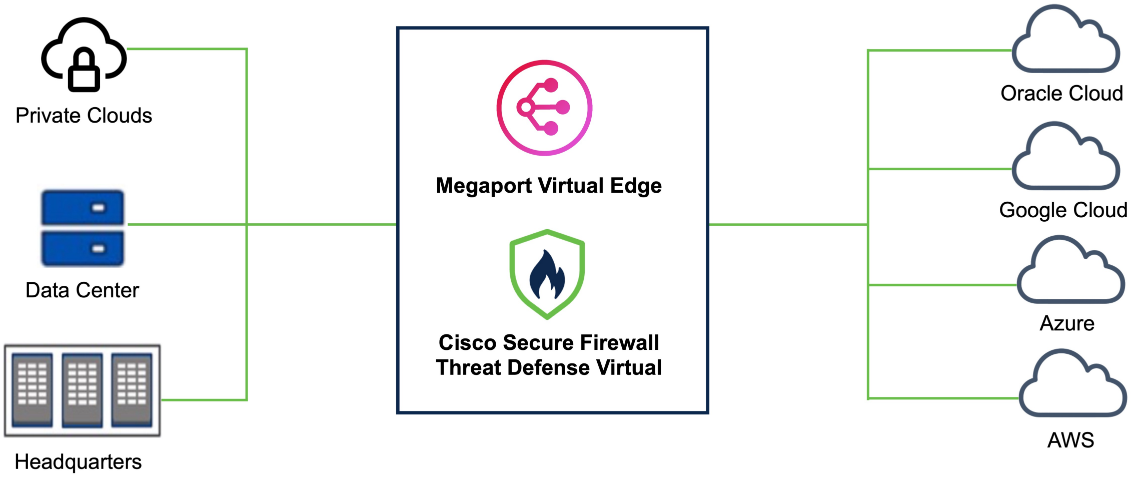
Business critical data can originate from diverse sources ranging from multiple public clouds, private clouds, and internal servers to a remote employee's device. Securing each data entity individually is time consuming and challenging due to lack of compliance between all the data points. With the increase in such use cases, you must be able to deploy the firewall quickly and securely at your network edge in a way that provides scalability and flexibility.

Megaport Virtual Edge (MVE) is an on-demand Network Function Virtualization (NFV) service on Megaport's Software Defined Network (SDN), with a global reach of more than 280 cloud on-ramps and more than 800 data centers. The MVE enables you to secure branch-to-cloud, cloud-to-cloud, and branch-to-branch connectivity over private networks, Layer-2 networks with dedicated bandwidth, and low latency. From the Megaport portal, you can deploy SD-WAN gateways, virtual routers, transit gateways, and virtual firewalls at the network edge.

From Secure Firewall version 7.2.8, you can deploy the Threat Defense Virtual as an MVE that enables you to create a security service chain in your hybrid and multi-cloud workflows; and deploy a single point solution for personal devices, data centers, and the closest availability zones of your cloud platforms such as AWS, Azure, and GCP. This integration reduces data transit over potentially unsecure networks and allows you to seamlessly implement your security solution without worrying about problems with robustness and scalability.

Use the Megaport portal to deploy the Threat Defense Virtual and connect all your data centers to multi-cloud applications in a single place. All the data packets are routed using Megaport's private global network. After deployment, the Threat Defense Virtual can be managed by either the on-box Firewall Device Manager, the Cloud-Delivered Firewall Management Center, or the On-Premises Firewall Management Center.

Figure 1: High-level Sample Topology



Use Cases

Cisco Threat Defense Virtual deployed as a Megaport Virtual Edge (MVE) can be used for scenarios ranging from securing traffic from your data center to a multicloud architecture to securing traffic transiting between multiple public clouds. You can use up to 25 connectors with the MVE to connect to your chosen environment.

Multicloud Deployment

Deploying the Cisco Threat Defense Virtual as an MVE enables you to securely route all traffic through the Threat Defense Virtual while not dealing with the complex task of creating a dedicated security solution for multiple cloud providers. It not only acts as a single-point solution but also addresses gaps in interoperability and user skill between multiple public cloud platforms. Megaport uses its end-to-end private global routing network to ensure a robust multi-cloud network architecture.

Hybrid Cloud Deployment

Similar to multicloud architecture, your organization can also deploy the Cisco Threat Defense Virtual as an MVE to ensure that the traffic between your private data center and cloud architecture is secure. With the help of Megaport’s global network, you can deploy the Threat Defense Virtual in a location that is geographically closer to your HQ, resulting in high performance and low latency.

How to Deploy the Threat Defense Virtual on Megaport

For information on how to deploy the Threat Defense Virtual on Megaport, see Deploy the Threat Defense Virtual on Megaport.

Additional Resources

- Cisco Secure Firewall

- Cisco Secure Firewall Threat Defense Virtual