Questions and Answers

Published: 2019-07-11

Common Questions and Answers	
Does Nimitz operate in Bridge Mode or Routing Mode?	Nimitz is required to run in **Routing Mode** for it's **WAN** facing interface, in order to operate and perform **Ingress** filtering. You may bridge the **LAN** facing interface if that meets your networks requirements.
Does Nimitz operate in kernel or user mode.	**User mode.**
How does Nimitz Work?	Nimitz operates at layers 3/4 (OSI Model) of the protocol stack to eliminate DDoS attacks at layers 3/4/7. It achieves this via our proprietary software that uses a **novel** form of **signature detection** that is **unique to our product**.Without violating a packets integrity or security.
Does Nimitz perform both ingress and egress filtering?	**No**, Currently Nimitz **only performs Ingress filtering**, due to additional complexities. Egress filtering is something that we may consider deploying in the future on a case by case basis.
Am I required to purchase both the hardware and software or can I assemble my own hardware?	**Yes**, you are required to purchase the hardware configured with Nimitz proprietary software.
Can I make my own custom configurations to the hardware?	**No.** Any custom modifications to the hardware outside of purchase void all warranties. In addition to this clients are provided access to a restricted environment via telnet/console cable in which to configure Nimitz. Allowing only for basic routing operations.
How are you able to keep the costs of your security appliances so low? When compared to industry leaders.	We couple our software with **commodity hardware.** Commodity hardware opens us up to the opportunity of using relatively powerful components (e.g. CPU's) that are readily available. That would normally be utilized for multiple, non-related tasks. Instead we repurpose that hardware and optimize it for a single dedicated purpose.
What happens if I am hit with a DDoS attack that you have not identified?	If any client is hit with a DDoS attack that Nimitz has not identified or a new one has been developed then we will simply require a **Packet Capture** of that attack. Following which point we will analyze it and update all clients units via cloud. Thus allowing for continuous upgrades.
Why do you provide protection in packets per second (pps) rather than Gbps?	The simple answer to that is that modern networks are relatively high bandwidth. This makes it difficult for most malicious agents to launch an attack against a network or organization that will overwhelm their pipe and result in down time. For example ~81% of DDoS attacks in 2018 were under 1G with ~86% under <5G, according to research done by Corero Network Security. So if you have a network that is capable of handling 10G of throughput but is operating at 40% capacity, you can still handle 6G of traffic between endpoints. But still experience performance degredation at endpoints, due to the number and contents of those packets reaching your endpoint that fall within that <6G range. This is because not all bandwidths are made equal. Eventually a packet has to reach a point where it is processed. Attackers can craft packets by modifying their sizes and flags to attack endpoints/ nodes along a path regardless of bandwidth. Preferring to tie up system resources through greater CPU hardware utilization. e.g. A 2mpps = 1G Syn Flood can be more devastating to a networks hardware than a 1mpps = 2G Syn Flood.
Further Questions?	Please email us at **info@nimitz.ca**