

How Does NETSCOUT DDoS Protection Work Within a Customer's Network?

NETSCOUT's Anti DDoS Solutions

As the global cyber threat landscape continues to evolve, NETSCOUT's Arbor Anti-DDoS solution has been protecting the world's largest and most demanding networks for more than a decade. Also, mitigation and prevention techniques became a lot smarter, due to advancements in DDoS cybersecurity solutions and allow multiple deployment scenarios in customer networks. All NETSCOUT's Anti DDoS solutions share the same principle of detecting attacks based on continuously monitoring clients traffic behavior. In the case of a DDoS attack the malicious traffic is filtered and the clean/wanted traffic is forwarded to its desired destination. The main components of the solution offered within the Cisco SolutionPlus program are NETSCOUT® Arbor Edge Defense (AED) and Arbor Sightline/Threat Mitigation System (TMS).

Arbor Edge Defense (AED)

Arbor Edge Defense (AED) provides inline security deployed at the network perimeter. AED's unique position inline, in front of the protected assets, its stateless packet processing engine and the continuous reputation-based threat intelligence enable it to automatically detect and stop both inbound threats and outbound communication from internal compromised hosts. Top customer use cases for AED are:

SD-WAN

NETSCOUT vAED runs on a Cisco 4000 Family Integrated Services Router (ISR) on a UCS-E Series server card. As a VNF NETSCOUT vAED provides Anti-DDoS security to Cisco's converged architecture.

Software-Defined Branch (SD-Branch)

NETSCOUT vAED runs as a VM on a Cisco ENCS family compute appliance. It provides DDoS protection as part of Cisco's SD-Branch.

Unified Data Center

In the Datacenter NETSCOUT vAED is deployed as virtual machine on a Cisco UCS Series server. Integrating NETSCOUT DDoS protection provides an additional level of security to Cisco's Unified Data Center.

Sightline/TMS

NETSCOUT Sightline is mainly deployed in complex network topologies. It analyzes various forms of network telemetry to transform raw data into business intelligence. Working in conjunction with our Arbor Sightline solution, which provides visibility and threat detection, Arbor Threat Mitigation System (TMS) surgically removes DDoS attack traffic from your network without disrupting key network services.

Besides protecting your network and services by detecting and mitigating DDoS attacks, NETSCOUT's Arbor DDoS solution will provide you with valuable real-time information about top-talkers, applications, and countries. Regular reports keep you informed about incidents and developments in your network for given period of time. NETSCOUT Sightline/TMS software is designed to protect your own network as well as offer Anti-DDoS services to your customers. A granular user management with customizable dashboard enables Anti DDoS as a managed security service to increase the business value of NETSCOUT Sightline/TMS.