Radware Helps A Telecommunications Giant Bolster Their Mobile Network Security

A global tier-one service provider's Latin American operations, which has a presence in 90% of Mexico and includes 19 million subscribers, has adopted Radware's DDoS attack defense and mitigation services as part of a multi-million dollar deal. Through its Cisco OEM relationships, superior technology, technical expertise, and responsiveness to customer needs, Radware was able to displace a competitive incumbent and provide an advanced security solution that helped this company bolster their security in the face of increasing, more complex threats.

The service provider selected Radware to identify and mitigate anomalies from infected user equipment, such as handsets and IoT devices, and protect data center infrastructure within its private cloud using a DDoS solution that is powered by Radware's DefensePro, DefenseFlow, and APSolute Vision products and services.

THE CHALLENGE

With malicious threats on the rise, global service providers must take proactive measures to bolster their security, shore up their infrastructure, and stay ahead of dangerous cyberattacks. This telecommunications company's Latin American operation was not completely satisfied with their existing DDoS solution, which presented an opportunity for a joint Radware-Cisco proposal.

The company was seeking to improve their security through an advanced detection and mitigation solution that would increase their mitigation capacity, allow for better service

restoration capability, and improve protection against anomalies from infected user equipment, such as mobile handsets and IoT devices. With high-volume outbound and inbound traffic coming from their roaming partner, this company needed a solution that inspects this traffic for malicious behavior, alerts of any anomalies, and eventually automatically mitigates any cyberattacks that arise.

This company was also looking to protect data center infrastructure within their private cloud to prevent network latency while maximizing availability of the internal network resources.

THE SOLUTION

The telecommunications company realized that a joint Radware/Cisco offering would satisfy their complex needs and allow them to achieve a security solution that encompassed multiple use cases. The initial use case was centered around providing mobile network protection that was implemented across two phases.

The first phase focused on inspecting outbound and inbound traffic within the mobile packet core for communications between the radio access network and remote roaming partners. If any anomalies or malicious behaviors are detected within traffic coming from user equipment, such as mobile handsets and IOT devices, this service provider's System Operations Center (SOC) team is immediately alerted. Radware's security products are currently being used at six sites to inspect GTP tunnels and look for malicious behavior within this traffic.

The second phase, which is currently in the implementation process, will be centered around mitigation. The service provider will use Radware DefensePro and DefenseFlow to detect malicious behavior and automatically mitigate it by blocking detected threats at the Cisco router. DefensePro is an on-premise DDoS mitigation appliance that utilizes behavioral-based technology to automatically detect and mitigate existing and zero-day attacks in real time without manual intervention.

DefenseFlow is used to orchestrate attack lifecycle management across networks and will collect measurements and statistics from various network elements and apply behavioral algorithms for accurate detection without generating false positives. APSolute Vision is a tool that provides centralized network management and monitoring.

By identifying and controlling infections/malicious traffic coming from home and roaming subscribers, the telecommunications company can confidently maintain availability of its mobile packet core.

This opportunity allowed Radware to leverage its strategic relationship with Cisco and position its offering as uniquely suited for this service provider's needs, which helped Radware rise above fierce competition from an incumbent and win significant new business.

MOVING FORWARD

Moving forward, this telecommunications giant is now in the process of deploying DefensePro and DefenseFlow cybersecurity solutions to safeguard multiple 4G data centers designed to protect customer infrastructure.

DefensePro's out-of-path deployment architecture will be a critical capability for them. Because the service provider's networks can be sensitive to latency and points of failure caused by adding a DDoS

mitigation device, DefensePro devices can be configured out-of-path instead of in-line. Then, only network traffic that requires inspection is diverted to the mitigation device, which receives a copy of the traffic to be scanned for attacks. This eliminates latency and additional risk of failure while still providing high availability of the internal network. Once an attack is detected, only the relevant traffic is diverted through the device, the attack is prevented in seconds, and “clean” traffic is allowed to flow through the network freely without delay or interruption.