CASE STUDY: **GOVERNMENT**

APAC Network Provider Protects Its Applications Against DDoS Attacks With Radware's DefensePro

THE CHALLENGES

Distributed denial-of-service (DDoS) attacks were creating network and application latency, and existing mitigation solutions and strategies resulted in false positives during spikes in network traffic — and ultimately in poor user experience.

THE SOLUTION

Radware's on-premise DDoS mitigation appliance, DefensePro, was implemented in addition to Radware's Emergency Response Team (ERT) Threat Intelligence Subscription service.

WHY RADWARE

Radware's machine learning and real-time signature creation provide accurate detection and mitigation of malicious traffic to ensure little to no impact on legitimate users.

BENEFITS

During cyberattacks and/or spikes in network traffic, the network provider was able to maintain customer service-level agreements (SLAs).

This government provider of networking and cloud services plays a pivotal role in supporting the online services, applications and websites of nearly all government departments and agencies for this APAC country. Because the provider hosts the country's most critical websites and cannot afford any performance impact, availability and data security are critical requirements.

THE CHALLENGES

The network provider began experiencing application DDoS attacks that created latency and intermittent problems in network and application performance, which impacted end-user experience. The network provider's internet service provider (ISP) was unable to successfully mitigate these attacks.

Also, a series of security policies created additional problems. The network provider was using a perimeter firewall to set rate limits for DDoS attacks. This conservative rate limit policy resulted in a high number of false positives blocking legitimate users, which was of particular concern during elections when a large volume of traffic needs to be handled.

THE SOLUTION

The customer conducted a proof of concept with Radware and NETSCOUT. NETSCOUT was unable to demonstrate that it could provide behavioral-based, automated DDoS mitigation, and its solution was unable to distinguish between attack traffic and legitimate users during spikes in network traffic. In addition, NETSCOUT used a manual detection and mitigation process in which the network provider had to define signatures and filters along with rate limits to catch volumetric Flood attacks. This human intervention can lead to additional errors and false positives.

The network provider selected Radware, which it was already using for application delivery services. Radware's security solution included DefensePro, which utilizes behavioral-based technology to automatically detect and mitigate existing and zero-day attacks in real time without manual intervention. The customer also purchased Radware's ERT Threat Intelligence Subscription to complement DefensePro by providing constant updates of new risks, vulnerabilities and attackers.

> "Radware allows us to provide our customers better availability with behavioral-based attack detection and mitigation that stops real attacks and eliminates false positives. Because it is automated, the solution allows our IT team to work on other business priorities rather than constantly fighting attacks."
>
> *— Security Architect at APAC national network provider*

BENEFITS

- During cyberattacks and/or spikes in network traffic, the network provider was able to maintain customer SLAs.
- Radware's security solution lets the customer successfully mitigate multivector attacks and defend against application DDoS attacks that misuse server and application resources, including HTTP Flood attacks and network scanning.
- Radware's machine learning and real-time signature creation provide accurate detection and mitigation of malicious traffic to ensure little to no impact on legitimate users.
- Radware's ERT helps the network provider to overcome in-house security skill shortages by providing best practices and strategies and an understanding of threats, attack tools, intelligence and mitigation techniques.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.