DUCEN™
A Sryas Company

CUSTOMER SPOTLIGHT

Network DDoS Protection

And Threat Intelligence

www.ducenIT.com

Protecting networks and mitigating attacks is critical to the continued operations and services at any organization. Explore how we deployed Network Distributed Denial of Service (DDoS) protection to mitigate a range of network security threats for a client who required their network to be highly available and secured at all times. Protecting client networks from malicious attacks was critical as an unavailability or loss of integrity and confidentiality would interrupted critical services for its customers. An effective and robust security program was implemented to protect telecommunication networks from such attacks. Though the client had existing strategies and solutions to mitigate the network threats, they were not sufficient to handle new breeds of DDoS attacks.

OUR CLIENT WANTED TO DEPLOY DDOS PROTECTION FOR ITS ENTERPRISE-LEVEL CUSTOMERS WITH THE FOLLOWING MAJOR FUNCTIONS AND CAPABILITIES :

Detection – Detects up to 18 types of DDoS attacks, including volumetric and application layer attacks, regardless of their origin.

Mitigation – Scrubs/filters traffic with source IP address blocking wherever necessary and an automated process for dealing with known threats.

Filtering / Scrubbing – Automated filtering and scrubbing for all types of DDoS attacks regardless of their origin.

DNS Protection – Protection of DNS servers against DDoS attacks.

Logging – Optional logging and archiving summary of threat information.

Reporting – Near real-time threat detection with automatic alerts. The feature to generate regular monthly and ad-hoc reports for incident /SLA reporting. Automatic alerts sent to notify customer personnel when threats are detected.

Multi-site hosting static web pages – Per circuit DDoS protection with ability to specify a single IP address or define IP ranges.

SOLUTION DELIVERED

Ducen combined the power of our Cyber Threat Intelligence (CTI), Analytics, and Business Intelligence solutions to defend against DDoS attacks:

MAJOR SERVICE PROVIDED BY DUCEN :

- ✓ Comprehensive threat management system that detects, surgically mitigates, and reports on DDoS attacks.
- ✓ Multiple methods of threat detection and mitigation, payload visibility, and filtering to ensure cloaked attacks could not bring down critical defenses.
- ✓ Detection mechanism that use machine-learning methods by correlating data across the network to reduce false positives and generate more accurate alerts.
- ✓ Correlation and analysis of incoming threats. Most DDoS attacks appear legitimate, so the threat mitigation tool performs operations with extreme sensitivity to discriminate between normal vs. abnormal traffic. This is achieved with both historical trending of normal patterns, to flag any change from normal, and deep packet inspection (DPI), to further investigate potentially malicious packets.

- Identification of new and recurring threats (botnets, viruses, malware sites etc.) and population of CTI.
- Full visibility and real-time data of behavioral clustering for DDoS attacks and correlating clustered threat attack IP's (botnets, viruses, malware sites etc.) with activity and frequency on other high risk parts of the site (i.e. wires to high risk recipients).
- Monitoring services within the Upstream Security portfolio which feed information (event and traffic) to the downstream systems, in accordance to the policy, with additional mitigation actions to combat new threats identified by the correlation engine.
- Real-time alerting and visibility into actual DDoS attacks on the site with attack type and volumetric, application based, or network based data.
- Managed security services, in support with threat intelligence, to perform threat and risk assessments, vulnerability assessments and incident response to enhance business operations.

TO MITIGATE THE NETWORK DDOS ATTACKS, DUCEN DEPLOYED AN IN-HOUSE BI & ANALYTICS PLATFORM THAT PERFORMS THE FOLLOWING FUNCTIONS :

- Powered by Threat Intelligence, Analance™ BI makes decisions on legitimate versus malicious traffic and performs defensive counter measures to maintain availability of bandwidth for our client's networks.
- The platform provides real-time access to network DDoS metrics to the end client with real-time and historical attack forensics and reporting.
- Analance BI solution constantly monitors and analyzes the threat landscape, which helps identify and stop attacks before they create serious havoc or extract sensitive information.
- Visualize current end-to-end networks conditions and then coordinate and correlate what's happening across the network at various points. By correlating traffic across multiple links, generates reports and distributes them to key stakeholders in seconds
- Provides anomaly detection, packet scrubbing, traffic analysis, and email alerts.
- Supports archived security event data to enable forensic analysis and compliance reporting.
- Defines ACL/RBAC, which controls the access to data.
- Enforces baseline protection by building ongoing, always learning models of network behaviour.

RESULT

- Stayed ahead of threats with enhanced intelligence, proactive prevention, early threat recognition, rapid response, and investigation of root causes.
- Reduced business risks posed by network DDoS attacks.
- Reduced capital and operational costs associated with web security.
- Reduced risk of outages and ensured application availability by protecting and mitigating DDoS and advanced threat attacks.
- Offered greater visibility into non-standard "internet" traffic patterns.
- Ensured proper operationalization of managed services to client's customers.
- Enabled client to share the processed/scrubbed data to its subscribed customers as per the contractual obligations (in near real-time basis or as aggregated history).
- Improved service quality, availability, and customer experience thanks to proactive monitoring and real-time visibility and alerts of DDoS attacks and prevention using threat intelligence.

WHY DUCEN?

- Thought leader in business process optimization
- Guiding principle of business: Continuous Improvement Model
- Single layer of accountability
- On-time and accurate delivery success
- Rapid development
- Young and dynamic team with proven record of accomplishments and work ethics

For more information

Visit www.ducenIT.com

DUCEN™
A Sryas Company