GREENET
INFORMATION SERVICE

Brief of GreeNet Attack Mitigation Solution (AMS)

Version: A.0

Revision records

The revision records accumulates notes for each document update. The latest version of the documentation contains updates from all previous versions of the documentation.

Document version 01（2021-06-28）

The first official release.

Catalogue

1. Background

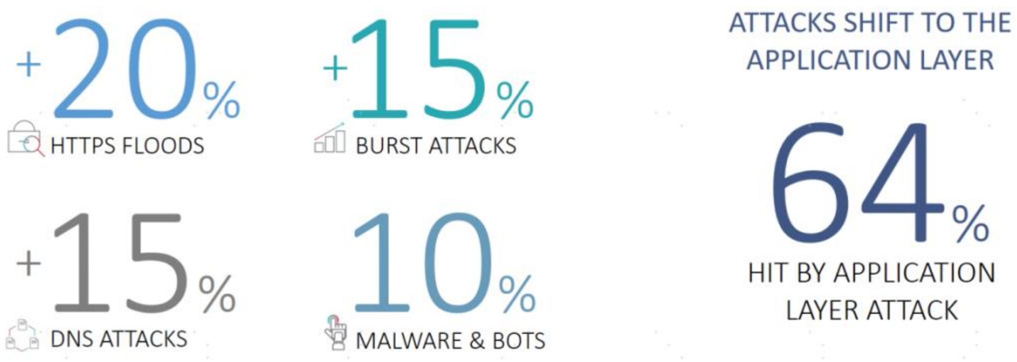
Distributed Denial of Service (DDoS) attack is the oldest Internet threat. Due to its simplicity and effectiveness, it remains the greatest risk to public services worldwide. As protections have been evolving, the techniques used by hackers have adapted and become more sophisticated. New types of attacks now target on applications and services. They are very difficult to detect because batches of layer 3 and layer 4 DDoS events become more complex, and are usually masked in apparently legitimate traffic or in the unique new "zero-day" attacks.

The traditional Anti-DDoS monitoring method is based on:

- Defend against attack intrusions and DDOS attacks by querying the attack signature database.
- Defense against DDOS attacks through thresholds.

However, the prevention methods above cannot cope with the endless attacks.

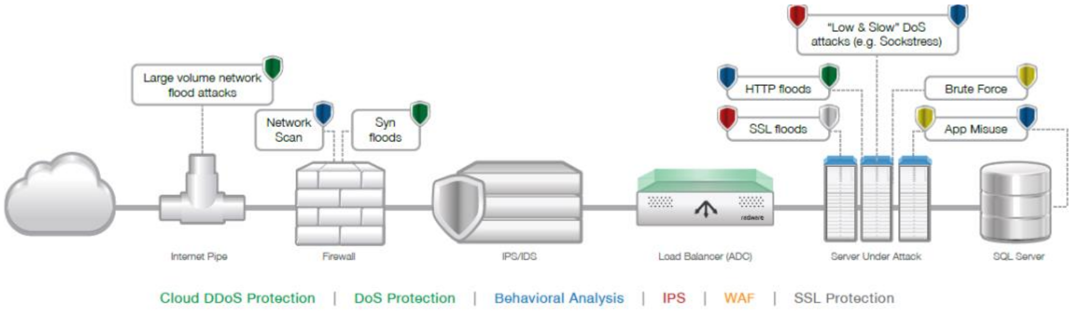
- The attack signatures can only be analyzed after the attack has occurred. Therefore, although this defense method is effective, it lacks sufficient proactivity.
- The potential for misclassification via threshold limits is very high, which would compromise normal applications and services while preventing attacks.
- New types of attacks are emerging all the time. Both signature-based and threshold-based defense methods can only reduce the negative impact of attacks from the local behavior of the network.



Therefore, in today's increasingly serious network security, we need a multi-level and real understanding of network attacks and effective defense.

2. Solution

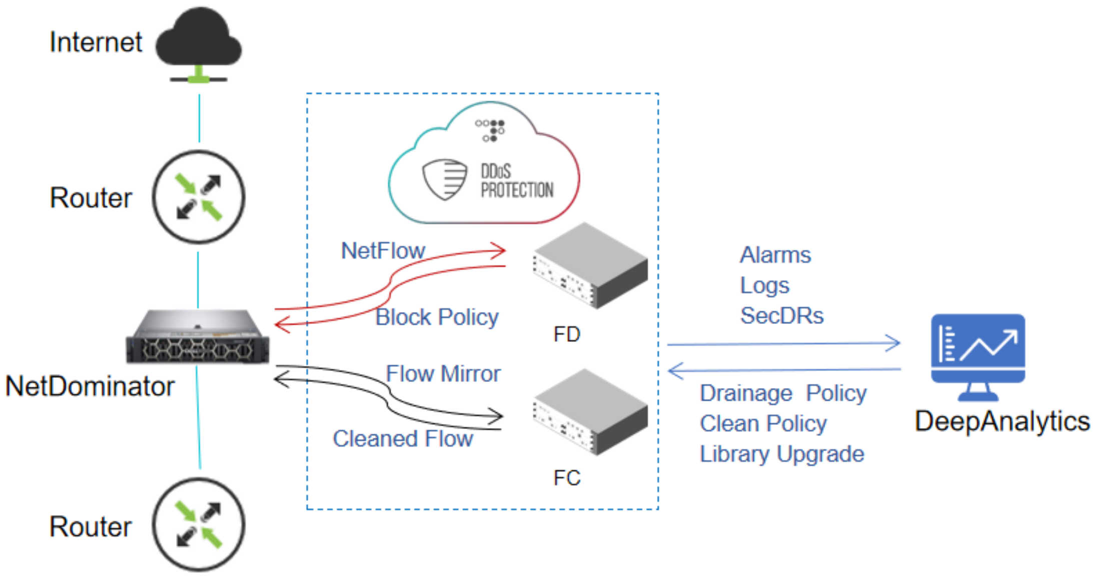
GreeNet and Radware have partnered to combine GreeNet's world-leading DPI technology with Radware's powerful security capabilities to provide users with high-performance DPI and anti-DDoS services. GreeNet AMS analyzes network traffic and isolates, blocks and prevents a wide range of application attacks to provide reliable protection for all network applications, users and resources.


"Low & Slow" DoS attacks (e.g. Sockstress)
Large volume network flood attacks
HTTP floods
Brute Force
Network Scan
Syn floods
SSL floods
App Misuse
Internet Pipe
Firewall
IPS/IDS
Load Balancer (ADC)
Server Under Attack
SQL Server
Cloud DDoS Protection | DoS Protection | Behavioral Analysis | IPS | WAF | SSL Protection

Based on years of deep understanding of customer needs and professional research on security, GreeNet has launched anti-DDoS solutions for carriers, enterprises, data centers, portals, online games, online videos, DNS domain name services, etc. Based on the protection of traditional traffic-based DDoS attacks, GreeNet AMS focuses on strengthening the protection against application layer attacks, the IPv4-IPv6 dual-stack protection and other functions to truly protect user business security.

GreeNet AMS conducts continuous and regular research and analysis on the traffic of the protected objects, presenting the normal curve of service traffic, and adopts different protection strategies for various types of business traffic and different periods of the same business to achieve refined protection.

GreeNet AMS uses in-depth per-packet analysis technology to start protection as soon as an attack occurs. Protection uses various technical means such as filters, behavior analysis and session monitoring to accurately protect against various Flood attack traffic, Web application attack traffic, DNS attack traffic, SSL DoS/DDoS attack traffic, and protocol stack vulnerability attacks.



The solution provides a multi-vector attack detection and remediation solution that can handle network layer attacks, server-based attacks, malware propagation and intrusion activities. The solution also defends against high and non-high traffic attacks, protection against volumetric and non-volumetric attacks, SYN flooding attacks, low and slow speed attacks, HTTP flooding attacks, impulse attacks, SSL-based attacks, burst attacks and so on. Because the solution can analyze traffic, it builds traffic baselines that can be customized for organizations.

The solution provides the industry's most advanced and automated protection against the fast-moving threats posed by recent IoT-based attacks such as Mirai. It is uniquely built to overcome the complexity and scale of today's sophisticated IoT-based botnets. GreeNet’s DDoS protection includes best-in-class behavior-based algorithms to prevent known and unknown DNS flooding attacks in the most cost-effective manner. It includes an innovative and aggressive DNS security model to prevent DNS waterboarding attacks.

Our DDoS protection protects against all kinds of network DDoS attacks including:

- UDP flood attacks
- SYN flood attacks
- TCP flood attacks
- ICMP flood attacks
- IGMP flood attacks
- Out-of-state flood attacks

Combining the anti-DDoS and DPI technologies, GreeNet's world-leading network behavior analysis prevents application resource abuse and zero-minute malware propagation including:

- HTTP page flood attacks
- DNS flood attacks
- SIP flood attacks
- Brute force attacks
- Network and port scanning
- Malware propagation

SSL attack mitigation provides protection against SSL-based DDoS attacks as follows.

- Uniquely mitigates floods that are directed to HTTPS pages
- Provides unlimited SSL decryption and encryption capabilities
- Operates in symmetric and asymmetric environments

3. Composition

The AWS includes NetDominator (DPI and implementation module), FC (flow cleaning module), FD (flow detection module) and DeepAnalytics (management center).

NetDominator

Application-based deep packet inspection (DPI) technology enables network visualization and traffic management that small traffic attacks and application layer attacks can be detected. DPI can sample and forward the traffic of the protected objects to FD to further analyze the DDoS attack type.

Flow Cleaner (FC)

The FC module mainly drains and cleans traffic according to the policies issued by the Management Center, re-injects normal traffic after cleaning, and records these actions in the logs and reports them to the Management Center. The cleaning center provides a variety of DDoS traffic cleaning methods to accurately identify normal traffic and clean various abnormal traffic, including traffic-based attacks, application layer attacks, scanning and snooping attacks, and malformed packet attacks. The cleaning center also act as a testing center. When operators do not have high requirements for testing and cleaning performance, they can deploy only the cleaning center.

Flow Detector (FD)

The FD module detects traffic based on Netflow, which comes from Netdominator. Once suspected attack traffic or attack traffic is detected, FD will send the diversion policy to NetDominator and send the cleaning policy to FC simultaneously. NetDominator forwards the traffic to FC for cleaning, and then sends the cleaned traffic back to the original link.

DeepAnalytics

DeepAnalytics unifies the management of NetDominator, FC and FD, and is the management center of AWS. It provides device management, policy management, performance management, alarm management, report management, etc. It also updates the DPI and cleaning center.

4. Scenarios

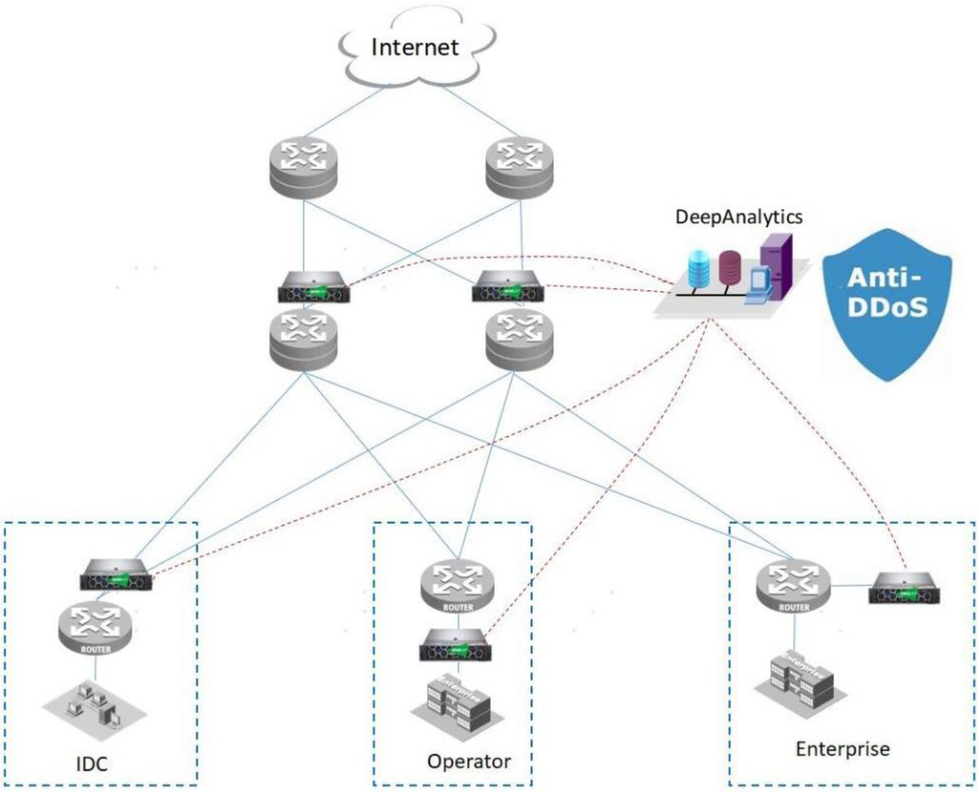
GreeNet AMS solutions can be widely used in carrier backbone networks, metro and enterprise networks, IDC, etc.

- Backbone network deployment: Relieve the egress pressure of MANs and protect the bandwidth resources of operators.

- Metropolitan area network deployment: Resist DDoS attacks on the MAN from external MANs and protect the availability of MAN bandwidth resources. Provide secure operation services and value-added services in the gathering place of protection targets, and ensure the security of bandwidth resources and services of protection targets.

- IDC deployment: Ensure uninterrupted secure server services, professionally protect HTTP, HTTPS, DNS and SIP servers, and provide operational value-added services.

- Enterprise network egress deployment: Ensure the security of enterprise network bandwidth resources and application service servers.



Many enterprise customers have suffered DDoS attacks with traffic exceeding 100Gbps and reaching hundreds of Gbps, far exceeding the link bandwidth and leading to MAN congestion. Faced with such a large amount of attack traffic, layered cleaning must be performed. Operators perform large-traffic attack detection and cleaning in the backbone network to defend against large-traffic transport protocol layer and application layer attacks from the Internet to ensure the smooth flow of MAN links. Customers defend against external attacks (including those inside the MAN) at the exit of the enterprise network, mainly defending against transport protocol layer and application layer attacks within the link bandwidth, and many application layer attacks, such as SSL-DoS/DDoS attacks, HTTP /HTTPS slowdown attacks and cache miss attacks targeted on DNS servers. A small amount of attack traffic can cause a significant attack effect. Therefore, only application-layer detection and cleaning devices can be deployed for real-time deep detection and cleaning.

5. Deployment

The AMS solution can be deployed in two modes: Inline and Bypass.

5.1 Inline Deployment

Inline deployment networks are simple, do not require additional interfaces, and are better than bypass deployments in terms of individual attack protection because the protection devices can monitor traffic in both directions in real time. However, since all traffic passes through the DDoS devices, this requires that the DDoS protection devices must be able to provide sufficient reliability to ensure that a single point of failure is avoided and algorithmic misclassification is reduced.

In an inline deployment, only the cleaning device can be deployed. The cleaning device is deployed behind the gateway and before the firewall, and it needs to connect the bypass card in series or adopt the dual-system hot standby mode to ensure the service traffic can pass smoothly when the cleaning device fails, and thus improving the reliability.

5.2 Bypass Deployment

In high-traffic scenarios, allowing DDoS protection devices to handle all the traffic would consume a lot of forwarding performance, leading to increased security investment. Meanwhile, in some operators' scenarios, the network structure is complex, making it difficult to deploy in a straight line. For some network service providers, they also want to avoid the possible short-term disruption of links caused by direct deployment of devices, so the bypass deployment approach has emerged. Compared with the in-line deployment, bypass deployment can ensure that the original network is not disrupted. However, it also introduces the technique of flow direction changing, using a series of methods such as drainage and reinjection to control the flow direction and handle of abnormal flows.

6. Feature

Hybrid Prevention

Integrated with Radware's on-premises (real-time DDoS protection solution) to provide volumetric attack protection based on behavioral analysis.

Easy Deployment

Uses the most advanced X86 processor to ensure wire-speed forwarding of interface traffic. The X86 platform features of fast development, providing customers with fast customization interfaces.

High Reliability

Use external dedicated BYPASS equipment. In the straight road scenario, when the AntiDDoS8000 fails, the traffic is forwarded by the BYPASS device to ensure uninterrupted business. The devices all support 1+1 backup technology, which supports smooth switching of the main and standby main control boards under uninterrupted business conditions.

Adopts an external dedicated BYPASS device. In the case of a straight path, when AntiDDoS8000 fails, the traffic is forwarded by BYPASS devices to ensure service uninterrupted. The devices all support 1+1 backup, allowing smooth switchover from the active control board to the standby without service interrupted.

In-Depth Inspection

In-depth detection and analysis of each byte of a packet, using abnormal packet filtering, feature filtering, defense against false sources, true source behavior detection, session-based defense, behavior analysis and traffic shaping, can effectively identify various types of attacks such as application-based attacks, scanning and snooping attacks and malformed packet attacks. This achieves accurate cleaning of various DoS/DDoS attack traffic.

Centralized Management

Provides a single management platform to manage and monitor all security components in a collaborative manner.

High Accuracy

Uses patented behavior-based detection and real-time signature creation algorithms. These algorithms create baselines of normal network, application and user behavior, and use these baselines to note anomalous traffic and accurately detect attacks. When a new zero-day attack is detected, this solution creates a signature in real-time using the attack signature and immediately begins blocking the attack within 18 seconds. By implementing patented behavioral analysis techniques, this attack mitigation solution detects both known and unknown attacks in a timely manner with a rather low false alarm rate.

Uses a behavioral engine to study multiple parameters of traffic. This behavioral engine analyzes multiple IP parameters in TCP (connection-oriented) and UDP (connectionless) traffic, as well as ICMP (router discovery) and IGMP (IP multicast) messaging. GreeNet also measures different parameters of HTTP and DNS traffic to detect attacks that attempt to target servers. By looking at the rates and ratios of these different parameters, GreeNet creates a multi-vector mathematical representation of normal or baseline traffic, which is then compared to incoming traffic to detect attacks.

For example, in the case of TCP or UDP, GreeNet determines the difference between a flash crowd or heavy traffic (which follows the normal proportion of traffic and therefore good traffic) and an attack in a given network.

Always-On Protection and Least Time-Consuming Mitigation

Ensures continuous protection for data centers. It provides on-premise full protection against multi-vector DDoS attacks. Only in the case of a volumetric attack, where an organization’s Internet pipeline is about to be saturated, the traffic will be diverted to the GreeNet scrubbing center for removing the attacking traffic before it reaches the Internet pipeline. This allows for a smooth transition between mitigation solutions.

The always-on protection ensures that organizations are fully protected, with mitigation measured in seconds. In addition, in the event of an attack that requires traffic to be moved to the cloud scrubbing center, the protection continues without any interruptions or gaps.

Monitoring&Analysis&Reporting All in One

Contains proactive monitoring and health checks of protected services or applications, providing an organization-wide security and compliance status from a single console. Ongoing reports on all attacks that are mitigated (automatically mitigated or invoked) by the system are available on the web-based service portal. A built-in Security Event Information Management (SEIM) system provides the security and compliance status of the entire organization from a single console. Data from multiple sources are collected and evaluated in a consolidated view of dashboards and reports. These views provide extensive and simple drill-down capabilities, enabling users to easily access information to expedite incident identification, provide root cause analysis, improve collaboration between NOC and SOC teams, and accelerate security incident resolution.

7. Summary

DDoS attacks cause lost revenue and increased expenses for organizations. Attackers are more sophisticated and use multi-vulnerability attack campaigns. The solution provides a hybrid, multi-layered mitigation with the a wide range of attack mitigation capabilities.

This hybrid solution provides the shortest mitigation time to instantly stop multi-vulnerability DDoS attacks and restore revenue streams.

GreeNet's attack mitigation solution is based on patented algorithms for behavior-based detection, real-time signature creation and automated policy generation, automating the attack lifecycle process. It provides a high level of protection against the most dynamic and sophisticated attacks with minimal impact on legitimate traffic. These algorithms provide organizations with the most automated, multi-vector attack mitigation in an integrated, single-vendor solution.