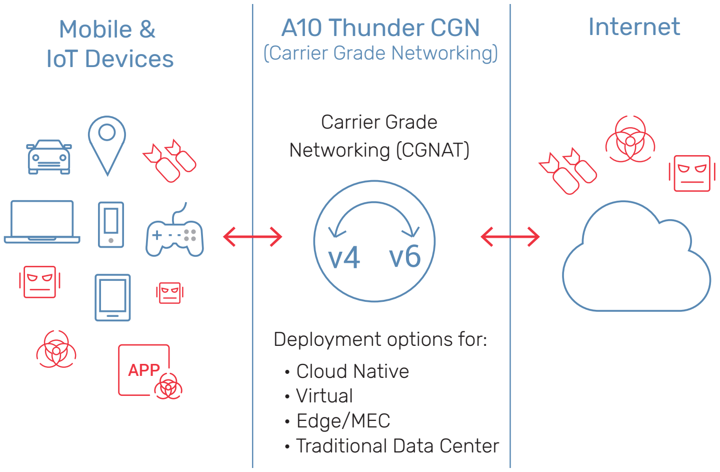
Solution Brief

DDoS Protection for CGNAT Environments

Service providers face increasing difficulty maintaining service availability for their subscribers while attempting to defend against malicious DDoS attacks. Year over year, these attacks increase in sophistication, size, and duration, outpacing the operator's ability to react and maintain network stability. Service providers also must protect critical CGNAT functions while transitioning networks to new 5G, MEC, edge or cloud native technologies.

The Security Landscape

Traditionally, service provider networks have depended upon firewall defenses at the internet edge to protect critical network infrastructure such as CGNAT. However, with the changing threat landscape and growing volumes of IoT devices, attacks can now originate from inside the network. This changes the paradigm. As DDoS and other types of attacks grow in frequency, sophistication and size, organizations need to have solutions that can mitigate attacks early before they have the opportunity wreak havoc.



Challenge

Service providers must maintain service availability as DDoS attacks grow. CCNAT, a critical function, is often the target for DDoS attacks. Service providers need integrated DDoS protection with carrier-grade NAT solutions to improve attack detection, reporting, and mitigation.

Solution

A10 Thunder® CGN, available in container, virtual, bare metal and physical form factors are augmented with integrated DDoS protection to give service providers enhanced infrastructure protection against the rising occurrence of DDoS attacks targeting CGNAT infrastructure and NAT pools.

Benefits

- Protects network infrastructure from DDoS attacks in carrier grade networking environments
- Maintains network stability and improves subscriber experience with a lower TCO

In particular, network elements that maintain state such as intrusion detection systems, firewalls, and carrier grade NAT (CGNAT) are prime targets for malicious activity. Their state tables can be exploited through various attacks to exhaust CPU and memory resources which severely impacts subscribers' quality of experience.

Research reports show an increase in DDoS attacks against CGNAT devices. Reflective attacks combined with some element of amplification can target specific addresses in the NAT pools to cause buffer exhaust, increased CPU utilization, and session quota exhaust and can be either internally or externally generated. In addition, internally generated attacks can target either NAT pool resources or external resources, resulting in blacklisting of the NAT IP addresses.

Integrated DDoS Protection in a Carrier-Grade Environment

A10 Thunder CGN for IPv4 preservation and IPv6 migration is augmented with integrated DDoS protection capabilities for improved attack detection, reporting, and mitigation. Integrated DDoS Protection provides service assurance by protecting the platform during attacks, mitigates attacks from the Internet targeting NAT pools, and mitigates attacks from users such as traffic from compromised hosts or botnets.

Integrated DDoS Mitigation Features

1. IP Protocol Anomaly Filters

IP anomaly filtering provides initial scrubbing for common attack signatures for incoming and outgoing traffic. It monitors incoming traffic to ensure that all protocol headers are properly formed and behaving in accordance with models built upon relevant standards and state machines.

IP anomaly filtering protects internal and external devices and the CGNAT network elements from attacks based on known packet signatures and disrupts network reconnaissance attempts where attackers use protocol vulnerabilities to gain target information, such as operating system type and version.

2. Connection Rate Limiting

Stateful devices, including carrier-grade NAT network elements, have a finite number of sessions that can be created and present a vulnerability that must be monitored and protected. Once the number of available sessions reaches zero, no new connections can be established, blocking both client communications and new endpoint independent filtering (EIF) mappings setting user quota/session limits for the overall number of connections available.

Thunder CGN also mitigates infrastructure attacks by managing connection rates. Connection rate limits can be set up based on TCP, UDP and ICMP protocol and are enforced on a per source IP address basis, limiting both originating connections from clients, and connections from the external networks. Once the rate limit is reached, sessions are no longer created for the source IP address regardless of absolute quota size.

3. IP Blacklist for NAT IP Resource Protection

NAT pool resources can easily be discovered with port scans and software exploiting vulnerabilities in STUN implementations. If a particular NAT pool address is targeted with high traffic loads, any client mapped to the address under attack will experience unacceptable performance including service interruptions. These attacks can compromise the entire data path within the CGN device, which then drives CPU utilizations to inoperable levels. To mitigate these attacks and protect critical CPU resources, the carrier-grade NAT device must drop this traffic early in the data path. The IP blacklisting feature provides NAT pool resource protection from high-volume infrastructure-based attacks.

4. Selective Filtering

Selective filtering protect servers and CPUs against reflection and spoofing types of volumetric attacks. Selective filtering identifies when packets are coming in at an abnormally fast rate, creates a destination IP and destination IP port entry in a logging table and drops the packets.

5. Reduced CPU Overhead for CPU Round Robin

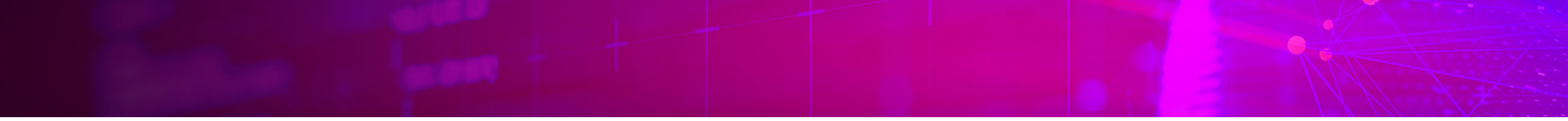
When CPU Round Robin is triggered, the packets are distributed across all available CPUs for processing in order to avoid oversubscribing on the targeted CPU. In some cases though, throughput and CPU utilization remained high until the excessive traffic ended. To reduce the overhead, the Thunder CGN drops SYN packets earlier on in order to decrease use of the targeted CPU.

Thunder CGN Prevents Service Disruption and Maintains Business Continuity

Service providers need to protect their critical CGNAT network infrastructure including the NAT IP pools, to avoid service disruptions and maintain business continuity. A10 Thunder CGN is built on the market-proven Advanced Core Operating System (ACOS®) platform that delivers unprecedented performance and scalability with the industry's best data center footprint. Thunder CGN solutions are augmented with integrated DDoS protection techniques to protect the CGN device by mitigating DDoS attacks to maintain network stability.

The most advanced carrier-grade networking solution, Thunder CGN evolves continuously to serve service providers worldwide for their integrated security, CGNAT and networking needs.

In addition, the integrated CGNAT feature set is included along with Gi/SGi firewall in the A10 Thunder Convergent Firewall (CFW) to offer a comprehensive security solution for service provider network deployments, while enabling a smooth transition to IPv6.



Next Steps

For more information, please contact your A10 representative or visit a10networks.com/cgn.

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers, higher education institutions and and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit: a10networks.com
or tweet @a10Networks

Learn More

About A10 Networks

Contact Us
a10networks.com/contact

Part Number: A10-SB-19189-EN-02 FEB 2021