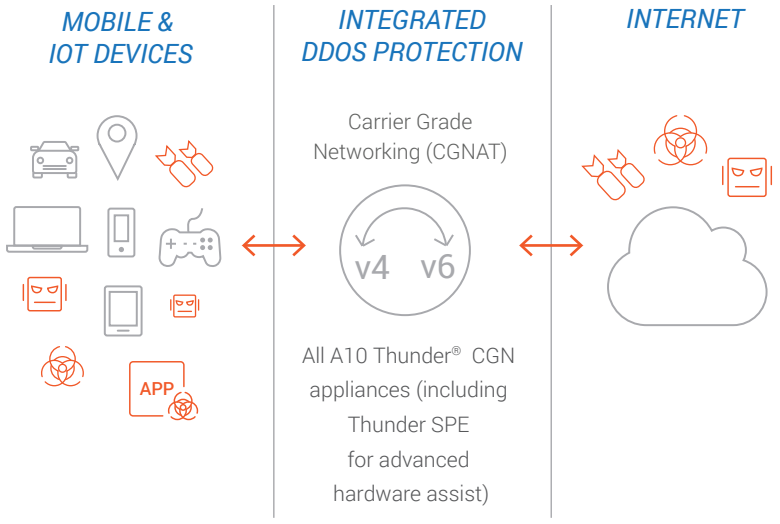
SOLUTION BRIEF

COMBATING DDOS ATTACKS IN A CGNAT ENVIRONMENT

Mobile and fixed operators 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, complexity, bandwidth consumption, and duration, outpacing the operator's ability to react and maintain network stability.

THE SECURITY LANDSCAPE

Traditionally, mobile and service provider networks are protected against attacks that come in through the internet. Critical network infrastructure is left unprotected based on the assumption that attacks will be stopped at the internet edge by employing a firewall defense. However, with the changing threat landscape, attacks can now originate from inside the network, such as the recently discovered WireX. This changes the paradigm. As these types of attacks grow in frequency, sophistication and size, organizations need to solutions in place to stop them before they have the opportunity wreak havoc.



CHALLENGE

With the increase in number of attacks against the core network infrastructure and CGNAT devices, in particular, it is imperative that service providers proactively stop these attacks to ensure maximum uptime of network resources and avoid service disruption. Service providers are looking for integrated DDoS mitigation capability with carrier grade networking solutions to improve attack detection, reporting, and mitigation without the need for external DDoS scrubbing infrastructure.

SOLUTION

A10 Thunder CGN appliances are augmented with integrated DDoS mitigation capabilities to give service providers enhanced infrastructure protection against the rising occurrence of large-scale DDoS attacks.

BENEFITS

- Protect your network infrastructure from DDoS attacks in carrier grade networking environments
- Maintain network stability and improve subscriber quality of 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.

Recent DDoS attack reports show an increase in 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. In addition, internally generated attacks can target either NAT pool resources, resulting in the aforementioned effects, or external resources, resulting in blacklisting of the NAT IP addresses.

INTEGRATED DDOS PROTECTION IN A CARRIER GRADE ENVIRONMENT

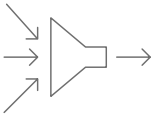
A10 Thunder CGN product line for IPv4 preservation and IPv6 migration is augmented with integrated DDoS mitigation capabilities for improved attack detection, reporting, and mitigation. This solution delivers a lower total cost of ownership (TCO) for a CGNAT solution by mitigating the attacks without the need for external DDoS scrubbing infrastructure.

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 to models built upon relevant standards and state machines. Examples include Bad IP Header Length, Bad IP TTL, UDP/TCP Bad Checksum, Invalid TCP flag combination, etc.

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 CGNAT 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 reach zero, no new connections can be established, blocking both client communications and new EIF (Endpoint Independent Filtering) mappings. If a large number of clients are infiltrated and launch an attack, the maximum number of connection requests per second the platform supports can be exceeded, disallowing any new connection requests. Also, attacks originating from external networks can be directed towards a particular NAT pool address/port using random IP source address/ports depleting the user session quota resources.

Thunder CGN appliances enforce techniques such as setting user quota/session limits to limit the overall number of connections available to the user per protocol; however, this method will not protect CPU resources from a large number of connection setup requests.

Enforcing connection rate limiting to manage the rate at which connections are set up helps to mitigate infrastructure attacks. 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 utilizing EIF. Once the rate limit is reached, sessions are no longer created for the source IP address regardless of absolute quota size. Connection rate limiting is applicable for both IPv4 and IPv6 flows, and is also applicable across hair-pinned connections.

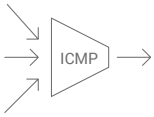
3. IP BLACKLIST FOR NAT IP RESOURCE PROTECTION

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 drives CPU utilizations to inoperable levels. To mitigate these attacks and protect critical CPU resources, the CGNAT device must drop this traffic early in the data path. NAT pool blacklisting provides NAT pool resource protection from high-volume infrastructure-based attacks.

The NAT pool blacklisting feature identifies malicious traffic exceeding a defined upper threshold for a particular IP address/L4 protocol (TCP, UDP, IP, and other protocol types) configured in the NAT pool, and executes the configured mitigation steps. Once the flow rate falls to acceptable levels, or the configurable mitigation timer expires, the affected IP address is returned service.

NAT pool blacklisting provides configurable parameters for TCP, UDP, IP, and other protocol types. L4 protocol-based attacks that exceed the configured packets per second (PPS) maximum per protocol will trigger the associated NAT IP address to be moved to the blacklist. During this time, all sessions mapped to the blacklisted resource are cleared, allowing affected clients to remap their sessions to other NAT resources with minimal service disruption. After the detected flow rate falls below the configured threshold, and the hold down timer expires (~10 seconds), the NAT address is returned to normal operation.

The NAT pool blacklist option supports configuration for both the mitigation time and actions to be taken upon attack detection. The mitigation technique is configurable and includes dropping all packets, logging the violation only, or implementing flow redirection via Remotely Triggered Black Hole (RTBH) filtering procedures. After the mitigation timer expires, the affected NAT resource is returned to service regardless of flow rate. If the attack continues, the appropriate actions are repeated until the flow rate is below the configured packets per second (PPS).



4. ICMP RATE LIMITING

According to the most recent attack reports, ICMP flooding was used in 10 percent of all infrastructure-based attacks and continues to be a common tool used in multi-vector attack strategies. ICMP flooding exploits normal ICMP processing behavior in targeted devices to exhaust resources either by attempting to process a flood of ICMP requests or forcing transmission of “destination unreachable/port” packets in response to UDP floods.

While NAT pool blacklisting provides ICMP protocol filtering for attacks targeting NAT pool resources, Thunder CGN also supports ICMP rate limiting for all ICMP flows traversing the CGNAT device regardless of direction or interface type. ICMP rate limiting can be applied globally or at the interface level.

SUMMARY

Service providers need to protect their critical 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 defense techniques to protect the CGN device by mitigating DDoS attacks to maintain network stability.

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

In addition, the integrated CGNAT feature set is included along with Gi/SGi firewall in the A10 Thunder CFW to offer a comprehensive security solution for mobile 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) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

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-01 JAN 2018