Behavioral Burst-Attack Protection

Table of Contents

Burst Attacks—Overview

Common DDoS attacks come in the form of sustained, high-volume traffic floods that ramp up gradually, reach a peak, and are then followed by either a slow or a sudden descent.

In recent years, a new attack pattern has emerged. Burst attacks, also known as hit-and-run DDoS, use repeated short bursts of high-volume attacks at random intervals. Each short burst can last only few seconds, while a burst attack campaign can span hours and even days. These attacks unleash hundreds of gigabits per second of throughput toward its the victim.

To combat burst attacks effectively and efficiently, a protection strategy needs to combine the following capabilities:

- Mitigate hundreds of gigabits per second of burst attacks, which last seconds, at random intervals
- Automatic signature creation to block only the attack traffic
- Dynamically adjust to changing and multiple attack vectors across bursts
- Minimize false positive

This paper introduces Radware's new Behavioral Burst-Attack Protection that is part of Radware's DDoS protection technology included in Radware's DefensePro, which addresses the challenges that burst attacks impose, combining the necessary ingredients into a complete and scalable protection for both on-premises and hybrid deployments.

The Challenge of Protecting Against Burst Attacks

While both burst attacks and sustained DDoS attacks utilize application and network floods, burst attacks impose a challenge to on-premises and hybrid DDoS protection strategies.

The majority of on-premises DDoS protection solutions detect burst attacks, but most of them limit the rate of bad (and legitimate) traffic to a certain threshold, resulting in a high level of false positives. To minimize the level of false positives, security experts need to identify the attack traffic by analyzing traffic captures and manually creating a signature to block only the attack traffic. If the attack vector changes across bursts, the signature needs to adapt to the changing attack characteristics. The process of repeated manual signature adjustments can become a labor-intensive task, which renders the whole protection strategy unfeasible. In addition, the dependency on manual based protection increases the time-to-mitigation and extends the time in which the organization is vulnerable until a signature is created.

Similarly, most hybrid DDoS protections utilize rate thresholds to trigger a diversion to a cloud DDoS-protection provider or a scrubbing center. Although hybrid solutions guarantee no pipe saturation, the majority suffer from the same high level of false positives, because both the on-premises DDoS gear and scrubbing-center DDoS gear use rate-limit techniques, utilizing manually created signatures to pinpoint attack traffic and reduce false positives.

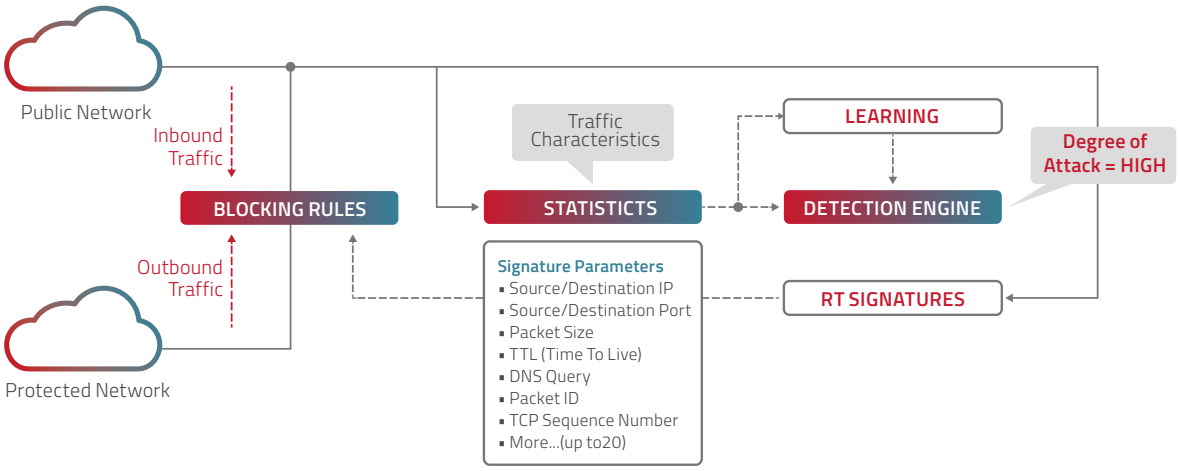
Behavioral DoS Detection and Mitigation of Burst Attacks

To address the challenges mentioned above to protect against burst attacks, Radware enhanced its innovative Behavioral DoS (BDoS) Protection technology to effectively detect and mitigate burst attacks. Radware's behavioral DDoS protection is at the core of Radware's DefensePro and is based on machine-learning algorithms that can learn normal traffic behaviors, detect traffic anomalies during an attack and automatically create signatures and adapt the protections to mitigate the attack.

Figure 1 depicts the main functional blocks of Radware's BDoS Protection. BDoS gathers statistics on various parameters for various protocols, such as TCP, UDP, ICMP, and IGMP. The statistics block feeds the learning block. The learning block builds a baseline of traffic in peacetime. The detection engine compares real-time statistics with the learned baseline in order to detect attacks.

Figure 1:

BDoS Functional Blocks



Attack detection in BDoS Protection combines two parameters. One parameter is rate, such as the bandwidth of a specific traffic type. The second parameter is rate-invariant, such as the portion of the specific traffic type out of the entire traffic distribution.

A fuzzy-logic inference system measures the degree-of-attack (DoA) surface. BDoS considers an attack to have started—and triggers attack handling—only when the overall DoA surface for the combined parameters is high. This guarantees accurate detection of attacks. For example, a high volume of traffic caused by a flash crowd will have a high rate anomaly, but the rate-invariant parameter will remain normal. As a result, the combined DoA surface will not cause BDoS to trigger an attack handling. However, if both parameters show an anomalous score, the combined DoA surface will trigger attack handling, and BDoS will start creating a blocking signature in real-time. It takes BDoS 10 to 18 seconds to create a signature.

In BDoS, a created signature blocks the attack traffic. Once an attack stops, BDoS clears the signature and monitors ingress traffic for new attacks. In the event of a new attack, BDoS kicks in to detect and characterize the attack traffic, and to create a new signature.

Burst attacks, however, which last only a few seconds, bypass BDoS Protection, because there is not enough time to create the signature. This is where Behavioral Burst-Attack Protection comes in.

The Anatomy of Behavioral Burst-Attack Protection

Behavioral Burst Attack Protection optimizes BDoS attack detection and characterization Consider the burst attack in Figure 2, as an example. There are three bursts, and each one lasts a few seconds.

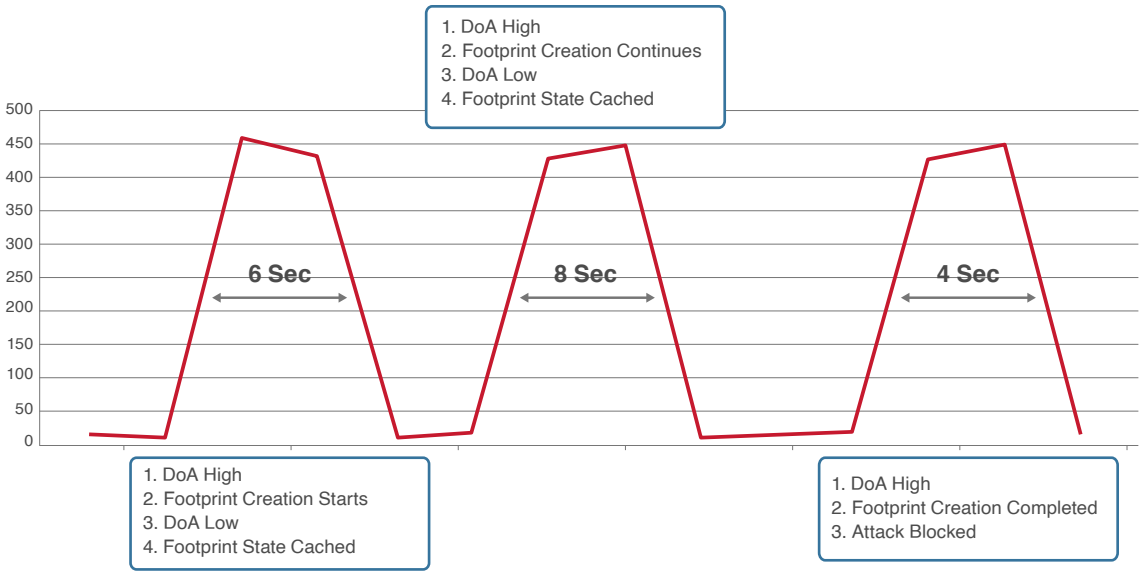


Figure 2:

A Day in Burst-Attack Mitigation

When burst 1 comes in, BDoS detects an attack due to high DoA, and proceeds to characterize the attack, to create a blocking signature. Since burst 1 ends after 6 seconds, no signature has yet been created. During the idle time between burst 1 and burst 2, BDoS caches the state and the parameters it has gathered for the candidate signature, and keeps them for the next burst. When burst 2 comes in, BDoS continues to create the signature from the point at which it stopped, using the cached information. Since burst 2 ends after 8 seconds (for a total of 14 seconds), BDoS does not yet finalize signature creation. However, when burst 3 comes in, for a total of 18 seconds of continuous attack, BDoS finalizes signature creation, and blocks the attack.

BDoS blocks the subsequent bursts instantaneously, since a valid signature is applied throughout the lifespan of the attack.

Once a burst attack stops, BDoS terminates the attack handling, clears the signature, and monitors ingress traffic for new attacks.

To handle cases of long idle intervals between bursts, BDoS changes the signature state to non-blocking. When the next burst comes in, BDoS changes the state to blocking, immediately dropping attack traffic. There is no need to re-characterize malicious traffic.

Multiple and Changing Burst-Attack Vectors

Burst attacks usually include multiple vectors, in order to challenge signature-based mitigation techniques. Since many mitigation strategies use manual signatures, it is more difficult to characterize a multi-vector attack.

BDoS includes multiple attack engines to detect and block various attack vectors. Each attack engine works independently to characterize multi-vector attacks. BDoS treats a multi-vector attack as a collection of attacks. A BDoS engine is assigned to each attack vector and a signature is created for it. The sum of created signatures, one signature per attack vector, effectively blocks multi-vector attacks.

Burst attacks also change vectors throughout the attack lifespan. This is an even greater challenge for attackmitigation strategies, because it involves modifying the blocking signature in real-time across bursts. BDoS continuously monitors the attack traffic and measures the DoA. If, after applying a signature, the DoA is low, there is no need to change the signature. However, if the attack changes in such a way that the applied signature is no longer effective (that is, the DOA is high), BDoS fine-tunes the signature to block the mutable (changeable) burst attack.

Radware's Hybrid DDoS Protection Of Burst Attacks

Radware provides hybrid deployments with unique protection against burst attacks. On-premise mitigation solutions guarantee in-line protection, but fail to protect against pipe saturation. Only a solution that combines on-premises and in-the-cloud protection against burst attacks ensures attack mitigation that is accurate, realtime, and fully automated.

Radware utilizes its Behavioral Burst Attack Protection technology in its DefensePro DDoS mitigation appliances, as well as in its Cloud DDoS Protection Service.
A typical Radware hybrid deployment will detect a burst attack and divert it to the cloud. Since DefensePro is deployed both on-premises and in the cloud, the burst attack characteristics, as well as the learned baselines, are shared with the cloud. This information allows Radware's Cloud DDoS Protection Service to immediately characterize and block burst attacks, shortening the time to mitigate, while providing the same technological benefits to hybrid customers that on-premise customers enjoy.

CONCLUSION

With the advent of attack vectors that have emerged recently, burst attacks pose a great risk to any mitigation strategy. Burst attacks combine sophisticated multi-vector, mutable attacks, with very high traffic volumes, which are unleashed suddenly upon their victims.

Radware's Behavioral Burst Attack Protection provides a genuine and innovative mitigation strategy to address burst attacks. Radware provides both on-premises, hybrid and cloud-only protection strategies with the ability to mitigate such attacks, by utilizing its DefensePro attack-mitigation appliances on-premises and in the cloud.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud, and software defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.