radware

Understanding the Security Industry's Most Effective DDoS Detection Algorithm

Whitepaper

SHARE THIS WHITEPAPER

Table of Contents

Executive Summary

Radware is often cited as having the best DDoS protection in the security industry, enabled by a powerful detection algorithm. This paper explains Radware's approach to developing and implementing this algorithm and why it considers *rate* and *ratio* in its calculations. The result is superior protection that mitigates attack traffic without impacting good traffic.

Radware's security solution is fueled by a powerful detection algorithm that:

- Considers all attack probabilities, not just volumetric.
- Uses a behavioral engine to generate multivector representations.
- Employs advanced active challenges to verify good versus bad traffic.

More Sophisticated Attacks Require a Better Algorithm

Conventional DDoS platforms were originally designed to stop volumetric attacks, the most rudimentary of DDoS assaults. These attacks are based on sending more volume or traffic than a pipe, interface or server, is expecting. For example, to target a Provider Edge (PE) router with 10G interfaces, an attacker sends 10G or more of traffic to the router on one of its interfaces. This action effectively saturates the router's interface or pipe causing congestion and blocking valid user traffic.

In the last 10 years, cyber security attacks have become significantly more sophisticated. We have seen the rise of application specific attacks that target the applications on a network (HTTP, DNS, SIP/VoLTE, other) and try to overwhelm the server application, not the connectivity pipe. Detection algorithms needed to evolve to keep up.

Radware's Algorithm Considers All Attack Probabilities

To mitigate the full range of network attacks – not just volumetric – Radware developed and patented a proven algorithm. Unlike other algorithms in the market, this advanced algorithm looks at the rate of overall traffic types, specific traffic parameters, as well as the ratio of different parameters within the IP flow. The Radware security solution can detect attacks regardless of their volume, including targeted application attacks that may or may not have a volumetric component.

Let's consider a simple scenario to better understand Radware's approach to attack detection. A grandmother comes for a visit at the same house time every afternoon to care for her grandchildren. Traditional rate based or volumetric solutions would measure and see that one person (the grandmother) arrives at that door every day. As long as one person, no matter who they are, comes to the door, traditional solutions would not detect any danger. Only if more than one person showed up at the door is an attack signaled.

In contrast, Radware looks at both rate and baselines the parameters (or ratios) of the traffic. In this case they would see that the grandmother arrives at the door every afternoon. But in addition to measuring the rate (one person per afternoon) they would also notice several parameters about her:

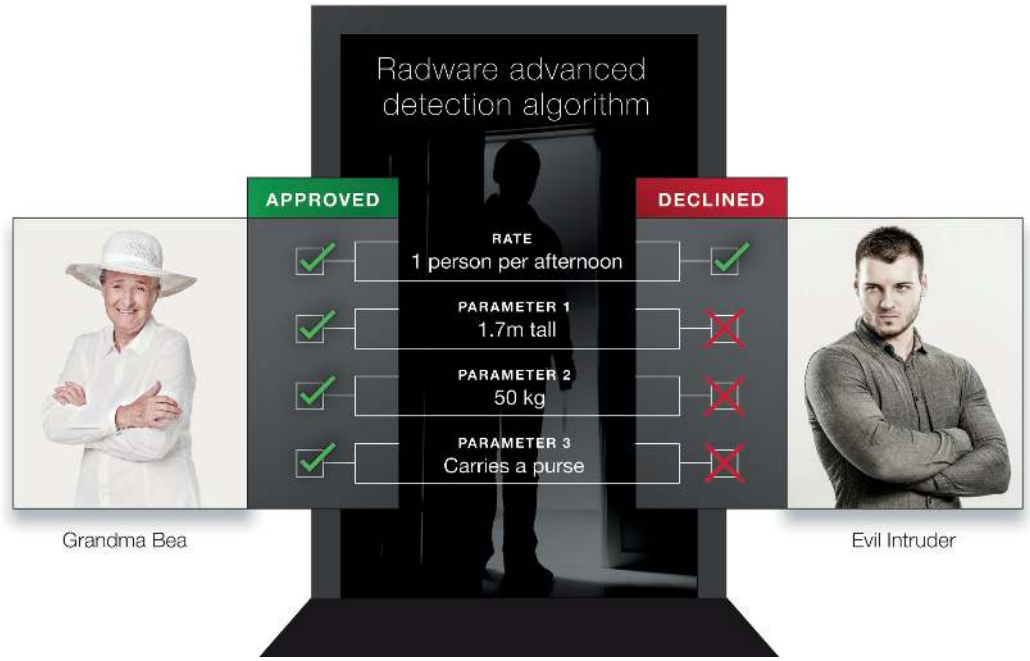
A. Rate: 1 person per afternoon
B. Parameter 1: 1.7m tall
C. Parameter 2: 50 kg
D. Parameter 3: Carries a purse

Radware then compares these parameters to anyone who arrives at the door.

Now let's say an attacker arrives at the same door one afternoon:

A. Rate: 1 person per afternoon
B. Parameter 1: 2.0 m tall
C. Parameter 2: 135 kg
D. Parameter 3: Carries a knife

Radware sees that the parameters for the attacker do not match the baseline parameters for the grandmother. Radware signals an attack. Traditional solutions, which look only at rate, still identify one person at the door and let the attacker in because no anomalies were detected.



With this approach, Radware generates few false positives. In our example, the grandmother comes to the door and brings several other grandmothers with similar features. Radware identifies this visit correctly as a flash crowd of normal traffic. Five grandmothers with the same "normal' parameters (height, weight, purse) would be correctly identified as a heavy but normal traffic pattern and therefore not an attack. Traditional

solutions would instead see the five grandmothers only as five times the normal rate and therefore it would falsely identify an attack.

Using a Behavioral Engine to Generate Multivector Representations

Radware looks at multiple parameters of the traffic using a behavioral engine. This behavioral engine analyzes multiple IP parameters within TCP (connection oriented) and UDP (connectionless) flows, as well as ICMP (router discovery) and IGMP (IP multicast) messaging. Radware also measures different parameters on HTTP and DNS traffic, detecting attacks trying to target the server.

By measuring all these parameters, Radware can then create a multivector mathematical representation of the normal or baseline traffic flows. This multivector representation is unique to any particular network and can then be used to make mathematical comparisons to incoming flows and determine Degree of Membership (DoM), how similar these flows are with regard to all measured parameters.

For example, if the Radware behavioral engine identifies a TCP flow, it measures both the overall rate of the TCP traffic as well as the rate of:

- SYN Packets- SYNchronize packet to request initial TCP handshake
- SYN + ACK Packets- Synchronize ACKnowlegement packet responding to initial request
- FIN+ACK Packets-Acknowledges receipt of final data from host
- RST Packets-Resets the connection
- TCP Frags-TCP fragmented packets

Based on these rates and the ratio of these different parameters to the overall TCP traffic, Radware is able to characterize this flow and determine DoM for the traffic compared to the running baseline the engine identifies for TCP traffic.

Similarly with a UDP flow, Radware measures the overall rate of UDP traffic as well as the rate of UDP Frags-UDP fragmented packets.

In either case of TCP or UDP, Radware is able to then determine the difference between a flash crowd or heavy traffic which follows the normal traffic ratios for a particular network (High DoM - therefore good traffic) and an attack which would have different ratios (Low DoM - therefore an attack) as shown in Figure 1.

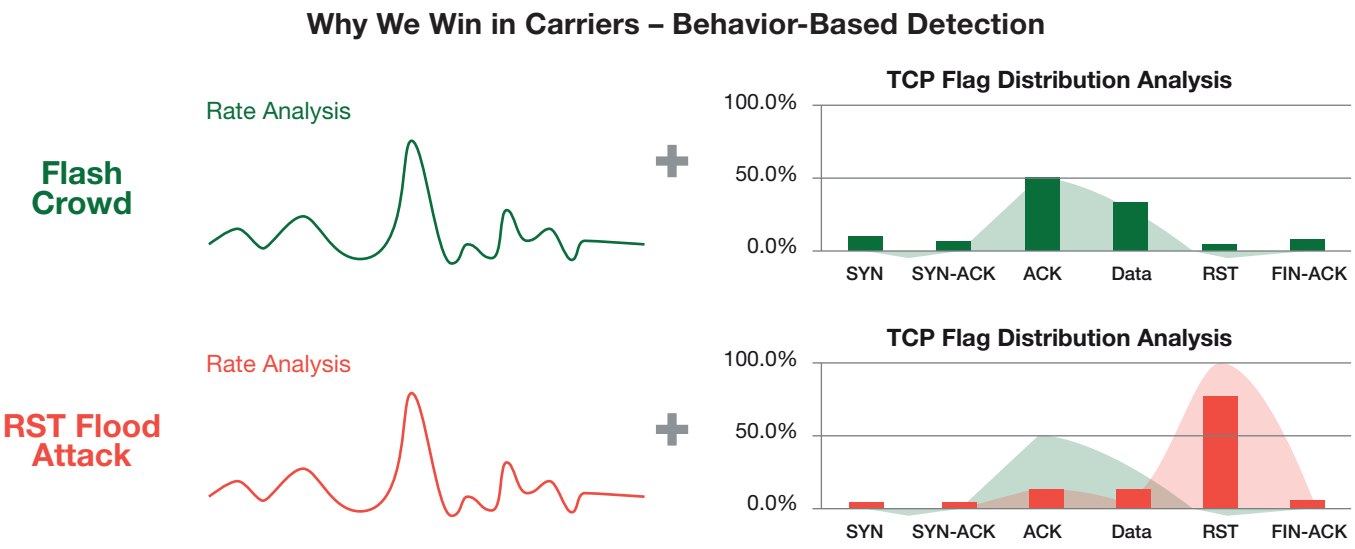


Figure 1: Radware's advanced algorithm can determine whether traffic is an acceptable flash crowd where the TCP flag distribution indicates a normal traffic or an RST attack flood indicated by very high TCP RST and a low number of TCP ACK flags that needs to be mitigated.

Using these sophisticated baselines, Radware's detection algorithm sorts the traffic flows into three major categories based on the DoM.

1. Normal: High degree of correlation with existing baseline and therefore good traffic
2. Suspect: Medium degree of correlation with existing baseline and therefore traffic should be further analyzed and challenged
3. Attack: Low degree of correlation with existing baseline and therefore traffic should be mitigated

Verifying Good vs. Bad Traffic

Radware's superior detection algorithm inspects suspect traffic and utilizes best-in-class challenges and response mechanisms to verify good traffic from attack traffic.

Challenge response mechanisms are when one party sends a question (or challenge) and the other party sends an answer (or response) to verify legitimate users versus bots. Radware offers advanced challenge response mechanisms for suspect traffic in DNS, HTTP and SIP.

Radware challenges combine simple passive challenges with more advanced active challenges. This combination enables escalation starting with simple passive and selective challenge requests, moving through advanced active and collective challenge requests and responses when needed.

Using DNS as an example, the Radware DNS challenge and response and escalation mechanism includes the steps outlined in figure 2.

Figure 2: Radware escalates from selective and collective challenges, then to selective and collective rate limits as needed to verify traffic.

The Radware detect algorithm challenges the DNS sources to verify that they are legitimate users rather than attackers. During the initial challenge, Radware ignores the first packet that it receives from a DNS source because, according to the DNS standard, a new DNS packet should be retransmitted within a limited timeslot containing the same Qname (domain name being queried).

To issue and track challenges and to verify that the DNS source responds to the challenges, Radware uses the Selective Discard Mechanism (SDM), a statistical table and function. Each entry in the SDM table receives a score for each query reaching the table. When a source answers the challenge correctly, the source's score increases and then gets listed in the internal DNS authentication table where it is whitelisted as a known good user for a specified period of time. When a source fails to answer a challenge correctly, its score decreases, making it more likely to be an attacker and less likely to be whitelisted.

To avoid misclassification of proxy devices, either as legitimate or as attacking entities, the SDM reduces source scores with each new query that reaches it and is not challenged. When a source falls below a certain score, it will be challenged again. A proper response to the challenge will raise the source's score and move it back to the whitelist where the next few queries from it will not be challenged. For scenarios in which the passive DNS challenge has passed but the detect algorithm still sees a DNS attack is present, Radware can escalate to an active DNS challenge in which Radware sends a DNS reply to the client with the TC (truncate) bit set to force the DNS client to move from UDP to TCP. The Alteon serves as a gateway converting from TCP to UDP for the server.

There are also several challenge escalations to use with HTTP that are applied only to suspicious traffic. The attack can then be identified and mitigated. Radware uses different HTTP challenge mechanisms such as cookie insertion, HTTP 302 redirect, Java script injection and polymorphic challenge. Should the session pass the challenge/response, then the session is whitelisted and passed, otherwise it is identified as an attack.

Radware's Detection Algorithm Earns Its Distinction

In summary, Radware's detection algorithm has proven its superiority to competing algorithms in deployments in leading enterprises and Tier 1 carriers worldwide. Using Radware's solution, organizations are able to detect sophisticated attacks and offer advanced challenges to individual flows that enable better detection of attacks with no impact to good traffic, enabling availability SLAs for good traffic and while thwarting the most sophisticated attackers.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 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: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.