INTRODUCTION

Distributed Denial of Service (DDoS) attacks are some of the oldest of Internet threats. Despite that, due their simplicity and effectiveness, they continue to be a top risk for public services around the world. As protections have evolved, the technology used by hackers has adapted and become much more sophisticated. New attack types now target applications and services, and not only are bulk layer 3 and 4 DDoS events becoming more sophisticated but many times they are masked in apparently legitimate traffic, or combined in unique new "zero-day" attacks, making it very difficult to detect them.

This whitepaper discusses some of the technologies used traditionally to detect and mitigate DDoS attacks, how they evolved, and why the state-of-the-art technology must rely on Application Specific Integrated Circuits (ASICs), inline symmetric or asymmetric deployments, a wide-spectrum of analysis methods covering from layer 2 (data-link layer) to layer 7 (application layer) of the OSI model, and why this must be done with high-performance, hardware-based architectures.

As part of the discussion we will explain some features and benefits of the Fortinet FortiDDoS approach, the differences compared to conventional devices based solely on stateful or stateless inspection, and the advantages of behavior-based methods of attack detection built on customized hardware vs. signature based methods built on standard CPU/RAM architectures.

WHAT IS A DDOS ATTACK?

ROUTER

No matter how simple or complex, DDoS attacks are aimed at exhausting the resources available to a network, application, or service so that legitimate users are denied access. These attacks usually are originated by a group of client computers that are either hijacked with malware or are volunteered by their owners.

TYPES OF DDOS ATTACKS

- **Common DDoS Attacks:** There are many kinds of attacks that are widely used today including older methods from the early days of the Internet to the latest advanced layer 7 attacks that target application services. SYN flood and HTTP GET floods are the most common and are used to overwhelm network connections or overload the servers behind firewalls and intrusion protection services (IPS).

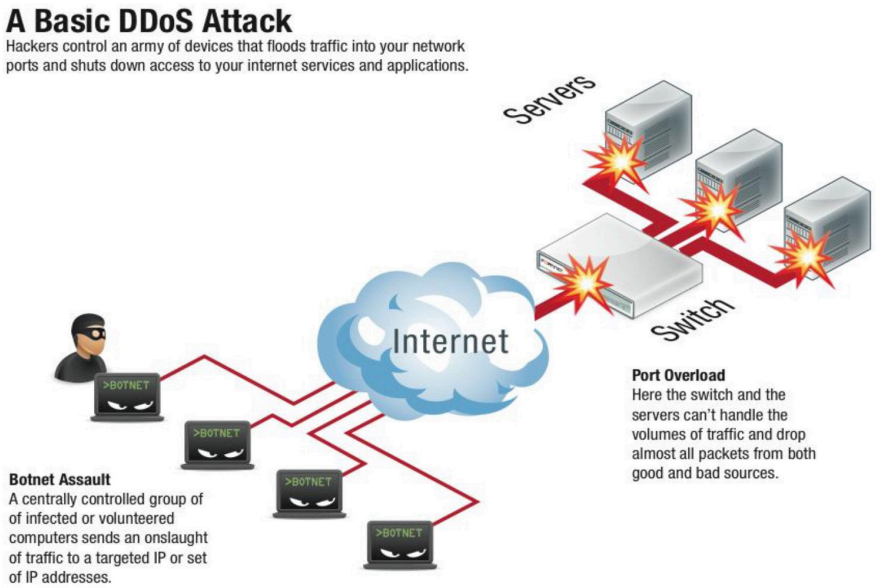

Figure 1: An example of a basic DDoS attack on a network switch and servers.

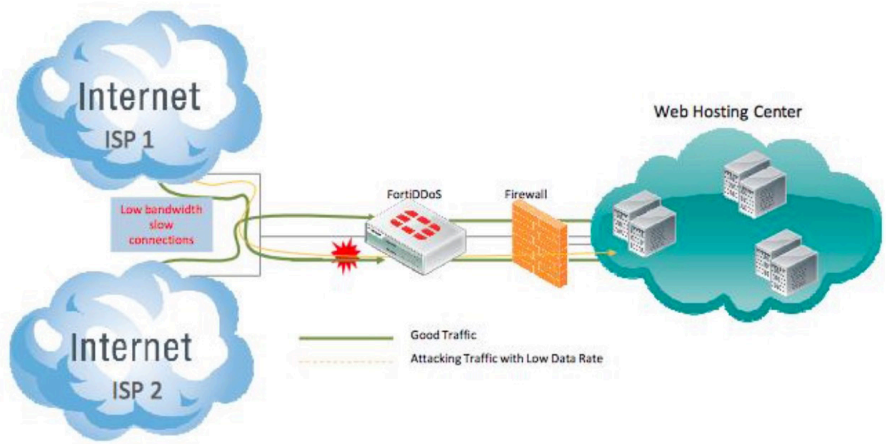

FIGURE 2: ATTACKS UTILIZING LOW BANDWIDTH TO EVADE DETECTION

- **Advanced Application layer DDoS Attacks:** Application layer attacks use far more sophisticated mechanisms to attack your network and services. Rather than simply flooding a network with traffic or sessions, these attack types target specific applications and services to slowly exhaust resources at the application layer (layer 7).
- Application-layer attacks can be very effective at low traffic rates, and the traffic involved in the attacks can be legitimate from a protocol perspective. This makes application-layer attacks harder to detect than other DDoS attack types. HTTP Flood, DNS dictionary, Slowloris, etc., are examples of application-layer attacks.

DDOS ATTACK MITIGATION PLATFORMS

Just as attacks were adapting to the new reality, DDoS defenses were adapting too, and evolved from being an integral part of existing protection technologies such as firewalls and IPSs to independent devices.

FIREWALL / IPS DDOS PREVENTION

Firewalls were the first choke-point devices used to separate trusted from untrusted networks. Then intrusion detection systems (IDS) and intrusion prevention systems (IPS) followed. It was natural that the most basic Denial-of-Service attacks were an integrated protection on such devices.

Conventional firewalls (packet filters, proxies, or stateful-inspection firewalls) look into packet headers to identify if there is a rule allowing traffic from a given source to a given destination. They drop connection attempts from a not allowed source or to a forbidden destination. Firewalls are able to observe if a session has been established or not by the peers (client and server) trying to establish a conversation (a connection). Once a session has been established, a firewall device keeps state of all connections allowed by its security policy, even for stateless protocols such as UDP or ICMP, and it does so from when the connection begins until the connection ends. This information is held on session tables, and in order to keep track of connections, even those that have not been completed yet have to be stored on the session table, because it is necessary for the firewall to determine if the next packet is valid or not. But the nature of this operation makes a firewall vulnerable to attack. The number of connections on the session table has a limit, and once the limit has been reached the firewall comes to a state where it cannot take any additional connections. Also, since it needs to observe the session completely, a firewall device cannot work on an asymmetric-routing scenario where only incoming or outgoing traffic is seen.

Almost every modern firewall and intrusion prevention system (IPS) claims some level of DDoS defense. Some Unified Threat Management (UTM) devices or next-generation firewalls (NGFWs) offer anti-DDoS services and can mitigate many DDoS attacks. Having one device for firewall, IPS, and DDoS is easier to manage and less complex to deploy, but a single device to do all the protection might be easily overwhelmed with volumetric DDoS attacks. Besides, resource-intensive protection necessary to detect and defend against sophisticated layer 7 detection mechanisms cannot typically be done on a firewall or IPS device, especially if it lacks the power of a dedicated processor or ASIC. Another trade-off is that enabling DDoS protections on the firewall or IPS may impact the overall performance of a single device, resulting in reduced throughputs and increased latency for end users. Due to this, enabling anti-DDoS mechanisms on firewall or IPS devices should be done with care and deployment of dedicated anti-DDoS protections in addition to the firewall or IPS is recommended in highly critical environments.

DEDICATED SOFTWARE-BASED PLATFORMS

Once technology vendors and security officers realized it was difficult to leave anti-DDoS protection to existing devices, some software-based products were launched. The idea was to pack a hardened operating system with additional programmed intelligence on software that could be installed on general-purpose servers. If you needed more performance, you only had to add more memory and CPU and you had it, until it reached the limits of the hardware architecture.

These solutions were typically based on signatures, meaning they were trying to understand patterns on how malicious traffic behaved. On this approach, a group of researchers would observe a new attack, analyze it and once it was understood, they would develop a pattern or signature of the attack, so the next time traffic with the

characteristics of the attack was seen, an action would be triggered. This was very similar to how IPS systems operated with the difference that they were optimized to catch DoS and DDoS attacks and not necessarily exploits, worms, bots, or other malware traversing the network.

This approach was not effective to mitigate zero-day attacks, which are commonly used for DDoS attacks. And this is because to detect an attack, somebody has to analyze it first in order to produce a signature.

The second problem with this software and generic platform approach, according to the IDC Report, DDoS Prevention: Time for "Defense in Depth," published April 2014, is that anti-DDoS software-based platforms can become overwhelmed by traffic volume and lead to false positives. And:

> "Signature-based defenses are strong at detecting known attack methods quickly and efficiently. They are able to run inline and immediately detect and drop or clean malicious traffic when an attack starts. However, when a new attack method arises, or an attack uses legitimate traffic for malicious purposes, signature-based defenses may not detect the attack. Behavior-based solutions solve this problem by digging deeper into the types of traffic and how resources react to requests and correlating with threat intelligence feeds and other sources to determine if traffic is malicious or not, regardless of whether it appears legitimate or is the result of a zero-day exploit"

HARDWARE-BASED SOLUTIONS

To solve the DDoS puzzle there are some key issues:

1) **Price-Performance:** The anti-DDoS solution cannot be the bottleneck on a network. It must have sufficient resources, at acceptable cost, to monitor 100% of the packets traversing the Internet link at line rate. Sampling packets, as several competitors with weaker hardware must do, can allow clever attacks to bypass the anti-DDoS device. It also must process all of the connection context information as fast as possible to minimize in-line latency. This means it has to correlate the current packet with packets that came from the same source, went to the same destination, and infer if packets that have similar (not necessarily the same) characteristics could be part of malicious behavior.

2) **Wide-spectrum Analysis:** DDoS attacks are complex. You can have thousands of connection attempts trying to reach the same target. That is a volumetric attack, which is (relatively) easy to detect. However, if a relatively small group of valid (from the protocol standpoint) HTTP connections that are already established are trying to read the same image file several times or read non-existent pages (an HTTP URL Get Flood), that might require more computing resources, more analytics, and a different approach. So, using techniques from keeping counters or state tables (stateful awareness, not to be confused with stateful inspection) or having inference machines to correlate traffic that has the possibility of becoming offensive at some point, is important.

3) **Secure:** the anti-DDoS device must be built in such a way that is not only invisible to the protected network, but the possibility of overwhelming it (that is, exhausting its resources) does not exist. If an attacker can somehow saturate the resources of your anti-DDoS device, he has succeeded in his DDoS attack.

Due the points above, it became critical to have solutions that could offer high performance, wide and deep analysis capabilities, and the ability to operate with low to zero risk of being a DDoS target. This is why hardware-based solutions came into the market.

FORTIDDOS

Powered by Application Specific Integrated Circuit Traffic Processors (FortiASIC-TP2) the FortiDDoS family of purpose-built network appliances provides effective, fast protection against DDoS attacks. FortiDDoS helps to protect Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks, while letting legitimate traffic flow without being impacted.

FortiDDoS uses a 100% adaptive behavior-based method to identify threats. It learns baselines of normal application activity and then compares traffic against those baselines while automatically adapting to normal traffic growth. Should an attack begin, FortiDDoS will see this as an anomaly and immediately take action in real time to mitigate it, usually in less than two seconds. Users are protected from known attacks and from unknown zero-day attacks, as FortiDDoS doesn't need to wait for a signature file to be updated.

Fortinet is the only company to use a 100% custom ASIC approach to its DDoS products, which allows massively parallel processing of 1000's of traffic parameters at significantly lower cost and energy requirements of traditional CPU or CPU/ASIC hybrid based systems. The second-generation FortiASIC-TP2 traffic processor provides detection and mitigation of all layers 3, 4, and 7 DDoS attacks for both inbound and outbound traffic.

Unmatched Performance: Using behavior-based detection and ASIC DDoS processors, FortiDDoS detects and mitigates more DDoS threats, including sophisticated low-volume application layer attacks. It also detects anomolies faster than any other solution available on the market today.

Lowest Latency: It's single-pass, hardware-based DDoS detection and mitigation engine creates less than 50 microseconds of latency in the data stream - almost 40% lower than competitive products.

Network Virtualization: FortiDDoS supports different Service Protection Profiles to discretely apply different protection policies to individual servers or sub-networks providing granular protection to your network. An attack on one protected network segment does not impact other segments. This feature is not only beneficial in supporting multiple layers of defense but also is a cost containment and administration-friendly feature for organizations that have multiple business entities to protect, and that need unique policies for each.

Virtual policy instances can also be effectively used in defense escalation. Rather than having a single set of policies, multiple sets can be defined in advance, such that the organization can automatically apply a more stringent set of policies if an attack escalates above customer-defined thresholds.

FORTIDDOS KEY FEATURES AND BENEFITS

100% Behavioral

FortiDDoS doesn't rely on signature files that need to be updated with the latest threats so you're protected from both known and unknown (zero-day) attacks.

100% Hardware

The FortiASIC-TP2 transaction processor provides full bi-directional detection and mitigation of layer 2, 3, and 7 DDoS attacks for industry-leading performance.

Continuous Attack Evaluation

Minimizes the risk of "false positive" detection by re-evaluating the attack to ensure that "good" traffic isn't disrupted.

Congestion Resistant

FortiDDoS won't easily be overwhelmed and succumb to a DDoS threat, with high throughput rates and full line rate detection and mitigation.

Automated Learning

With minimal configuration, FortiDDoS will automatically build normal traffic and resources behavior profiles saving you time and IT management resources.

Multi-Attack Protection

By understanding behaviors FortiDDoS can detect any DDoS attack from basic Bulk Volumetric to sophisticated layer 7 SSL-based attacks without the need to decrypt traffic.

SOFTWARE-BASED VS HARDWARE-BASED DDOS MITIGATION – AN EXAMPLE

Figure 3 - Signature Based: Attacks take up to 120 seconds to match against signature profiles.

- All traffic is blocked for the duration of the attack, including "good" traffic from legitimate users.
- False positives must wait until system perceives attack has stopped.

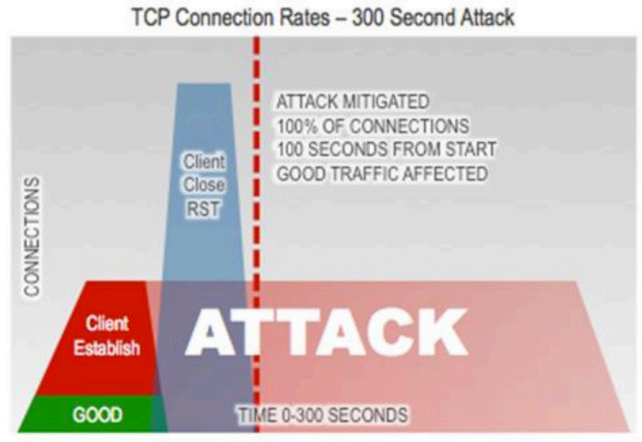

Figure 3: Competitor 300 Second Attack

Figure 4 - FortiDDoS Behavior-Based: Attack is identified and mitigated in less than 30 seconds.

- Traffic is slowed, but still "good" traffic is permitted.
- Repeated attack reevaluation minimizes risk of false positives.
- IP Reputation blacklists offending IP addresses.

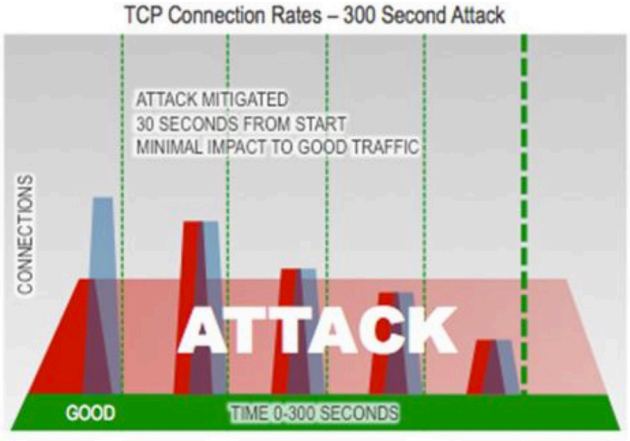

Figure 4: FortiDDoS 300 Second Attack

ADVANTAGES OF USING FORTIDDOS OVER A TYPICAL FIREWALL DEVICE

Today even inexpensive hardware routers claim they have some sort of protection against DDoS attacks because they are stateful inspection firewalls. Let's clarify this matter.

Dynamic packet filtering, dynamic filtering, stateful connection analysis, stateful flow analysis, stateful analysis, stateful inspection, stateful packet inspection are all terms that refer to methods that maintain state information for a connection in order to be able to protect it. The idea behind this is to observe the packets that belong to connection from when it begins until it ends, and analyze it while the connection changes from state to state, allowing potential analysis of deeper protocol information, not only based on the headers of TCP packets but also analyzing upper-layer protocols. Connections are important for communication because they provide a reliable way to transmit data, allowing the devices involved to know if there was an error in the path between the two endpoints involved in the connection. The state of a connection is defined by a state table (a portion of

memory where each connection is recorded along with its source-destination information and current state) and is analyzed by a state engine (an engine that defines the valid states and the correct transition from state to state) that resides on the operating systems of the client and the server as well as some intermediate devices, like firewalls. There are messages that are used to establish a connection, which have certain order and characteristics. There are attacks (both DDoS and non-DDoS) that can be implemented against the state engines and state tables of operating systems. Network security devices that are aimed at protecting such clients and servers need to be aware of the states of a connection in order to properly defend it. An anti-DDoS product would be incomplete if contained no mechanism to properly analyze connection states, analyze the application-information of a connection, and/or defend against attacks against the state tables resident in downstream firewall and server operating systems.

FortiDDoS is not a stateful device, but implements analysis that uses stateful techniques to better protect against specific DDoS attacks. To protect against certain attacks FortiDDoS needs to understand the state of a connection, and for that it needs to be able to understand, analyze, and store state information. This is what allows FortiDDoS to protect against attacks using anomalies such as TCP state violations, Out-of-TCP-Window Packets and state transition anomalies. For example a whole class of DDoS attacks will use ACK, RST, and FIN packets which are connection-ending signaling packets when no connection was ever active. Knowing that there is no connection allows FortiDDoS to reject these packets instantly as "foreign packets," so they have zero impact on the users or servers. Without the connection knowledge there are only two options to detect these as anomalies - set an arrival rate threshold above which all packets are dropped - affecting good traffic as well as bad, or rate-limit the arrival of all ACK/RST/FIN packets also affecting all users. Neither of these options is very attractive for the customer and most competitors do not attempt to stop ACK, RST, or FIN Floods for that reason - a gap in the defense coverage.

FortiDDoS does not expose its own IP address to the data stream so it cannot be attacked directly. FortiDDoS goes to great lengths to ensure that both memory and real-time resources cannot be overwhelmed by the data rate, packet rate, or number of sources used in attacks. Its data throughput and packet processing rates (with 100% sampling of packets) are industry leading. For example a SYN attack over 10 GbE internet connection can theoretically generate about 16 million packets-per-second (16 Mpps) through the link. FortiDDoS can 100% sample up to 24 Mpps. A "leading" stateless vendor's flagship product can only manage 8.6 Mpps-11.4Mpps, according to its public documentation - not enough to fully protect a 10 GbE link.

However, since some customers believe that state awareness is risky in certain environments, this stateful analysis can be disabled via configuration in FortiDDoS.

ADVANTAGES OF USING FORTIDDOS AND OVER A TYPICAL IPS DEVICE

Typical IPS devices also claim some anti-DDoS protection. While it is true they can (and do) incorporate some basic protection, the majority of current IPS products evolved from software-based solutions that were signature-based. Their strengths came from having a large group of analysts (either their own, third-party or community-based) discovering new attacks, programming signatures to detect them, and providing those signatures to their customer bases.

Signature-based solutions don't do a complete job when it comes to anti-DDoS protection. The logic behind their engines sand signatures is built on detecting a pattern in the flow of traffic, reading from the packet payloads on single connections, which is good for slow attacks from single sources. Detection of most DDoS attacks doesn't come from analyzing a single flow of traffic but from analyzing things like how many times, from how many sources, a certain resource (a file for example) has been requested from a web server. There is a pattern here, but you don't see that as part of some text or code traveling within a packet. Patterns are seen across time, many thousands of sources, and many destinations.

Typical IPSs run their protections on standard CPUs, not custom processors. They are designed to deeply inspect the standard flow of traffic, not the excessive traffic generated by DDoS attacks.

CONCLUSIONS

A behavior-based, dedicated custom-processor product is the most viable solution for anti-DDoS protection due to its inherent strengths in performance (high throughput, high packet processing, 100% sampling and low latency), reliability, massively parallel analysis capabilities, and self-security. anti-DDoS protection is a "big data" problem requiring knowledge of millions of source IPs and the packets they are sending, which needs massively parallel computations to sort the good data from the attack data in real time. Standard CPU/RAM architectures do not perform as well by a factor of three or more.

"... behavior-based solutions [are] more viable and, in many cases, a more desirable option." says IDC's John Grady in his April 2014 report **DDoS Prevention: Time for "Defense in Depth.**"

A hardware-based DDoS appliance can be a predictable cost-effective solution that provides full layer 3, 4, and 7 DDoS protection for your data center for both volumetric and "slow" attacks.

FortiDDoS offers advanced performance, and **100% behavior-based detection that eliminates the need for signature updates.**

Behavioral-based adaptive methodologies and dedicated hardware-based ASICs used by FortiDDoS outperform DDoS appliances that rely primarily on signature matching and CPU/RAM or CPU/ASIC combinations to protect against DDoS attacks.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

SUNRISE OFFICE
13450 W. Sunrise Blvd.
Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Jan 04, 2017