FORTINET

White Paper

Is Your Data Center Ready for Today's DDoS Threats?

DDoS attack types, protection methods and testing your detection and mitigation defenses

Introduction

Distributed Denial of Service (DDoS) attacks are some of the oldest Internet threats and continue to be the top risk to networks around the world. As protections have evolved, the technology used by hackers has adapted and has become much more sophisticated. New attack types now target applications and services, and many times they're masked in bulk layer 3 and 4 DDoS events making it difficult to detect them.

The financial services industry is one of the largest targets of cyber criminals for DDoS attacks followed closely by the government sector. Besides disrupting Internet operations through a brute-force data onslaught, DDoS attacks have recently been used to hide more sophisticated attempts to break into financial and e-commerce information. These attacks often have the intent of disrupting operations mostly through the destruction of access to information.

Most organizations spend a lot of time and effort to choose a DDoS mitigation solution, however often they don't provide the same level of diligence in testing their defenses. Relying on a vendor's word and datasheets isn't the best way to make sure you're protected from a DDoS attack. There are many ways to test your DDoS defenses ranging from free options to dedicated appliances that can simulate a broad range of basic and advanced DDoS types so you don't have to wait for your first real attack to uncover the weak links in your mitigation solutions.

Whatever approach you choose, the most important element of testing is to create realistic scenarios based on your unique valid user traffic. Understanding what attacks are blocked is important only in the context of determining whether legitimate traffic gets serviced acceptably. Should the defenses block all traffic, good and bad, the DDoS attack might be stopped, but the end result to the company might be catastrophic losses.

Business Challenges

- Network Security
- Application Availability
- Business Continuity
- DDoS Protection

Segments

- Financial Services
- Government
- Enterprise
- Internet Data Center
- Managed Services

The Financial Services sector is a top target of DDoS attacks to disrupt business operations and to mask breaches of sensitive data

Testing information provided by:

ixia

What is a DDoS Attack?

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. The effort is usually a highly coordinated event that attempts to overwhelm network bandwidth and server capacities of the targeted victim's network operation environment.

A few years back, it was common to use spoofing techniques where a hacker would actually use very few machines (or even just one) to spoof multiple IP addresses. That has given way in recent years to the rise in "botnets." A botnet is a group of coordinated devices, usually computers and smart phones that are either infected by malicious code or are volunteered to participate in an attack. The latest method used by attackers is to launch DDoS events from servers in data centers that have large amounts of bandwidth available to them. Without the need to recruit thousands of devices, a motivated hacker can launch a broad-based attack by only getting access to a handful of data center servers.

> Most news stories focus on large-scale DDoS events like the recent 400 Gbps attack on CloudFlare in 2014. Although these are significant, most successful DDoS attacks today are much smaller as they target layer 7 services.

What Can Trigger a DDoS Attack?

DDoS attacks are launched generally for three categories of motivations: political, retaliatory and financial. Political attackers target those that disagree with their political, social or religious beliefs. When a botnet gets shut down or major cyber crime ring is busted, it can trigger retaliatory attacks against those who aided or assisted the authorities. Financially motivated attacks are a pay-to-play scheme where hackers are compensated by a third-party to conduct the attack on their behalf. With each motivation the results are the same; your network and online services are down, and can be for an extended period of time.

Common DDoS Attacks Today

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). Please see the sidebar article for more information on common attack types.

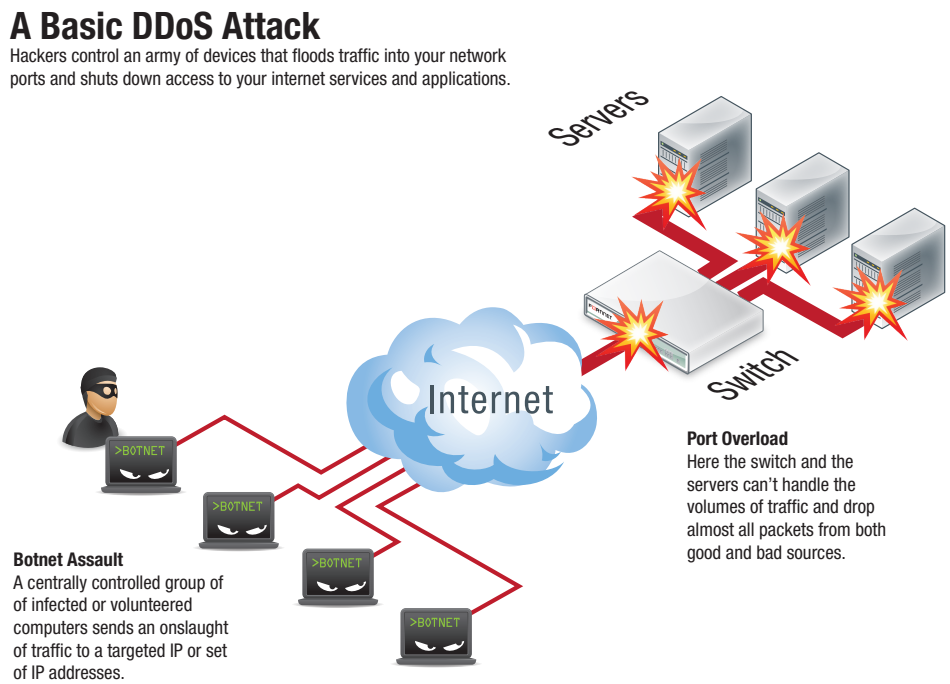

Figure 1: An example of a basic DDoS attack on a network switch and servers.

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 level (layer 7).

Application layer attacks can be very effective using small traffic volumes, and may appear to be completely normal to most traditional DDoS detection methods. This makes application layer attacks much harder to detect than other basic DDoS attack types. Most ISPs and DDoS mitigation service providers use basic methods to protect you from large-scale attacks, however they don't have the sophisticated detection tools to intercept these smaller application-level threats and normally pass them through to your network.

DDoS Protection Options

There are many options available for DDoS attack mitigation ranging from simple DIY server configurations to advanced data center-based hardware solutions. Most ISPs offer layer 3 and 4 DDoS protection to keep your links from becoming flooded during bulk volumetric events, however they don't have the capability to detect the much smaller layer 7-based attacks. **Data centers cannot rely on their ISP alone to provide a complete DDoS solution that includes application layer protection**.

The following are the top three mitigation solutions that most mid-sized and large organizations use if they are serious about defending against all DDoS attacks; cloud-based DDoS Service Providers, existing Firewall/IPS equipment and Dedicated DDoS Attack Mitigation Appliances.

DDoS Service Providers: There are many hosted cloud-based DDoS solutions that provide layer 3, 4, and 7 mitigation services. These can range from inexpensive plans for small websites to large-scale enterprise plans that can cover multiple ones. They're usually very easy to set up and heavily advertise to small and mid-sized organizations. Most offer customized pricing options and many have advanced layer 7 detection services for large organizations that require sensors to be installed in the data center. Many companies opt to go this route, but most experience unpredictable and significant overage charges when they're hit with high-volume DDoS attacks. They also are disappointed with performance as the service providers redirect DDoS traffic to mitigation centers instead of stopping it real time which is especially problematic for typical short duration attacks.

Firewall or IPS: Almost every modern firewall and intrusion protection system (IPS) claims some level of DDoS defense. Advanced next generation firewalls (NGFWs), such as Fortinet's FortiGate products, offer DDoS and IPS services and can mitigate many DDoS attacks. Having one device for firewall, IPS and DDoS is easier to manage, but one

Common DDoS Attack Types

Bulk Volumetric

Designed to overwhelm and consume available internet bandwidth or overload servers.

SYN Flood: Spoofed SYN Packets fill the connection table of servers, and all other devices in your network path

Zombie Flood: In zombie or botnet floods, non-spoofed connections overload network and application services.

ICMP Flood: ICMP packets, such as those used for "ping", overload servers and network connections.

TCP/UDP Port Flood: TCP/UDP packets overload the servers and network ports not being used for a service, such as TCP port 81.

Fragment Flood: Fragmented packets overload servers.

Anomalous Packet Flood: Deliberate or accidental packet errors in scripts by hackers overload network equipment and servers as they attempt to deal with anomalies.

Unwanted Geographical Area Floods: Packets are flooding in from an unwanted or potentially malicious geographic area (country, region, etc.).

Blended Attacks: More and more DDoS events are using combinations of the basic attack types and some are even masking service-level attacks within high-volume basic ones to throw off detection services.

DNS Amplification: The attacker targets DNS servers and uses the DNS EDNS0 protocol to increase a DNS response message sent to an attack target by a factor of 70.

Application Layer Attacks

Smaller, more sophisticated attacks that target layer 7 services on servers like HTTP, SMTP and HTTPS.

HTTP GET: These attacks involve connection-oriented bots that attempt to overload servers and connections on service ports (such as HTTP) by mimicking legitimate users.

HTTP POST: POST body messages are sent at a very slow rate and disrupt proper connection completion.

HTTP Slow Read: Attackers force servers to send a large amount of data, however it forced to be sent in many small fragments and read at a very slow rate by the receiver.

Slowloris: Using HTTP GET, attackers launch multiple partial and time-delayed HTTP refer headers to keep the connections open as long as needed to deplete resources.

HTTPS: Similar to HTTP attacks, these attack SSL services on servers.

SMTP: Attacks targeted at SMTP mail server services.

VoIP: Attacks targeted at SIP INVITE services.

Layer 7 DDoS Defense Options

The three primary solutions most companies use to protect their data centers from advanced application layer DDoS attacks.

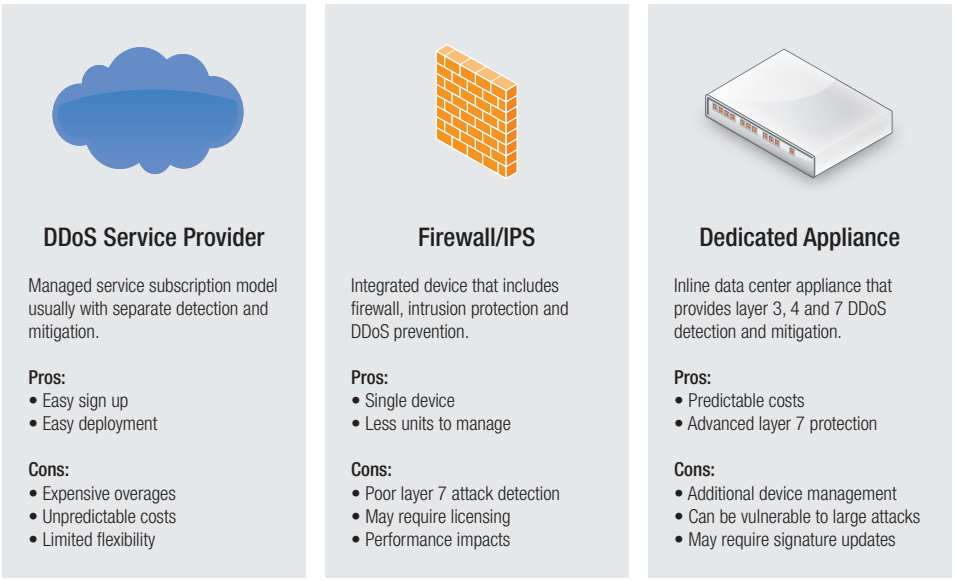

Figure 2: The three options most organizations deploy for advanced DDoS protection when they need more than the bulk layer 3 and 4 mitigation their ISP offers.

device can easily be overwhelmed with volumetric DDoS attacks and doesn't have the sophisticated layer 7 detection mechanisms as other solutions offer. 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.

Dedicated DDoS Attack Mitigation Appliances: These are dedicated hardware-based devices that are deployed in a data center that are used to detect and stop basic (layer 3 and 4) and advanced (layer 7) DDoS attacks. Deployed at the primary entry point for all web-based traffic, they can both block bulk volumetric attacks and monitor all traffic coming in and leaving the network to detect suspicious patterns of layer 7 threats. By using a dedicated device, expenses are predictable as the cost is fixed whether you suffer from one attack in 6 months or are attacked every day. The trade-offs are that these devices are an additional piece of hardware to manage, lower-bandwidth units can be overwhelmed during bulk-volumetric attacks, and many manufacturers require frequent signature updates.

Dedicated hardware-based DDoS attack mitigation solutions come in two primary versions, Carrier and Enterprise. Carrier versions are large solutions designed for global ISP networks and are very expensive. Most organizations that want to protect their private data centers usually look at the Enterprise models to provide cost-effective DDoS detection and mitigation. Today's models provide capacities that can handle large-scale volumetric attacks for 100% layer 3, 4 and 7 protection or can be used to supplement basic ISP-based bulk DDoS protection with advanced layer 7 detection and mitigation. Although these devices require an up-front investment compared to hosted solutions, they are generally much less expensive in the long run when overage charges are factored in to total costs.

You'll need to choose the best option that meets your requirements. Each has its pros and cons. However no matter which defense strategy you decide on, don't rely on anyone else telling you that you're protected from DDoS attacks. Once you're up and running, you need to validate that your data center is protected and that's where a solid and regular testing program is required.

Testing your DDoS Defenses

How do you know if your roof leaks if it isn't raining? DDoS attacks can come at any time, and from any source. You may have already experienced an attack on your data center or if you haven't, are concerned enough about your mission-critical network services that you don't want to wait until the threat happens. Whether you have a proactive DDoS attack mitigation strategy, are in the market for one, or just want to determine how a DDoS attack would impact your data center, you need a method to test your vulnerabilities that's better than waiting for the first storm to hit.

DDoS Test Planning

Before you roll up your sleeves and dig into the actual testing of your DDoS vulnerabilities you need a plan. DDoS attacks have evolved into some of the most sophisticated threats and require more than just simple testing of a handful of points in your infrastructure. Today's attacks still involve many of the traditional bulk methods used to overwhelm your network ports and services, however many of the advanced threats target the complex interactions between

network elements that won't be uncovered unless you know where to look. The following are the key things you need to include in your testing plan:

Inventory of web-facing infrastructure: What elements are exposed to attackers? Which are the most vulnerable? How much bandwidth do you have? These are the places an attacker is going to get in and you need to make sure you know every possible route and what capacities you have that may become bottlenecks during a DDoS event.

Identification of key systems/assets: Which systems are critical to your business should they be attacked? Which ones need the most protection? This includes all the elements behind your entry points that an attacker can disrupt such as web servers, databases, DNS servers, and routers.

Interconnectivity points/dependencies: If you lost your authentication server due to an attack how many other systems would be taken down? If your database server was overloaded, how many applications would be at risk? Today's sophisticated attacks are more subtle and targeted at application-level services and are purposely designed to have cascading impacts across many systems in your data center.

Future Data Center Plans/Roadmap: What elements are you planning on changing? How will these affect the complexity of your data center and do they present any new risks? Adding new hardware or services comes with many known and unknown challenges. The more you identify up-front the better you'll be prepared as things change.

Once you have scoped out your infrastructure and prioritized your critical systems, you're ready to develop a tactical plan to test these elements and how they would react to different types of DDoS attacks.

Define anticipated legitimate workloads: Effective DDoS defense planning starts with baselining the infrastructure response to anticipated legitimate workloads. Special care

Myths and Realities About DDoS Attacks

Many IT professionals think they're safe from DDoS attacks either with protections in their current firewall, switches and other network devices, or mistakenly think their ISP is able to provide 100% mitigation. The following are a few common misconceptions and truths about DDoS attacks.

My ISP takes care of DDoS attacks for me. Many ISPs and hosting companies are happy to null-route an attacked IP domain to solve the problem of DDoS attacks. This works for many bulk layer 3 and 4 events, however smaller layer 7 attacks easily bypass their protections and they pass along these application-level threats to your network. Most successful attacks are under 1 Gbps, with 80% of all DDoS attacks under 50 Gbps. An ISP can assist in arresting a high-volume packet flood to your network, however data centers need additional layer 7 protections. Some also mistakenly believe their ISP will help them get to the root of the attack. Most ISPs are too busy and they have strict and bureaucratic processes for reaching one another. Typical response times from ISPs are in days and weeks to help determine the sources of DDoS attacks.

It only happens to the other guy. Most network and security operations engineers usually only hear about DDoS attacks happening to other organizations. They think that they don't have enemies or have any other reason to be the target of an attack. In reality, their perceptions of risk factors and susceptibility are often misplaced in that simply having a web presence makes them a target, even if by mistake.

Server DDoS protections have me covered. Many engineers think that they can custom-compile kernel code, set some options in Apache, install "mod_dosevasive" and use "iptables" and their DDoS attacks problems are solved. In reality, most servers do not have the capacity to handle DDoS attacks. Under most average-sized DDoS attacks, the server CPUs will be too overloaded to give the Apache modules or Linux commands a chance to mitigate the event.

It's against the law. Call the police! Yes, DDoS attacks are illegal but most law enforcement agencies will only pursue large attacks (10 Gbps and up) on large companies or institutions like banks, government agencies and major international corporations. Most likely they'll politely tell you that you're going to need to work with your ISP or a private investigator.

My routers and switches protect me from DDoS attacks. Even though your networking hardware may have access control lists (ACLs) that can block DDoS threats, the attackers can adapt quickly. The average hacker can easily get around your ACLs within minutes with a little determination.

A dedicated DDoS appliance will just get flooded too. Many wonder if there is any point in buying specialized DDoS appliances. Without DDoS mitigation equipment, your servers will be thoroughly exposed even to ordinary attacks. Newer devices on the market provide capacities of over 20 Gbps of throughput that can be overprovisioned to protect you from larger attacks. Combined with ISP DDoS protections you get a solution for bulk and sophisticated layer 7 attacks.

FortiDDoS Attack Mitigation Appliances

Fortinet is the only company to use a 100% custom ASIC approach to its DDoS products, which eliminates the overhead and risks associated with CPU or CPU/ASIC hybrid systems. The second-generation FortiASIC-TP2 traffic processor provides detection and mitigation of all layer 3, 4 and 7 DDoS attacks for both inbound and outbound traffic.

FortiDDoS uses a 100% adaptive behavior-based method to identify threats. It learns baselines of normal application activity and then monitors traffic against them. Should an attack begin, FortiDDoS would see this as an anomaly and then immediately take action in real time to mitigate it. 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.

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 does it faster than any other solution available on the market today.

DDoS Congestion Protection: With models up to 24 Gbps of full duplex throughput you get the capacity you need to defend against larger-scale DDoS attacks. Line Rating provides maximum throughput at full line speeds.

Easy-to-use and Easy-to-manage: Adding DDoS mitigation to your network takes only minutes with FortiDDoS' automated setup tools and pre-configured default options. It's intuitive GUI, full CLI and advanced reporting give you tools to easily manage your DDoS defenses and get detailed attack reports and analytics.

Lowest TCO: FortiDDoS appliances average less than 50% the TCO of similar devices from other manufacturers.

Lowest Latency: It's single-layer, hardware-based DDoS detection and mitigation engine delivers a latency rate of less than 50 microseconds.

Best False Detection Avoidance: The FortiDDoS short sub-minute blocking period and continuous attack reevaluation methods identify and mitigate only threatening traffic.

should be given to modeling the complex interaction of user and infrastructure services at a scale and randomness found in real-world target networks. The changes to this workload under DDoS attacks and the exposure you are willing to accept are critical in understanding whether proposed defense solutions and strategies make sense for your organization.

Bulk Volumetric Testing: This type of testing is going to determine how your infrastructure will stand up to large scale DDoS attacks such as a SYN, UDP, or SIP floods. These tests should be done across all critical web-facing infrastructure elements and use the highest volume of packet flooding your test systems can generate.

FortiDDoS Put to the Test

In a recent test conducted using the Ixia BreakingPoint platform, the FortiDDoS was put through a series of simulated basic and advanced DDoS attacks including layer 7 service-based DDoS attacks like GET/POST and SMTP Flooding.

FortiDDoS Attack Detection

Attack Type	Mitigated
SYN Flood	Yes
SYN ACK Flood	Yes
DNS Flood	Yes
SMTP Flood	Yes
SIP Flood	Yes
Loic	Yes
Slowpost	Yes
Slowloris	Yes
Sockstress	Yes
Botnet TDL4	Yes
Botnet Evil	Yes
Botnet Rudy	Yes

- FortiDDoS detected almost all attack types from basic SYN Floods to sophisticated layer 7 attacks like HTTP Post and Slowloris.
- FortiDDoS detected attacks in an average of 5 seconds from the start of the test.
- The FortiDDoS adaptive behavior-based model continued to let "good" traffic through as it continually reevaluated the attack numerous times.

Layer 7 Testing: In these tests, you're going to want to check the resiliency of services on all your network's critical infrastructure elements, even if they're not directly exposed to the Internet. Most layer 7 attacks can easily subvert many ISP and hosted DDoS mitigation solutions and are passed along to your data center. Tests in this area include HTTP GET, HTTP POST and Slowloris that can tie up server resources with only a fraction of the packets required in a bulk volumetric attack.

Botnet Testing: There are many tests that can generate both bulk volumetric and layer 7 attacks, but they generally tend to spoof IP addresses and are somewhat easy to detect with pattern matching tools. Botnet testing mimics the random packet generation methods used by real botnets making it more difficult to detect.

With all of these tests you'll want to evaluate how your infrastructure responds to these attacks and the impact on legitimate user workloads. If you have a DDoS mitigation solution in place, you'll additionally want to test how it responds in terms of accuracy, speed, and effectiveness in detecting and mitigating these threats.

Testing Options

There are two primary methods to test your data center for DDoS readiness using either software or hardware-based testing platforms.

Software-based Tools: There are many software-based options that are widely available for testing your DDoS defenses including many Open Source ones. Most of these are modifications of tools used by hackers and mimic

> "To deliver the greatest value to enterprises, sophisticated DDoS defenses must be subject to proactive testing against timely, realistic attack scenarios. Fortinet's strategic approach to optimizing the performance of its FortiDDoS solution over time helps keep customers protected and better able to anticipate and respond to changes in the dynamic DDoS threat landscape."
>
> *Fred Kost*
> *VP Security Solutions, Ixia*

their basic attack techniques. For small scale testing, or to conduct bulk volumetric attacks, they offer the basics. You will need a combination of advanced tools to obtain a comprehensive set of results for layer 7 threats. These tools can simulate large spoofed floods, but are limited in producing botnet-style ones.

Hardware Platforms: For serious data center testing, a hardware-based testing platform is used to generate DDoS traffic in the multi-gigabit volumes typically used by hackers. These are dedicated appliances that test all the major attack types and generate packets that are virtually identical to those used by botnets. These can either be purchased by an organization for regular DDoS threat evaluations or offered as a service by a testing provider to conduct tests as needed or on a regular basis.

Software based solutions can be much less expensive and are usually a good fit for smaller organizations. Large-scale data centers usually opt for regular DDoS audits by a testing provider, and the largest data centers for ISPs and telecommunications firms will buy their own dedicated testing hardware.

Once you get your results, you'll know how well you're protected and what you'll need to do to fix the problems in your network. If you have a DDoS mitigation solution, you'll be able to verify the claims of the vendor and make sure their solution is performing as advertised.

Conclusion

DDoS attacks are on the rise for almost any organization, large or small. The potential threats and volumes are increasing as more devices including mobile handsets join the Internet. If you have a web property, the likelihood of getting attacked has never been higher.

The evolving nature of DDoS attack technologies requires organizations to make shifts that need greater foresight and more proactive defenses for network and application-level services. ISP DDoS protections aren't enough against the latest attacks requiring an additional level of DDoS security in your data center to defend against layer 7 threats. There are many different types of DDoS defense solutions on the market today. You should choose one that can defend against basic attack types and advanced layer 7 DDoS threats.

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. Some models, such as FortiDDoS, offer advanced features like line rating for congestion prevention, and 100% behavior-based detection that eliminates the need for signature updates.

Whether you have a DDoS mitigation solution or not, you need to understand what DDoS attacks can do to your data center. The only way to validate your defenses is to conduct comprehensive and regular DDoS testing. For most enterprise and ISP data center managers, this requires a complete hardware-based testing solution.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480