Protecting against **DoS/DDoS** Attacks with FortiWeb© Web Application Firewall

A FORTINET WHITE PAPER
Introduction

Denial of Service attacks are rapidly becoming a popular attack vector used by hackers and hacktivists. With the proliferation of botnets, there has been a massive increase of Distributed Denial of Service (DDoS) attacks and more and more organizations, not only large enterprises and service providers, are seeking a solution.

One of the major DDoS attacks in 2011 targeted a gaming network and was carried out by the “Anonymous” hacktivist group. The attack camouflaged a data breach resulting in the theft of over 77 million customer records from an online gaming portal. Several major credit card companies were also hit in 2011 with attacks that took down their web sites for several hours in retaliation to their decision to cut off services to WikiLeaks. Other high profile attacks hit a US government agency, a blog hosting site, a UK anti-crime site, and an Asian stock exchange.

Contributing to the popularity of DDoS attacks is the fact that many people support their use for various social and political reasons. Organizations are sometimes targeted because they are associated with a business, country, or policy that these activist organizations find unacceptable. While the attackers do not necessarily gain financial profit from the attacks, the organizations suffer lost revenue, damage to corporate brand and credibility.

Ready access botnets are available for hire for as little as 10$ in the digital black market. Using forums and dedicated web sites criminals advertise botnets availability and allow attackers to easily utilize a bot network and execute attacks.

The importance of protecting against DDoS attacks is crucial with the critical role web-based applications play in companies’ revenue models. Availability of these applications becomes an absolute criticality to maintain business viability.

FortiWeb Protection Against DoS/DDoS Attacks

- Multiple DoS/DDoS-specific protection policies
- Network and Application layer protection
- Protects both HTTP and HTTPS protocols
- Sophisticated botnet challenge / response protection
- Geo IP Analysis
A DoS attack is the result of an attacker sending an abnormally large amount of network traffic to a target system. During a DoS attack, a server can be flooded with far more traffic than it can handle. This traffic flood slows down the server, effectively blocking legitimate users. The most common example of a DoS attack is a DDoS attack, in which an attacker directs a large number of computers to attempt apparently normal access of the target system using standard access methods. If enough access attempts are made, the server is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but the target server is not accessible to anyone else.
Application DoS/DDoS Attack

An application-layer DoS attack is an attack targeting the application service itself. While it was only a few years ago that a DoS attack primarily targeted networks using low level protocol attacks such as PING, Smurf and different worms, today’s attacks are targeting specific web applications in more sophisticated manners. Attackers use legitimate requests to overload the server. More sophisticated DoS attacks come after site reconnaissance to understand which request creates the most CPU-intensive SQL query to the backend database. Other attacks can try to manipulate server memory, writing to hard disks and server-specific attacks.

Anatomy of DDoS Attacks Using Botnets

A bot is a computer running malware software that allows a remote attacker to control it in different malicious ways. Attackers use bots to send spam, distribute malware to other users, act as a proxy to conceal real user identity and participate in mass distributed denial of service attacks. Many times the bots reside on compromised systems, with innocent users unaware their computer has been compromised by Trojans after they accessed an infected web site or ran malware programs on their computer inadvertently.

In DDoS attacks the compromised computers controlled remotely by the attacker are installed with a program that can generate high rate of traffic. In most cases these programs can create different types of malicious or legitimate traffic that, when clustered together with hundreds and thousands of other computers, create a massive attack that overwhelms the target server.

FortiWeb Protection Against DoS/DDoS Attacks

Using a variety of protection techniques, FortiWeb can help protect organizations from DoS and DDoS attacks. FortiWeb uses both network and application layer protection mechanisms to identify requests from legitimate users and block access to attacks originating from clients associated with botnets.

After identifying an attack FortiWeb adds the malicious client IP to its blocked IPs list and automatically denies access from the IP for a configurable period of time. FortiWeb does not need to inspect additional requests from this source therefore preserving resources.
The Next Challenge: Application Layer DDoS

With the understanding that DDoS attacks are utilizing botnets running dedicated malware software to create huge amounts of legitimate connections and requests from each compromised computer, the only solution to identify whether these requests are from valid users or infected machines is to create a challenge response system.

FortiWeb uses a configurable threshold mechanism to challenge clients for a response. If the client responds correctly to the challenge, FortiWeb allows access to the server for this client. If it does not FortiWeb understands that this is a hijacked user using an automated traffic-generating tool and blocks its IP immediately. For legitimate users this challenge response process is completely transparent and will not affect their browsing experience.

Advanced Protection with FortiWeb Web Application Firewall

While DDoS attacks are more commonly targeting web servers and network availability, many times they are camouflaging application server breach attempts (such as those performed on the global gaming network described above). Protecting against these types of breaches requires additional protection mechanisms in addition to the DDoS protection capabilities.

Combining both Web Application Firewall and sophisticated DDoS protection capabilities in a single platform, the FortiWeb solution allows enterprises to protect against application level attacks targeting the Web application and web services infrastructure. Using advanced techniques to protect against SQL injection, Cross site scripting, and a range of other attacks, FortiWeb helps to prevent identity theft, financial fraud and corporate espionage which can result in significant damage.

FortiWeb provides flexible and reliable protection to address a wide range of attacks (such as defined by the OWASP Top Ten), by utilizing a range of in-depth security modules and technologies. Sophisticated attacks are blocked using a multi-layered security approach. Incorporating a positive and a negative security module based on bi-directional traffic analysis and an embedded behavioral based anomaly detection engine means FortiWeb can protect against a broad range of threats, all without the need for network re-architecture and application changes.
Guarantees security of web applications and secures sensitive database content by blocking threats such as cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of service, cookie poisoning, schema poisoning, and countless other attacks.

Aides in PCI DSS 6.6 compliance by protecting against OWASP Top 10 web application vulnerabilities.

Automatically and dynamically profiles user activity to create a baseline of allowed activity.

Application and network based Denial of Server (DoS) policies.

SSL encryption co-processing accelerates transaction times, offloads encryption functions, reduces web server processing requirements.

Server load balancing and content-based routing increases application speeds, improves server resource utilization and stabilizes applications.

Data Compression allows efficient bandwidth utilization and response time improvements.

Real time data analysis provides an analytics interface that helps organizations analyze their web application usage from multiple vectors and maps requests to their geographic location.

### Conclusion: FortiWeb Web Application Firewall

Attacks on web applications are on the rise, ever changing and advancing in sophistication. Botnets are being used to send spam, distribute malware and above all – participate in DDoS attacks which inflict huge damage on companies.

FortiWeb web application firewall provides enterprises with the protection techniques that are required to stop these attacks. FortiWeb uses multiple protection layers incorporating both a negative and security model and incorporates sophisticated DDoS protection techniques that help identifying real users from malicious botnet activity.

FortiWeb DDoS protection is an add on module to its existing web application firewall. Fortinet also provides a standalone dedicated DDoS solution and DDoS capabilities in its FortiGate offering.

See [www.fortinet.com](http://www.fortinet.com) for more information.