Spirent **CyberFlood**

DDoS | Applications and Security Test Solutions

Overview

Today's DDoS attacks are more dangerous and more virulent than those seen in the past. Recent attacks have breached the 600Gbps barrier with 1 terabit DDoS attacks expected to be the new normal.

Attacks are also more prevalent than ever before, with a reported 1/3 of all downtime incidents being attributed to DDoS attacks. On any given day, worldwide, more than 2,000 attacks can be observed.

Not only has the cost to pay for an attack hit bargain-basement pricing (sold for as little as $150 on the Dark Web or underground black market for a week-long barrage), incidents are surging with cloud, IoT, and mobile computing adoption rates increasing the security perimeter.

Survive DDoS attacks by proactively and continually hardening the networked products and services against attacks by planning for the unexpected, and ensuring your testing is unique to your environment.

According to IDC's 2017 study, *Worldwide DDoS Prevention Products and Services Forecast*[1] DDoS threats cannot be ignored. Organizations are implored to take action sooner, rather than later, with steps to protect their infrastructure. Their forecast includes the following assessments:

- Advanced attacks will include diversionary, application layer, and multi-vector/multi-layer, helping drive growth in the market throughout the forecast period as more businesses see the value in robust defense.
- Hybrid defense scenarios (single solutions that pair on-premises equipment with cloud services) will continue to grow and augment defense-in-depth scenarios (similar solution components from multiple vendors that are not integrated) as organizations seek to defend themselves against all vectors of DDoS attacks.

Distributed Denial-of-Service (DDoS) Protection

Validating your DDoS mitigation strategy is more than just flooding your security infrastructure with a ton of traffic to see what happens. CyberFlood, leveraging its unique and industry-leading architecture, combines both legitimate/normal traffic with DDoS attack traffic, emulating what happens in the real world. When validating DDoS protection, you need to confirm your DDoS solution can not only mitigate the DDoS attack, but also not inadvertently impact your legitimate users.

Statistics are provided within CyberFlood, in real-time, allowing you to interactively measure both user experience and security mitigation. With this capability, you now have full visibility into how your security infrastructure is performing. Need more scale or only DDoS traffic? CyberFlood offers attack-only and extreme scale test types allowing you to emulate large-scale DDoS attacks targeting large industry verticals and service providers.

DDoS Categories—Volumetric & Protocol

CyberFlood helps you validate *today*. Deploy your DDoS mitigation strategy at scale with multi-10G line-rate attacks, generating tens of million of packets-per-second. Confirm legitimate user traffic is not inadvertently impacted by your DDoS protection, all of which is measured accurately by CyberFlood within one single test methodology. Maximize network uptime, minimize costly service disruptions and customer churn using our solutions, which include:

- Scalable DDoS capability
- Vast attack coverage
- Simple to set up and execute tests
- Huge scale and performance to push any device to its limits

1. IDC, Worldwide DDoS Prevention Products and Services Forecast, 2017-2020, DOC#US41659116, Aug 2017

Spirent Services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements.

For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

Attack Samples

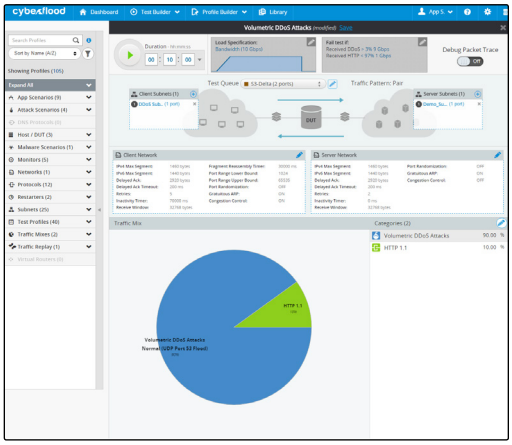
- Internet Control Message Protocol (ICMP)
- User Datagram Protocol (UDP)
- Spoofed IP
- Malformed IP
- Malformed UDP
- Malformed ICMP floods
- Ping of death
- Synflood (millions-per-second)
- Smurf attack

Volumetric: As the most common type of DDoS attack, volumetric assaults are relatively easy to deploy via botnets which can overwhelm a website and/or infrastructure with minimal experience on the attack-side.

Protocol: Many protocols such as DNS were designed long before DDoS attacks emerged, when networking was fairly straightforward with terrestrial, rudimentary hardware in place. Since then, popular network protocols like DNS have been shown to be vulnerable to DDoS abuse. As a consequence, developers and administrators are challenged to manage real-world exposure and vulnerabilities that can be punishing if gone untested.

DDoS Test Types

One-armed DDoS (Client only)
Targeting Real Services: Create advanced tests with a mixture of DDoS and legitimate traffic to test the efficacy of mitigation policies and its impact on non-attack user traffic. Percentages of attack vs. normal traffic can quickly be adjusted to find the exact point where security services impact application performance and access.



Simple to set up and execute tests with mixed traffic

AssaultMode™ DDoS for Multi-10G
Attack Traffic: Find the upper limits of any security device by targeting it with an onslaught of attack traffic. Create tens-of-millions of attacks per-second, and spoof hundreds of thousands of hosts.

Ordering Information

Description	Part Number
Cyberflood Base License for C100	CF-SW-BASE
Cyberflood Volumetric DDoS Suite	CF-SW-DDOS
Cyberflood Protocol DDoS	CF-SW-PDDOS
Cyberflood Cybersiege Global IP Traffic Selector-1YR	CF-SW-IANA-1YR

Other CyberFlood options are available for specific hardware platforms and Advanced Fuzzing options, please contact Spirent sales for more information.

Contact Us
For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev F | 09/18