Spirent C200 Appliance

For CyberFlood and Avalanche

In today's digital world, it's essential that the performance of content aware networks, security systems and web applications are carefully assessed to ensure that business transactions and communication are not impacted. The C200 is a powerful Layer 4-7 stateful traffic performance solution in a 1U form factor that is capable of very high throughput security assessment with high-strength cryptographic and hyper-realistic application traffic. By taking up less valuable rack space users can scale to test beds supporting multiple terabits of application layer traffic generation.

Built-in CyberFlood

The C200 comes with a built-in CyberFlood controller. Within minutes from unpacking users can be up and running tests with the powerful, web-based CyberFlood solution without the need for additional hosting platforms.

Performance and Flexibility

The C200's 4 x QSFP28 interfaces provide quite speed connectivity for 10G, 25G, 40G, 50G, and 100G Layer 4-7 application and attack traffic, users are able to specify load variables and easily create tests with mixed traffic profiles emulating real-world network scenarios. With built-in advanced cryptographic acceleration technologies the C200 can meet today's and the future's most demanding test needs for encrypted traffic with high strength ciphers at massive scale.

Application and Security Testing Solutions

The C200 for CyberFlood and Avalanche appliance provides the industry's highest performance and capacity with multi-speed support for 10G, 25G, 40G, 50G, and 100G in a slim-line 1U form factor. Users can assess the limits of security and performance for network infrastructures, Web applications and media services ensuring Quality of Service (QoS) and Quality of Experience (QoE) for your customers. The C200 is compatible with both CyberFlood and Avalanche assessment solutions giving you the most versatility for application layer testing.

Applications

- Network performance testing
- Web application testing
- High-performance HTTPS/TLS testing
- Security testing/validation
- Attack and Malware assessment
- Advanced DDoS
- VPN/IPsec performance
- Application Identification testing with over 15,000 application scenarios
- Advanced video application testing
- Mobile network firewall testing
- Replay UDP/TCP traffic at scale

Advanced Security and Performance Testing with CyberFlood

CyberFlood is a powerful, easy-to-use web based assessment solution that generates thousands of different realistic application traffic scenarios, attacks, and malware to test the performance, scalability and security of today's application aware network infrastructures. Unlike other test solutions, CyberFlood generates real high performance user applications based on actual application scenarios, real attacks and malware for realistic security, load and functional testing.

NetSecOPEN Testing Standards-based Methodologies

NetSecOPEN is a network security industry group where network security vendors, tool vendors, labs and enterprises collaborate to create open and transparent testing standards. The goal of this group is to create a suite of standards that can be used for the evaluation and/or certification of network security products. The NetSecOPEN standard methodologies are built into CyberFlood providing easy-to-use pre-made methodologies for testing modern network security infrastructures, including goal seeking tests that will automatically find the maximum performance of devices under test. For more information on NetSecOPEN, go to www.netsecopen.org.

NetSec ✓OPEN

User Realism with Avalanche

Avalanche software on the C200 supports the configuration of extremely realistic user behaviors so tests accurately reflect your company's network usage patterns. The system interacts seamlessly with sites using dynamic and interactive content, HTML links and online fill-in forms. Multiple types of browsers can be emulated, providing detailed control over browser connection behavior, SSL versions, authentication and browser client headers.

User behavior such as think times and "clickaways" (HTTP aborts) can be simulated, and the system also supports HTTP basic and proxy authentication. In addition, next-generation integrated video testing is available for protocols such as HTTP Adaptive Bitrate streaming for Apple®, Microsoft®, and Adobe®.

Features & Benefits

- **>100Gbps Line Rate Stateful Traffic—**Provides the capability to generate over 100Gbps of line rate stateful Layer 4-7 traffic. Each C200 supports high density 16 x 10G interfaces and up to 4 x 40G or 4 x 100G interfaces

- **Flexible Software Options—**The C200 is compatible with CyberFlood providing a web-based, easy-to-use yet powerful application and security/attack testing and with Avalanche for advanced directed one-ended and two-ended testing

- **Throughput with Mixed Traffic—**Create and execute tests with preconfigured traffic mixes to achieve high throughput HTTPS/TLS encryption, or easily create your own mixes from a database of thousands of application scenarios and blend in attack traffic to verify security policies under load

- **Network Security Testing—**Provides extensive testing for secure network communication, vulnerability assessment with an always up-to-date attack and malware database

- **Network Devices Performance Testing—**Provides performance and capacity testing on a variety of network devices including: Firewall, Application Firewall, Load Balancer, SD-WAN, Cache, Proxy, URL Filter, Content Filter, Anti-Virus, Anti-Spyware, Reverse-Proxy, SSL Accelerator, HTTP/HTTPS Accelerator, WAN Accelerators, SMTP Relay, IDS/IPS, and IPsec VPN Gateway

- **Application Server Performance Testing—**Validates the performance of several types of real servers including: Web Server, CIFS Server, Application Server, Mail Server, DHCP Services, FTP Server, DNS Server, RTSP/ RTP QuickTime Streaming Server, Multicast Server, RTMP Servers, and more

- **Performance Operation Modes—**Easily change the C200 mode of operation to adjust CPU and memory allocation behind test interfaces providing maximum flexibility for a variety of performance options

- **Reliability Testing—**Perform long duration soak tests with the TestCloud application load to ensure solutions work at high capacity for long periods of time.

- **IPSec Testing—**Validate IPSec VPN capacities including tunnel setup, maximum tunnels, and data rates over encrypted tunnel for remote access and site to site use cases

Spirent C200 Appliance	
Feature	
Number of test users	Up to 16 users on specific configurations
Network interfaces	4 x QSFP28 supports a number of interface options Up to 16 x 10G Fiber (SR4) Up to 8 x 25G Fiber (SR4)* Up to 4 x 40G Fiber (SR4) Up to 4 x 50G Fiber (SR4)* Up to 4 x 100G Fiber (SR4 or LR4) (Transceivers sold separately)
CPU	32 high-powered cores for advanced traffic and attack generation
Cryptographic Processing	256 Symmetric and 320 Asymmetric Cores
CyberFlood Feature Details	
Web Based Interface	Easy to use multi-user web-based interface makes setting up and executing comprehensive tests fast, easy and consistent
Application Scenarios	Over 15,000 current and popular application and user scenarios
Attack and Exploits	Over 4,000 attacks and exploits covering areas such as SQL injection, cross site scripting, targeted OS, in-line device, end point services. Users can send attack over TLS sessions and apply evasions techniques to further stress security solutions detection capabilities
Malware	Over 50,000 continually updated recent and zero-day malware samples including command and control behavior and binary malware transfer scenario
DDoS	Test DUTs using different DDoS attacks to confirm its ability to detect and block them successfully with a suite of volumetric and protocol DDoS attacks that can be configured for stand- alone attack tests or mixed with normal user traffic to verify impact on performance
HTTPS/TLS Testing	Support for SSLv3, TLS v1.0, TLS v1.2, and TLS v1.3 with selectable certificate and cipher suites
CyberSecurity Assessment	Quickly create tests that verify the effectiveness of IDS, IPS NGFW and other security solutions with and without user load of traffic
HTTP/HTTPS Rate	Open millions of new connections per second to ensure connection rate and capacities of your network
Advanced Mixed Traffic Assessment	Create custom and highly configurable tests and assessments with user action lists that allow test assessments to be created which will walk through a set of user application interactions for HTTP, HTTPS, SMTP, POP3, IMAP, and FTP protocols (additional protocol support coming soon).
HTTP/HTTPS Bandwidth	Find the maximum throughput achievable using emulated, realistic HTTP clients and HTTP servers and leveraging a configurable network topology
HTTP/HTTPS Connections	Open millions of concurrent TCP connections within the state table of your DUT to find the maximum concurrency it can support. Leverage HTTP as the protocol for added realism during this test
Mixed Traffic Tests	Measure the impact on application performance when using real-world built-in applications or extended with the power of TestCloud. Individually measure the bandwidth and success rate of each application added to the test to confirm the impact of the network under test. Add attacks and security to traffic mixes to stress security devices under load
Traffic Replay	Replay your own custom traffic profiles at scale to determine the impact of specific traffic flows on network devices and services
VPN Testing	Easily assess capacities and capabilities of site to site and remote access IPSec from tunnel setup to data traffic handling
DNS Tests	Stress your DUT by sending hundreds of thousands of DNS queries per second for it to process and traverse through it as well as for it to process the corresponding events that occur on the DNS responses
Automation	CyberFlood RESTful API and Avalanche TCL
Dimensions	Height 1U, width 17.5" inches (without rack mounts), depth 37.1" inches
Weight	46 lbs. (11kg)
Operating environment	Supported 0° to 35°C ambient temperature
Non-operating environment	-20C to 70C
Relative humidity	10% to 70% (non-condensing)
Power requirements	Dual outlet 100-240V, 50/60 Hz-1600W 15A
Regulatory approvals	FCC Class A, EN 55022 Class A, EN 55024, EN 61000-3-3:2013, 61000-3-2:2014 or equivalent Product Safety requirement

* 25G/50G for use with Avalanche software only.

About Spirent

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information visit: www.spirent.com

Ordering Information

Description	Part Number
C200 with 4 x QSFP28* Interfaces CyberFlood Capacity License (add on unit)	CF-KIT-001-C200
C200 with 4 x QSFP28* Interfaces with CyberFlood Performance Licenses	CF-KIT-002-C200
C200 with 4 x QSFP28* Interfaces with CyberFlood Security and Performance	CF-KIT-003-C200

C200 appliances come with built-in CyberFlood controller and base software for HTTP bandwidth and connections tests.

Other CyberFlood and Avalanche software options are available, please contact Spirent Sales for more information.

* QSFP28 transceivers are sold separately.
* 25G/50G for use with Avalanche software only.

Spirent Services

Professional Services

- Test lab optimization: Test automation engineering services
- Service deployment and service-level optimization: Vendor acceptance testing, SLA benchmarking, infrastructure and security validation
- Device scalability optimization: POC high scalability validation testing

Education Services

- Web-based training: 24x7 hardware and software training
- Instructor-led training: Hands-on methodology and product training
- Certifications: SCPA and SCPE certifications

Implementation Services

- Optimized new customer productivity with up to three days of on-site assistance

Ospirent™