CF1000 CyberFlood Appliance

Terabit-Scale Application Performance Testing Solution

In today's rapidly evolving digital landscape, driven by cloud computing, hyperscale AI datacenters, IoT, and massively distributed application workloads, it is essential that the performance of content aware networks, security systems, and application delivery infrastructures are rigorously validated. Distributed applications, cloud connectivity, and large-scale AI inference fabrics are pushing the traffic volumes and connection rates far beyond traditional thresholds, placing unprecedented strain on network and security architectures of modern data centers. Business critical transactions and real-time communication must perform as expected and scale to meet accelerating bandwidth demands, rapid east west traffic growth, and increasingly complex encrypted flows.

The **CF1000** is a terabit-scale Layer 4–7 stateful traffic and application test platform engineered for this new era of ultra-high speed, AI driven networks. Designed to support realistic, high strength cryptographic workloads including post-quantum and hyper realistic application traffic at extreme scale. The CF1000 delivers over **1.2 Tbps** of application throughput while providing market leading price/performance value. This enables network security vendors, cloud and application delivery infrastructure providers, and hyperscale AI data center operators to accelerate development cycles, right size infrastructure investments, and ensure the highest levels of end user performance, resiliency, and Quality of Experience (QoE).

Ultra-High Application Performance Testing Solution

The CF1000 testing platform delivers the industry's highest performance, highest capacity Layer 4–7 application and security testing solution, supporting **400G QSFP** and **100G QSFP28** interface options.

The CF1000 enables users to validate the performance limits of network and security devices, web applications, media services, AI inference workloads, and more, ensuring consistent Quality of Service (QoS) and Quality of Experience (QoE) across modern, high demand environments.

Paired with CyberFlood and Avalanche, the CF1000 can generate over **1.2 Tbps of application traffic** and over **500 Gbps of encrypted traffic** within a single appliance. Multiple CF1000 units can be combined into a unified testbed to achieve multi-terabit scale for advanced validation of next generation network infrastructures.

Applications

- Network performance testing
- Web application testing
- AI Inference Assessment
- High-performance HTTPS/TLS testing
- SSL VPN/IPSec performance testing
- Application identification testing with hundreds of thousands of application scenarios
- Advanced video application testing
- Mobile network firewall testing
- Zero-Trust Scale and Performance Testing
- Replay UDP/TCP traffic at scale
- Optional advanced security testing solutions are also available

Performance and Flexibility

The CF1000 is available with 4 x 400G OSFP and8 x 100G QSFP28 interface configurations in a single 2U appliance. Users can specify load variables and easily create tests with mixed traffic profiles, emulating real-world network scenarios.

With advanced cryptographic capabilities, the CF1000 delivers the industry's highest TLS performance capability, with over 500 Gbps of encrypted throughput and 820K connections per second from a single appliance. It enables users to validate today's and the future's most demanding test needs for encrypted traffic with high-strength ciphers at massive scale.

CF1000 Performance Examples[1]	
HTTP Uni-directional Throughput	950 Gbps
HTTP Bidirectional Throughput	>1.2 Tbps
HTTP Connections per Second	>6 Million
TLS v1.2 Throughput	>500 Gbps
TLS v1.2 Connections per Second	820 K

[1]Performance numbers are obtained using a single CF1000 as a client and server. TLS v1.2 Performance done with the AES-128-GCM-SHA256 cipher suite.

Modular Terabit Scale

The CF1000 includes an integrated CyberFlood controller, enabling users to begin testing within minutes using the powerful, web-based CyberFlood interface, without the need for any external hosting platforms. Its modular appliance architecture offers exceptional scalability, allowing multiple CF1000 units to be stacked into a single, cohesive test system. This provides the flexibility to validate the performance boundaries of multi-terabit security controls, application delivery platforms, and hyperscale AI datacenter networks with ease and efficiency.

Advanced Performance Testing with CyberFlood

CyberFlood is a powerful, easy-to-use web-based testing tool that generates thousands of realistic application traffic scenarios to test the performance and scalability of today's application-aware network infrastructures. Unlike other testing tools, CyberFlood generates real high-performance user applications, based on actual application scenarios, and provides load and functional testing capabilities.

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 netsecopen.org.

User Realism

The CF1000 enables the creation of highly realistic user behavior models, ensuring tests accurately reflect your organization's real world network usage patterns. The system interacts seamlessly with websites that use dynamic and interactive content, including HTML links, scripts, and online forms. Multiple browser types can be emulated, offering granular control over connection behavior, SSL/TLS versions, authentication methods, and browser client headers. User dynamics,such as think times, navigation delays, and "clickaways" (HTTP aborts)—can also be simulated to provide even greater realism. In addition, the CF1000 supports HTTP basic and proxy authentication, along with next generation integrated video testing for protocols such as HTTP Adaptive Bitrate (ABR) streaming across Apple®, Microsoft®, and Adobe® environments.

Features and Benefits

- **>1.2 Tbps Stateful Application Traffic:** Provides the capability to generate over 1.2 Tbps of bidirectional stateful Layer 4-7 traffic. Each CF1000 supports high-density 4 x 400G OSFP and 8x100G QSFP28 interfaces.
- **Flexible Software Options:** Allows for compatibility with CyberFlood, providing a web-based, easy-to-use, yet powerful testing tool, and with Avalanche for advanced, directed one-ended and two-ended testing.
- **Automatic Goal Seeking:** Determines the maximum capabilities of a device with minimal user interaction.
- **Throughput with Mixed Traffic:** Allows users to create and execute tests with preconfigured traffic mixes to achieve high throughput HTTPS/TLS encryption, or easily create custom mixes from a database of hundreds of thousands of application scenarios. Supports test creation using next-generation web protocols, including the industry's first support for HTTP/3.
- **Network Devices Performance Testing:** Provides performance and capacity testing on a variety of network devices including Firewall, Application Firewall, Load Balancer, SD-WAN, SASE, 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 services including Web, SMB, Application Services, Email, DHCP, FTP, DNS, RTSP/RTP QuickTime Streaming, Multicast, RTMP, HTTP ABR, and more.
- **Performance Operation Modes:** Makes it easy to change the CF1000 mode of operation to adjust CPU and memory allocation behind test interfaces, providing maximum flexibility for a variety of performance and use case options.
- **Reliability Testing:** Supports long duration soak tests with the TestCloud application load to ensure solutions work at high capacity for long periods of time.
- **AI Inference Testing:** Realistic emulation of user interactions, multi-turn conversations, and multi-modal prompts at scale to assess performance, scalability, and security on AI inference infrastructure and AI/LLM applications under production-like conditions.
- **VPN Testing:** Validates IPSec and SSL VPN capacities including tunnel setup, maximum tunnels, and data rates over encrypted tunnels for remote access and site-to-site use cases.
- **ZTNA Testing:** Test the Zero Trust Policy Enforcement Point (PEP), validate that secure network and application access are delivered and verify that connections and per-user access policies are functioning as intended without impacting performance or QoE.
- **Realistic Web Testing:** Uses web-capture capabilities to import and replay recorded sessions of complex website interactions and traffic to validate performance and comprehensive application policies.

Technical Specifications

Product Feature	Description
Available Hardware Configurations	
CF1000 with 4 x 100G OSFP and 8x 100G QSFP28	4 x 400G interfaces
	8 x 100G interfaces
Software License Options	
Performance Testing Software	Includes HTTP/HTTPS Throughput, HTTP/HTTPS CPS, HTTP/HTTPS Concurrent Connections, DNS, Throughput with Mixed Traffic (default protocols), Advanced Mixed Traffic, and Network Traffic Replay test methodologies.
TestCloud Subscription	Allows options for always up-to-date downloadable content for application scenarios.
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	Hundreds of thousands of current and popular applications and user scenarios that can be easily used in custom mixed traffic tests.
HTTPS/TLS Testing	Support for TLS v1.2, and TLS v1.3 with selectable certificate and cipher suites, including Post-Quantum Cryptography (PQC).
HTTP Connections Tests	Open thousands to millions of new connections per second to ensure your DUT can handle the new connection rate of your network.
HTTP Bandwidth Tests	Find the maximum throughput achievable using emulated, realistic HTTP clients and HTTP servers and leveraging a configurable network topology.
HTTP Open Connection Tests	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.
VPN Testing	Easily assess capacities and capabilities of site to site and remote access IPSec and SSL VPN from tunnel setup to data traffic handling.
Advanced Mixed Traffic Assessment	Create custom and highly configurable tests and assessments with user action lists that execute a set of user application interactions for HTTP, HTTP/2, HTTP/3, HTTPS, SMTP, POP3, IMAP4, SSH/SFTP/SCP, SIP, Streaming, DNS over TLS and HTTPS, and other protocols.
Mixed Traffic Tests	Measure the impact on application performance when using real-world built-in applications or extended applications 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.
AI Inference Testing	Validate the end-to-end AI inference infrastructure and LLM application performance. Evaluate how network components, API gateways, firewalls, ADCs, GPU capacity, and security controls impact LLM inference throughput, latency, and accuracy. Ensuring AI Data Center infrastructure delivers optimal performance without overspending on compute and networking resources.

Technical Specifications continued

Product Feature	Description
CyberFlood Feature Details continued	
ZTNA Testing	Validate the scale and performance of the ZTNA architecture by emulating authenticated, unauthenticated and unauthorized users via SMAL and OIDC to validate least-privilege access policies
Traffic Replay	Replay your own traffic profiles at scale to determine the impact of customer traffic flows on network devices and services
DNS Tests	Overload your DUT by sending hundreds of thousands of DNS queries per second for it to process and traverse, as well as process the corresponding events that occur on the DNS responses
Automation	CyberFlood RESTful API and Avalanche Tcl API
Dimensions	2RU - 3.5" H x 17.2" W x 22.6" D; fits standard 19" rack
Weight	34 lbs (15.6 kg)
Operating Environment	0°C to 40°C (32°F to 104°F)
Non-Operating Environment	-20°C to 70°C (-4°F to 158°F)
Operating Relative Humidity	8% to 90% (non-condensing)
Non-operating Relative Humidity	5% to 95% (non-condensing)
Power Requirements	100-240 Vac, 50/60 Hz, 2000 W

Ordering Information

Part Number	Description
CF-KIT-001-CF1000	CF1000 Base Appliance Kit 4 x OSFP and 8 x QSFP28 (add-on unit)
CF-KIT-002-CF1000	CF1000 Performance Kit 4 x OSFP and 8 x QSFP28

Performance Kits include HTTP/HTTPS Throughput, HTTP/HTTPS CPS, HTTP/HTTPS Concurrent Connections, DNS, Throughput with Mixed Traffic (default protocols), Advanced Mixed Traffic, and Network Traffic Replay test methodologies. OSFP and QSFP28 transceivers are sold separately. Security Testing options and other bundles are also available. Avalanche licenses are available separately for the CF1000. Please contact VIAVI Sales for more information.

VIAVI Services

Education Services

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

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

cf1000-ds-hse-nse-ae
30195084 900 0426