CF400 CyberFlood Appliance

For CyberFlood and Avalanche

In today's digital world of cloud computing, IoT, and a hyper-connected digital economy, it's essential that the performance of content-aware networks, security systems, and web applications is carefully assessed. Business-critical transactions and communication must perform as expected and scale to meet accelerating traffic demands–especially encrypted traffic.

The CF400 is a powerful Layer 4-7 stateful traffic performance solution that is capable of extremely high throughput with high-strength cryptographic and hyper-realistic application traffic. It can generate over 400 Gbps of application throughput, delivering the industry's best price/performance value to VIAVI users. The CF400 enables network security and application delivery platform vendors to shorten their development and sales cycles, and allows hyperscale network operators to rightsize their network investments and deliver high end-user application performance and Quality of Experience (QoE).

Performance and Flexibility

The CF400 is available in a Dual-speed 8 x 100G QSFP28 and 8 x 100G Multi-speed QSFP28/QSFP+ interface configurations. The multi-speed option provides quint-speed native connectivity for 10G, 25G, 40G, 50G, and 100G Layer 4-7 application traffic. Users can specify load variables and easily create tests with mixed traffic profiles, emulating real-world network scenarios. The CF400 can generate over 400 Gbps of application throughput, delivering the industry's best price/performance value to VIAVI users.

Ultra-High Application Performance Testing Solution

The CF400 for the VIAVI CyberFlood and Avalanche testing tools provides the industry's highest performance and capacity testing solution, with support for quint-speed 100G interfaces.

Users can test the performance limits of network devices, web applications, and media services, ensuring Quality of Service (QoS) and QoE for their customers.

The CF400, along with CyberFlood and Avalanche, can deliver 400 Gbps of application traffic and 200 Gbps of encrypted traffic performance testing capabilities in a single appliance.

Applications

- Network performance testing
- Web application testing
- 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

With built-in advanced cryptographic acceleration capabilities, the CF400 delivers the industry's highest TLS performance capability, with 200 Gbps of encrypted throughput and 200,000 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.

CF400 Performance Examples[1]	
HTTP Bandwidth (Bi-directional)	590 Gbps
HTTPS Bandwidth	280 Gbps
HTTP Connections (GET) per second	4,500,000
HTTPS Connections (GET) per second	300,000
HTTP Concurrent Connections	320,000,000

1. Performance numbers are obtained using a single CF400 as a client and server. TLS v1.3 Performance is with AES-128-GCM-SHA256 cipher suite.

Modular Terabit Scale

The CF400 includes a built-in CyberFlood controller. Within minutes, users can be up and running tests with the powerful, web-based CyberFlood solution, without the need for additional hosting platforms. In addition, the modular appliance architecture provides the flexibility to stack multiple appliances together in a single test system to validate the performance limits of multi-terabit scale security controls, application delivery platforms, and hyperscale data center networks.

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 www.netsecopen.org.

User Realism with Avalanche

Avalanche software on the CF400 supports the configuration of extremely realistic user behaviors, so that 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. 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

- **>400 Gbps Stateful Application Traffic:** Provides the capability to generate over 400 Gbps of stateful Layer 4-7 traffic. Each CF400 supports high-density 8 x 100G or 16 x 10G or 16 x 25G or 8 x 40G or 16 x 50G 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, CIFS, 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 CF400 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.
- **VPN Testing:** Validates IPSec and SSL VPN[2] 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	
CF400 with 8 x 100G QSFP28	8 x 100G interfaces 8 x 40G interfaces
CF400Q (Multi-Speed) with 8 x 100G QSFP28	8 x 100G interfaces 16 x 10G interfaces 16 x 25 interfaces 8 x 40G interfaces 16 x 50G 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 application 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[2] from tunnel setup to data traffic handling

2. Expanding set of SSL VPN dialects

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, FTP, 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
ZTNA Testing	Validate the scale & performance of the ZTNA architecture by emulating authenticated, unauthenticated & unauthorized users via SAML 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 – 40°C (32°F – 104°F)
Non-Operating Environment	-40°C – 70°C (-40°F – 158°F)
Operating Relative Humidity	8% – 90% (non-condensing)
Non-operating Relative Humidity	5% – 95% (non-condensing)
Power Requirements	100-240 Vac, 50/60Hz, 2000W

Ordering Information

Part Number	Description
CF-KIT-001-CF400	CF400 Base Appliance Kit 8 x QSFP28 (add-on unit)
CF-KIT-002-CF400	CF400 Performance Kit 8 x QSFP28
CF-KIT-004-CF400Q	CF400 Multi-speed Base Appliance Kit 8 x QSFP28 (add-on unit)
CF-KIT-005-CF400Q	CF400 Multi-speed Performance Kit 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.

QSFP28 and QSFP+ transceivers are sold separately.

Security Testing options and other bundles are also available. Please contact VIAVI Sales for more information.

Requirements

The client used to access the virtual host/CyberFlood controller must meet the following minimum requirements to run CyberFlood:

- Any Windows, Mac or Linux PC running the latest browser versions
- Firefox browser
- Google Chrome browser

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

cf400cyberflood-ds-hse-nse-ae
30194667 901 0326