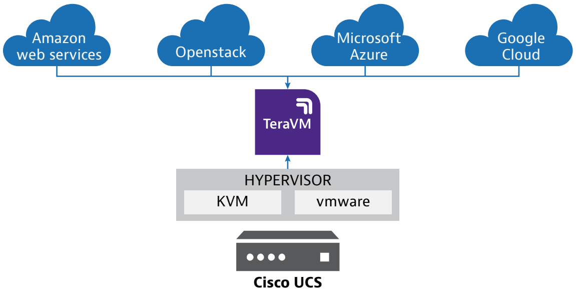
TeraVM™

VIAVI Solutions

TeraVM is a software based L2–7 test tool running on x86 servers and in the Cloud (Azure, Amazon, Google, Openstack etc.), delivering a fully virtualized application emulation and security validation solution to test and secure devices, networks and their services.

Why TeraVM?

- **Flow based tool with realism**
  - Provides per-flow statistics in real time
  - Statefully emulates and measures individual endpointand application performance for data, voice, video and security services
  - Easily pinpoint and isolate problem flows and bottlenecks
- **Adaptive engine**
  - Dynamically and Automatically find the maximum capacity of Devices Under Test
  - Same test profile can be used for multiple platforms
- **Centralized License Server/Elastic Test Bed**
  - Scale with realism and grow on demand with license sharing across geographical locations
  - Flexibility to run anywhere… lab, datacenter and the cloud, with consistent performance coverage
  - Sharing test resources and methodologies delivering the most cost-effective solution
  - Shareable Cybersecurity threat database, maximizing resource utilization and total cost of ownership
  - Auto License Check-In on test completion
- **Wireless Mobility (5G, 4G, 3G, 2G) validation with realism**
  - Highly scalable user and control plane traffic. Scale beyond 100 Gbps of traffic



Key Facts

TeraVM is 100% virtual

- Same test tool used to test physical solutions and/or virtual solutions
- Supports all major hypervisors: ESXi, KVM
- Supports all major cloud platforms: OpenStack, AWS, MS-Azure, Google Cloud, Oracle OCI, Containerization
- Supports 1 GbE, 10 GbE, 40 and 100 GbE NICs

Automation and Orchestration

- REST, CLI, Perl, TCL, XML, Java API, Python, Jython
- Cisco LaasNG, Cisco pyATS, Qualisystems (CloudShell)

L2–7 Stateful Traffic Application Emulation

- Voice: CUCM, CUBE, VoIP, WebEx, VoLTE, SIP & RTP, MOS
- Video: CMTS, CDN, Multicast, AMT, ABR, IPTV, VoD, OTT streaming, Video conferencing, WebEx, TelePresence, HTTP Video
- Data: TCP/UDP, Teraflow, Ookla speed test, HTTP/HTTPS, SMTP/POP3, FTP, P2P, DNS, Quick UDP Internet Connections (QUIC)

Secure Access Firewall/VPN (ASA Firewall, FirePOWER)

- Secure TCP/UDP Protocols (SSL, TLS, DTLS, IPSec IKE)
- Client and Clientless VPNs (Cisco AnyConnect SSL and IPsec)
- 802.1x EAP-MD5, EAP & PEAP with MS CHAPv2 Authentication
- Mobile Secure Gateway validation (S1-U over IPSec)

Cybersecurity Threat and Malware Penetration

- 40,000+ attacks (Spam, Viruses, DDoS, Malware), updated monthly
- DDoS attack applications:
  - Flood: SYN, Reflective SYN, Reset, UDP, Ping, ARP
  - Attacks: Teardrop; UDP Fragmentation; Configurable Rates, Start and Stop
  - Spoof Mac addressing
- Mixed application flows: Good, the Bad and your Own

Wireless RAN and Core Emulation

- vRAN: 5G-NR, 4G-LTE, 3G, 2G – 1,000s of RANs
- vCORE: 5G (NSA & SA), 4G-LTE 3G, 2G, Mobility, SecGW, MEC, Network Slicing – Millions of UEs and Bearers
- CIoT: IPDD over NAS, NIDD over SCEF at Scale
- WiFi ePDG offload (EoGRE)

Wireless Core Interface Testing

- Support testing across multiple key Core interfaces
- Error Injection over 5G-N2 (AMF)
- Error Injection over 4G-S1 (MME)