VIAVI

VIAVI Solutions

TeraVM™

What is TeraVM?

TeraVM is a software based L2–7 test tool running on x86 based servers, in the Cloud (Amazon, Azure, Google Cloud, Oracle OCI, Openstack) and as a container, 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 endpoint and 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
  - Faster setup, faster testing, faster results = more testing = better quality
- **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
  - System utilization reports (Location, User, Testbed, Licenses in use, Usage stats)
- **Wireless Mobility (5G, 4G, 3G, 2G) validation with realism:**
  - Emulate a city worth of stateful UE and subscriber network activity
  - 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)

Application Support

General
– System utilization reports (Location, User, Testbed, Licenses in use, Usage stats)
– License check-in default timer

Adaptive Engine
– Dynamically and Automatically find the maximum capacity of Devices Under Test
– Same test profile can be used for multiple platforms
– Faster setup, faster testing, faster results

Network Interface Support
– Support for 1/10/40 Gbps I/0

Data
– Jumbo Frame support with max MTU/ Segment configurable
– TeraFlowUDP Out-of-Sequence Statistics
– TCP / UDP, Teraflow, Ookla speed test
– HTTP / HTTPS
– HTTP 2.0
– SMTP / POP3 (incl. file attachments)
– FTP (Passive/Active), P2P applications, DNS
– FTP client session count limit
– DNS client (w/ HTTP/S applications incl. IP address resolution)
– DNS Server

Address Assignment
– Configurable MAC
– DHCP, PPPoE (IPv4 & IPv6)
– Dual Stack (6RD, DS Lite)

Ethernet Switch
– VLAN Tagging (up to 8 concurrent tags)
– ACL, 802.1p, DSCP

Data Center
– VxLAN, GRE, SR-IOV

Automation
– REST, CLI, Perl, TCL, XML, Java API
– Python, Jython
– Cisco LaasNG , Qualisystems (CloudShell), Luxoft Software Defined Lab (SDL), Openstack, Cisco pyATS

Replay Application Repository
– Intelligent UDP & stateful TCP Replay: Ability to dynamically change content
– Replay large PCAP files: TCP, UDP and raw data playback
– IP Replay: multiple TCP/UDP streams
– Amplify and dynamically substitute data into PCAP files

Video
– CMTS, CDN, Multicast: IGMP v1/v2/v3 & MLD v1/v2
– Automatic Multicast Tunneling (AMT)
– Video on Demand (VoD)
– Adaptive Bit Rate (HLS, HDS, MPEG- DASH, Smooth)
– Video conferencing, WebEx, Telepresence
– HTTP based video

Voice
– Secure VoIP & WebEx calls in HTML5 UI
– Dual-Stack VoIP Gateway emulation
– Cisco CUCM, CUBE
– VoIP: SIP & RTP (secure & unsecure), SMS
– VoIP client scaling with auto generated unique AKA authentication request per client
– VoLTE Emergency calls support
– Dual Hosted UACs, SIP Trunking
– Voice & Video quality metric (MOS simultaneously supported)
– EVS codec support, various bit rates, silence suppression
– G.711 Support for SID – RFC3889
– SIP Updates for IMS incl. PANI information
– MCPTT group calls (incl. KPI support)

Secure Access / VPN
– SSLv2/3, TLSv1.0/1/2/3 and DTLSv1.0/2
– TLS Client-side Cipher Suite Selection
– Dynamic IPv6 Assignment for AnyConnect VPN Client
– Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/ v2 (DH groups 31 & 32)), Generic remote access, CSFR support
– VPN Clients: Cisco AnyConnect, Fortinet, Juniper, Pulse Secure,, F5, Huawei, AT&T SSLT
– Cisco Umbrella
– SAML, SSO, Active Directory based login
– 802.1x EAP-MD5, EAP & PEAP with MS CHAPv2 Authentication
– 802.1X Accounting Start and Stop Records
– Site to Site VPN - IPV6/V4
– Additional security to limit access to public IP address assigned to TeraVM in public cloud environments
– Cisco AnyConnect ECDSA, EdDSA Cert
– authentication
– PPTP VPN Client and Server supported

Security
– 40,000+ Malware attacks & Cybersecurity threats, updated monthly
– Spam / Viruses / DDoS / Malware
– Malware Application Profiles
– DDoS attack applications:
– Flood: SYN, Reflective SYN, Reset, UDP, Ping, ARP
– Attacks: Teardrop; UDP Fragmentation; Configurable Rates, Start and Stop
– Spoof Mac addressing

– Cybersecurity Database w/ proven exploits
– Good and Bad mixed traffic flows
– Statefully scale Cisco specific threats
– Ability to use 3rd party threat libraries
– Ability to turn on /off Extended Master Secret (RFC 7627) support flag to test Cisco FTD, ASA and other security solutions
– Support for TLS 1.3, TLS 1.2 simultaneously on Client and Server
– Configurable TLS record size
– TCP delayed ack (timer based)
– HTTP Strict Transport Security (HSTS) header support
– TLS SNI support incl. unique certificate per FQDN

SLA Monitoring
– TWAMP-RFC 5357, PING-RFC 792
– Cisco Netflow Records/Exporter emulation at scale

Mobility - 5G, 4G, 3G, 2G
– Core and RAN: 3GPP Rel.8, 10, 11, 13, 15
– vRAN emulation:
– 5G-NR, 4G-EUTRAN, 3G-UTRAN, 2G-GERAN at 1,000s of RANs
– Core Emulation:
– 5G (NSA & SA), 4G-LTE, 3G, 2G with Mobility at millions of UEs and Bearers
– 5G, 4G, 3G, 2G Core interface testing
– Error Injection over 5G-N2 (AMF), 4G-S1 (MME)
– Encrypted RAN load for SecGW
– GTP tunnel support; GTPv2 (4G) S11/S5; GTPv1 (3G) Gn (4G) S1-U
– VoLTE (secure/unsecure), ViLTE
– ePDG Wifi Offload (EoGRE)
– VoWiFi (functional testing)

Internet of Things (IoT)
– Client emulation
– CoAP-RFC 7252
– NIDD over SCEF, S11-U, S1-U
– SCEF Emulation Including Protocol Relay

Platform Support
– Google Cloud Support
– Oracle OCI
– Containerized TeraVM (docker)

Hypervisors
– VMware ESXi
– KVM Ubuntu
– Amazon AWS
– Microsoft Azure
– KVM Redhat
– Openstack

NetSecOPEN Tests
– NetSecOPEN Test Suite

NetSec⊘PEN

Specific Test Coverage

TeraVM includes Cisco specific endpoint emulation and real time measurements

- Dynamic IPv6 Assignment for AnyConnect VPN Client
- Cisco AnyConnect SSL VPN Client
- Cisco AnyConnect IPSec IKEv1/IKEv2 VPN Client
- Cisco NetFlow Records, NetFlow Exporter Emulation
- Cisco Identity Services Engine (ISE) with 802.aX client

- Cisco Umbrella
- Captive Portal testing
- Cisco TelePresence
- Captive Portal testing
- Cisco TelePresence
- Cisco WebEx
- Cisco Phones

- Cisco Video Clients
- Cisco DNA Center
- Mobile phones for Security Gateway
- IoT Device

VIAVI
VIAVI Solutions