VIAVI Solutions

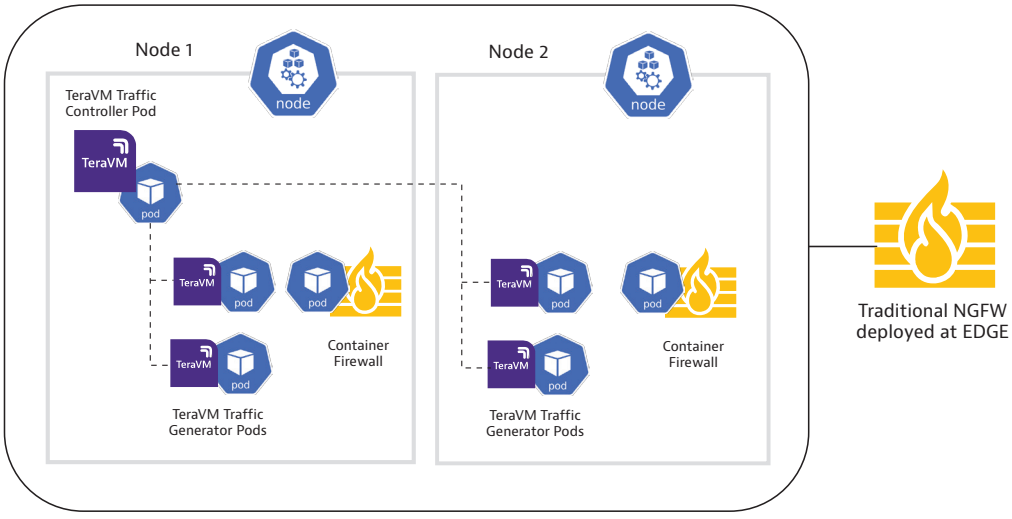
Brochure

VIAVI
Containerized TeraVM Security Test Solution

Validates Container Security Solutions deployed in Google GKE and Amazon EKS Kubernetes services

Overview

With Next Generation Firewalls (NGFWs) evolving to be deployed in container clusters, there is a need to validate these new container based firewalls for performance and efficacy before deployment. Conventional Test Tools are designed for testing firewalls deployed at EDGE of network. But to test container firewalls, the test solution is required to be inside the container environment as these firewalls have to focus on securing east-west traffic flowing between Kubernetes namespaces in addition to securing inbound and outbound traffic.



A Kubernetes (K8S) Container Cluster

The TeraVM Classic product by VIAVI is the industry's first commercial tool that offers a cloud native testing solution natively integrated with Kubernetes. Available from TeraVM v15.1 release since June 2020, containerized TeraVM is deployable in public cloud managed Kubernetes services such as Google Kubernetes Engine (GKE) and Amazon Elastic Kubernetes Service (EKS) and also on Kubernetes on bare-metal on-prem servers.

TeraVM Classic in Container Form Factor

A TeraVM test bed is a group of TeraVM components that generate IP test traffic with customizable traffic profiles. In a Containerized TeraVM deployment the test bed is containerized and consists of a number of Pods that are deployed over an available number of Nodes. The setup consists of TeraVM Controller Pod that acts as a management entry-point and Test Module pod pairs that act as worker. The traffic can be easily scaled by adding more Test Module Pod pairs.

Customers can easily deploy TeraVM Classic tool to specific namespaces in Kubernetes environments hosted on-prem or in public clouds and with major public cloud managed Kubernetes services such as GKE and EKS. The deployment is made seamless in different environments using Kubernetes package manager Helm and the deployment is parameterized with helm custom values. The Containerized TeraVM works with default CNI plugins in EKS and GKE. TeraVM also support other third party CNI plugins as Calico and Flannel if the cluster requires so.

The IP address and networking configuration required for the tests are automatically populated by the individual Traffic pods. In additional TeraVM also offers the ability to generate traffic towards service IP's instead of the Pod IPs, thereby emulating realistic kubernetes cluster traffic behaviour.

TeraVM Classic supports a wide variety of voice video and data traffic Profiles to be emulated in the container network including HTTP(S), FTP(S), SMTP(S), POP3(S), VOIP, TCP Playback, UDP playback. All Traffic Profiles support customizable TLS settings with selection of TLS 1.2,1.3, Ciphers, signature hash algorithms, SNI extension, custom X.509 certificates, configurable key size, Common Names, TLS Record Size to name a few.

Use Cases – Containerized TeraVM

URL Filtering. Containerized TeraVM can be used to generate HTTP/HTTPS traffic with million URLs for exercising container firewall's URL filtering policies, validating the ability of the firewall to block blacklisted sites.

Kubernetes metadata based policy testing. Containerized TeraVM's traffic pods allow annotations that makes it possible to test metadata based policy on the containerized firewalls.

Application Traffic and TLS inspection. Containerized TeraVM can generate various L7 application traffic that allows to test the firewall for Content inspection and TLS decryption capabilities.

Performance and Recommended specification for TeraVM Traffic Pod		
K8s Service provider	**System Characteristics**	**Performance per TeraVM Traffic Generator Pod Pairs**
Amazon Cloud - EKS	Machine type: c5.2xlarge CNI: Amazon VPC CNI plugin	HTTP Throughput Performance Per TeraVM Traffic Generator Pod (2 vCPU/1 CPU): • 1.7 Gbps (single k8s node) • 1.6 Gbps (across two k8s node) **Total Resources used by a Pair of TeraVM Traffic Generator Pods** Number of vCPU: 2 Number of CPU: 1 Memory: 4 GB (2 GB per TeraVM Traffic Generator Pod) Disk: 2 GB
Google Cloud - GKE	Machine type: c2-standard-8 CNI: Kubenet (Default)	HTTP Throughput Performance Per TeraVM Traffic Generator Pod (2 vCPU/ 1 CPU): • 2.7 Gbps (single k8s node) • 2.7 Gbps (across two k8s node) **Total Resources used by a Pair of TeraVM Traffic Generator Pods** Number of vCPU: 2 (1 vCPU per TeraVM Traffic Generator Pod) Number of CPU: 1 Memory: 4 GB (2 GB per TeraVM Traffic Generator Pod) Disk: 2 GB

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-containerization-br-wir-nse-ae
30193057 900 0421

VIAVI Solutions

Brochure

VIAVI
TeraVM
Cybersecurity Database

Agile and Progressive Security Validation.

Cybersecurity threats are evolving at a pace, that it has now become extremely difficult, to continuously assess and validate the effectiveness of security against the latest exploits. In many cases, it has become so complex and costly that many security defences simply go unvalidated. At the rate that new vulnerabilities are being exposed, there is a real worry that security defences are lagging behind.

TeraVM's Cybersecurity Threat Database provides the capability to analyze security with a comprehensive repository of traffic signatures, enabling assessment with the Good, the Bad and your Own. The TeraVM threat database includes known Common Vulnerability and Exposures (CVE), unknown (researched threats) and the ability to include your own traffic profiles, providing the maximum coverage possible for threat assessment.

With TeraVM, you can be assured that you will have the most up to date assessment capability, as and when the threat-scape changes. This not only helps to ensure that you have the right level of security but your investment in threat assessment is protected for the future.

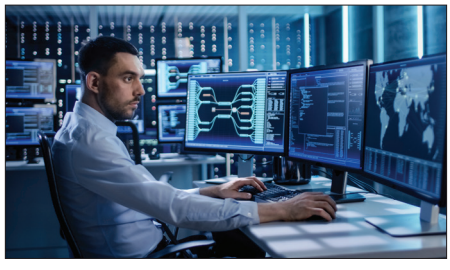
Efficient and Reliable Assessment of Security Counter Measures

Security Hardening

By emulating the latest CVE security threat and exploit profiles, users of TeraVM can quickly assess security vulnerabilities in a safe and contained manner. TeraVM enables users to quickly pinpoint where the weaknesses are in their security counter measures ensuring the appliance or application is patched for any vulnerabilities.

Performance Under Duress

Determine with precision the effectiveness of security counter measures against scaled and targeted attacks. Assess what the impact is on normal network operations in a safe and contained manner. Use TeraVM to emulate common distributed denial of service attacks with known exploits and device vulnerabilities.



Exploit Recovery

Use TeraVM's security threat and exploit application library to assess how effective planned procedures are in recovering from a breached security defence. TeraVM delivers a safe contained environment in which to build knowledge and skills for pragmatic recovery plans.

Evolve with the Threat-scape

TeraVM's security threat and exploit application database is updated on a regular basis, ensuring you have the right defenses as and when needed. Assess with the latest vulnerabilities, protocol attacks and malware. TeraVM enables users to store up to a terabyte of additional traffic signatures. Future proof your investment in security assessment by choosing TeraVM.

TeraVM – Security Assessment with the Good, Bad and your Own

TeraVM is an IP traffic emulation and performance measurement solution used to validate the performance of networks and applications. Using TeraVM, emulate the most realistic attack scenarios by delivering mixed flows of legal and malicious content. TeraVM enables users to use a mix of known (CVE), unknown (researched threats) and your own traffic signatures, with the ability to store up to a terabyte of traffic signatures.

Assess a range of security counter measures such as appliances, applications and policies to ensure that the most robust security principles are applied. TeraVM's evolving threat database ensures that any future changes in the threat-scape or security counter measure e.g. a security appliance upgrade, does not diminish or expose the secure environment to vulnerabilities and exploits.

Common Vulnerability and Exposure (CVE) profiles

The TeraVM threat database includes known threats that target network user devices and applications, but more importantly also includes malicious traffic destined for server-side appliances and applications. Enabling users to assess for the lowest exploit risk.

The database includes many of the known vulnerabilities for vendors of security appliances and software applications. In addition, the repository includes vulnerabilities of the common open source server side applications. A sample of the CVE related threats and exploits contained in the TeraVM threat database include:

Network Users
• Network Services, Servers & Infrastructure
• Adobe: Acrobat and Reader, Flash Player, Photoshop
• Apple: Safari, QuickTime Player
• Cisco: IP Phone
• Facebook: ImageUploader
• Google: Chrome
• McAfee: VirusScan
• Mozilla: Firefox, Seamonkey, Thunderbird
• Microsoft: Windows, Internet Explorer, Powerpoint, Outlook, etc
• Sun Microsystems: Java Runtime Environment, JDK

Network Users
• Citrix: XenCenterWeb
• Cisco: ACS, Catalyst, IOS
• McAfee: SecurityCenter, E-Business Server
• Microsoft: IIS, Exchange Server, SQL server
• Oracle: Hyperion Financial Management
• Sun Microsystems: Web Server
• Symantec: Veritas NetBackup
• WordPress: Numerous themes and plugins
• Joomla: VirtueMart
• Zope: Application Web Server

For a complete overview of the latest threats and exploits visit: https://www.viavisolutions.com/en-us/node/60199

TeraVM Capability Overview	
General	Real-time isolation of problem flows
Data	TCP / UDP
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address	MAC, VxLAN
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet Switch	VLAN and Double VLAN Tagging (Q-in-Q)
	ACL, 802.1p, DSCP
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (RTSP)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure VPN	SSL/TLS/DTLS, IPsec (IKE v1/v2)
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN Client
	Juniper Pulse, Juniper Network Connect
	802.1x EAP-MD5
Security attack mitigation	Spam / viruses / DDoS
Voice	VoIP: SIP & RTP (secure & unsecure), H.323
	Dual Hosted UACs, SIP Trunking
	Voice & video quality metric (MOS)
LTE/4G	GTP tunnel support
SLA	TWAMP
Automation	CLI, Perl, TCL, XML, Java API

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-cybersecurity-br-wir-nse-ae
30187517 900 0918

VIAVI Solutions

Brochure

VIAVI
TeraVM

Ethernet over GRE (EoGRE) validation for WiFi-offload.
Per UE stateful application performance assessment.

TeraVM™ supports validation of WiFi-offload scenarios using Ethernet over GRE (EoGRE) and/or IPsec, providing performance visibility on each and every tunnelled user endpoint's (UE) encapsulated application traffic. This highly scalable solution enables emulation of thousands of wireless access points and millions of tunnelled endpoints.

TeraVM's stateful per flow architecture enables functionality such as transparent ethernet bridging with configurable tunnel options such as keep-alive and failover scenarios.

TeraVM supports validation of the two key GRE headend encapsulations:

- L3 IPv4 encapsulation (GRE): Static IP address assignment
- L2 IPv4 encapsulation (EoGRE): DHCPv4 over GRE

Validation for WiFi-offload scenarios

TeraVM provides for validation of untrusted WiFi access points of evolved Packet Data Gateways (ePDG) and/or trusted WiFi access gateways (TWAG).

Understanding the performance and reliability of the wireless LAN gateway is key to ensuring a seamless user experience that is, that the UE does not loose connectivity and continues to have access to a range of application service types.

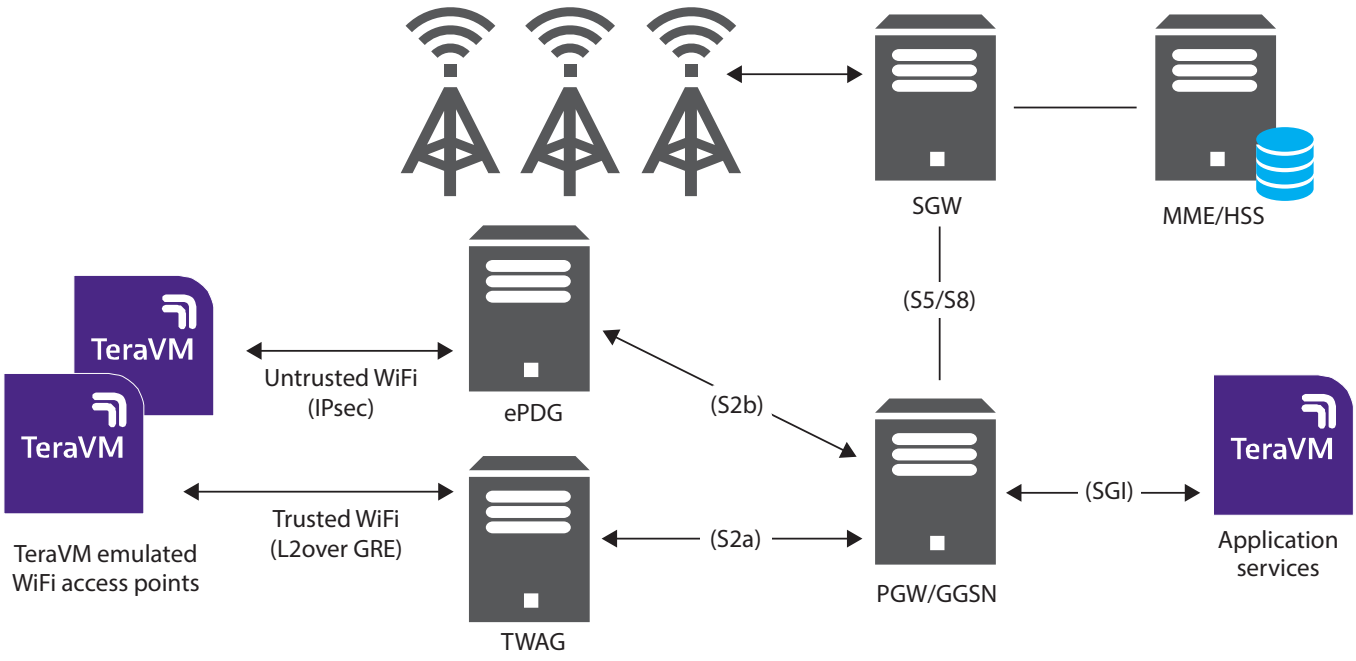
TeraVM as a stateful emulation solution, supports tunnel failover: where each tunnel may select to use keepalives, move from UEs from primary to secondary flows with unique measurements for failed pings.

Advantages

- Emulate millions of GRE encapsulated tunnels
- Meaure per tunnelled endpoint, per application performance
- Dedicated metrics, including tunnel endpoint failovers & ping failures

Features

- Support for L2 and L3 GRE encapsulation
- Unique MAC address assignment per EoGRE Tunnel
- Stateful voice/video applications
- Cloud platform enabled support for AWS, Azure, OpenStack
- Out of millions of UE sessions, easily pinpoint and isolate UEs experiencing poor application quality inside GRE tunnels



TeraVM validation of WiFi-offload gateways

Introducing TeraVM

TeraVM is an application emulation and security performance solution, delivering comprehensive test coverage for application services, wired and wireless networks.

TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere—lab, datacenter, and the cloud, with consistent performance coverage, ensuring that highly-optimized networks and services can be delivered with minimal risk.

EoGRE emulation with the most realistic load scenarios

Using TeraVM users can emulate the most realistic load scenarios for performance validation of throughput, connections, and latency for unique UE traffic being encapsulated in GRE tunnels.

TeraVM enables emulation for both IP over GRE and/or Ethernet over GRE use cases. TeraVM's flexible configuration enables users quickly assess performance of the various headend encapsulation options. TeraVM's stateful application emulation and per-flow performance validation is ideal for assessing the end-users quality of experience in the GRE tunnel.

TeraVM can be deployed to cloud services such as Amazon Web Services (AWS), Azure, and/or OpenStack, providing for flexible assessment scenarios and cost efficiencies.

TeraVM EoGRE use cases

EoGRE service validation

Validate EoGRE gateway functionality to provision UEs with static/dynamic IP and assess for tunnel failover scenarios that is, allocate secondary tunnels.

UE application performance validation over GRE

Validate the performance of unique UEs accessing and making real calls through EoGRE enabled gateways, determine performance for both normal and extreme load conditions.

TeraVM Capability Overview	
General	Real-time isolation of problem flows
	Elastic Test Bed (up to 1Tbps)
Network interface support	Support for 1/10/40 Gbps I/0
	Mellanox ConnectX-4 support for 56/100Gbps
Data	TCP / UDP, Teraflow, Ookla speed test
	HTTP (v1/2, incls. stateful response parser)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address assignment	Configurable MAC
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet swith	VLAN Tagging (up to 8 concurrent tags)
	ACL, 802.1p, DSCP
Data Center	VxLAN, GRE, SR-IOV
Replay	Replay large PCAP files TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (VoD)
	Adaptive Bit Rate Video (HLS, HDS, MPEG-DASH, Smooth)
	Video conferencing, Webex
Secure Access / VPN	Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/v2), Generic remote access
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN
	Cisco ScanSafe
	Juniper Pulse, Juniper Network Connect
	SAML (F5, Citrix SSO), Dell SSO
	802.1x EAP-MD5
Security attack mitigation	Spam / Viruses / DDoS
	Cybersecurity Database
Voice	VoIP: SIP & RTP (secure & unsecure), SMS
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	EPC and RAN (Rel.8, 10, 11)
	VoLTE (secure/unsecure), ViLTE
	WiFi Offload (EoGRE)
SLA	TWAMP, PING
Automation	CLI, Perl, TCL, XML, Java API
	Python, Jython
	Qualisystems (CloudShell)
	OpenStack

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-eogre-br-wir-nse-ae
30187449 900 0918

Brochure

VIAVI
TeraVM IMS Messaging

Send/receive SMS. TeraVM performance testing for LTE.

VIAVI TeraVM supports short message service (SMS) for 3GPP IP Multimedia Subsystems (IMS). Users of TeraVM can emulate on a per subscriber basis unique SMS activity while actively partaking in voice over LTE (VoLTE) calls.

Key benefits

VIAVI TeraVM SMS feature permits the users to emulate 3GPP IMS multimedia aware endpoints, which can actively receive and/or send short messages while on a VoLTE call.

TeraVM SMS is fully stateful and can partake in message exchanges with 3rd party short messaging service centre (SMSC) servers. TeraVM stateful messaging enables functional performance and load performance testing of messaging services, plus enables assessment to deliver the message whilst active calls are ongoing.

The fully integrated SMS feature enables flexible provisioning including the ability to send messages to one or to many recipients defined in a list of recipients and/or to send many messages to emulate real-world diversity.

In addition, TeraVM enables a level of realism by facilitating message bursting or message chattiness across the IMS framework. Message bursting is used to stress test the ability of the various Short Message Gateway (SM-GW) and CSCF functions to process, deliver and report on the messages generated.

Sample Test Configurations

SMSC Gateway Testing

Emulate 3GPP IMS multimedia enabled endpoints with dedicated endpoints for SMS send and receive. Determine functional performance of the SMSC, ensuring correct configuration and the ability to send and receive SMS on a per endpoint basis.

TeraVM SMS flexible configuration

- Unique message/message lists per emulated subscriber
- Send/Receive SMS messages while making VoLTE calls
- Configurable SMSC details, use multiple SMSCs
- Emulate per subscriber message bursting

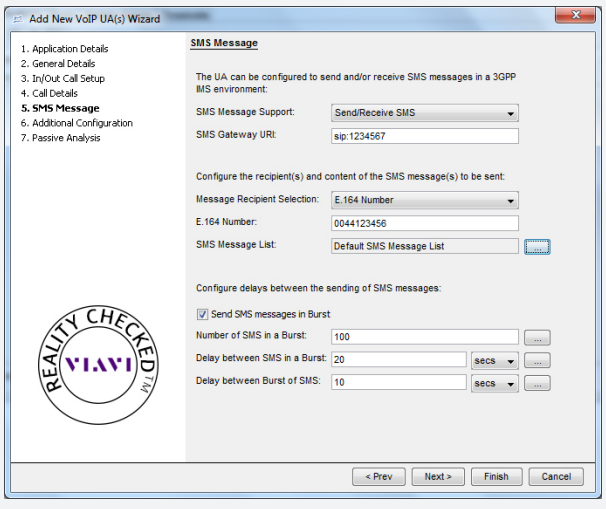


Figure 1: TeraVM integrated SMS feature

VoLTE + SMS Performance Testing

Emulate on a per UE basis voice calls using adaptive multi-rate (AMR) multi-media codecs, test using both narrow- and wide-band codec types. Functional performance test SMS on UEs partaking in live calls, assess performance of concurrently sending/receiving SMS.

Real Application Performance Testing

Emulate unique traffic flows per UE configuration. Assess quality on multiple applications including delay sensitive applications such as voice and video when receiving SMS.

Detailed performance measurements

Dedicated SMS performance measurements per emulated 3GPP IMS multimedia endpoint. Sample performance measurements include.

- Messages Out Attempted/s
- Messages Out Delivered/s
- Messages Out Failed
- Messages Out Acknowledged/s
- Messages Received/s
- Messages Accepted/s
- Messages Acknowledgements sent/s
- Messages Acknowledgements delivered/s
- Messages Acknowledgements Failed
- SMS Mean time to Message Acknowledgement ms
- SMS Mean time to Message Acknowledgement Delivery ms

Supported Products

The TeraVM SMS feature is supported on the D500, D1000, and TVM R620 systems.

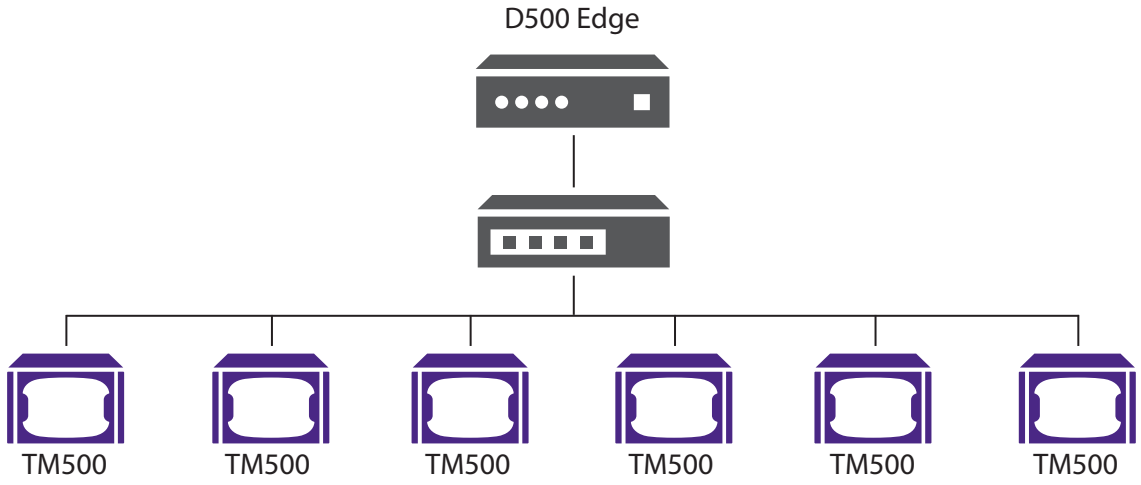


Figure 2: Example D500 deployment

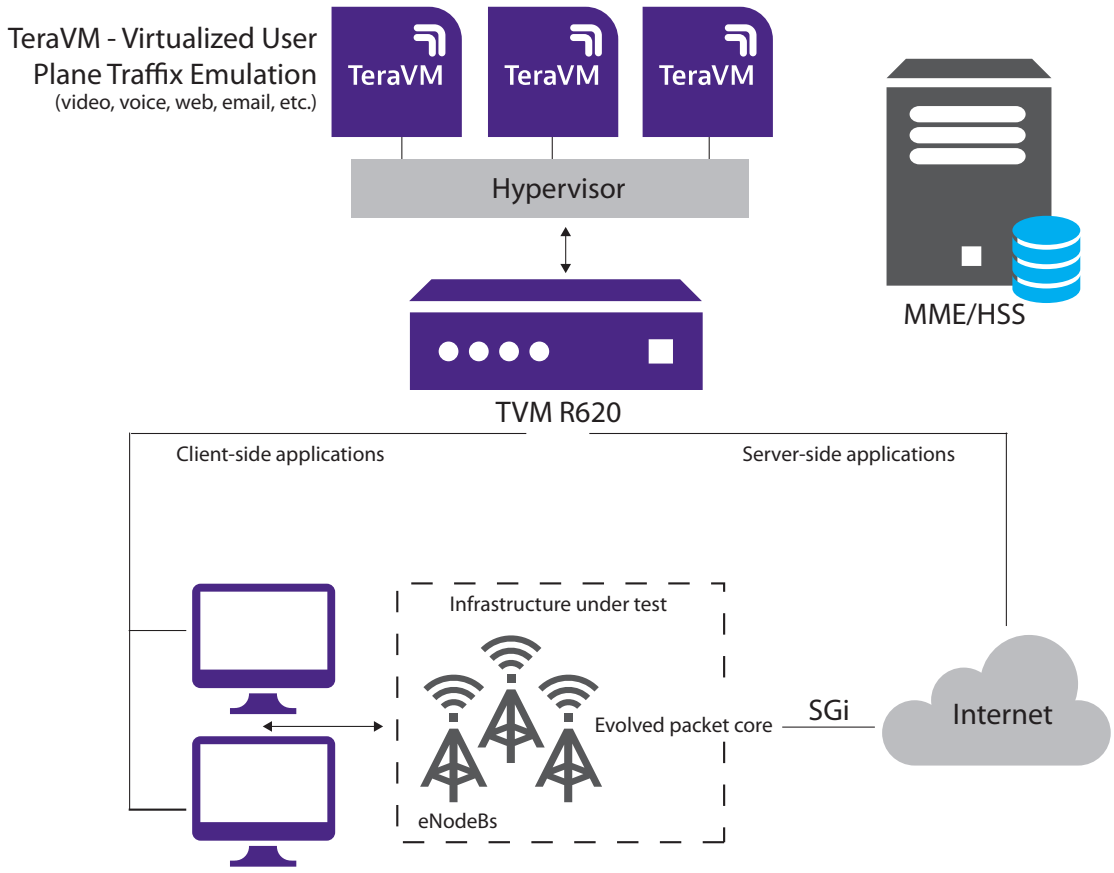


Figure 3: Example RVM R620 deployment

Comprehensive Test Capability

VIAVI TeraVM provides the industry's most comprehensive test suite with over 3,000 unique metrics; ranging from application performance to protocol tunneling down to simple port enabled testing with throughput and latency metrics. A user-defined threshold can be set on any of these metrics to easily pinpoint and isolate problem flows.

- Per flow performance measurements
  - Measure quality of experience for each and every UE on each and every emulated application traffic flow
- Comprehensive list of performance metrics per application type
  - Packets per second, Dropped/Out of Sequence Packets, Retransmitted Packets, Jitter, Latency, TCP
  - Connection Rate, Application Goodput, unique application timings, Video/ Audio quality score, etc

Software Packages

Standard Software License Bundle	
Concurrent multi-users (up to 6)	
Graphical & Command Line Interface	
IPv4 and IPv6 addressing	
Real-time isolation of problem flows	
Address Assignment	DHCP, PPPoE (IPv4 & IPv6)
Data	Web (HTTP)
	Email (SMTP)
	File Transfer (FTP, P2P application)

Diagnostics & control	ICMP (PING)
Security attack mitigation	Denial of Service attacks
Optional Software Licenses	
Flow Fault Finding: Real-time isolation of problem flows	
Video	Multicast Video (IGMP & MLD)
	HTTP Adaptive Bit Rate Streaming
	Video on Demand (RTSP)
Data	Name Server resolution (DNS)
	TCP / UDP (TeraFlow)
Voice	VoLTE (unsecure and secure AKA/IPsec)
	VoIP: SIP & RTP (secure & unsecure)
	Dual Hosted UAC
	Telepresence media conferencing
Media analysis	Video analysis includes MOS scoring
	Voice analysis includes MOS scoring
Diagnostic & control	TWAMP

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-ims-br-wir-nse-ae
30193099 900 0918

VIAVI Solutions

Brochure

VIAVI
TeraVM CloudShell Solution

TeraVM Integration with QualiSystems CloudShell

Overview

Technology providers face stiff competition and increasing pressures to maximize return on investment. TeraVM integration with CloudShell enables technology providers and vendors to dramatically improve their test infrastructure and processes to bring virtualized solutions market faster.

Shifting to virtualized development and testing environments with virtual network functions and virtual test resources can provide measurable cost savings when compared to hardware-based labs.

However, without an effective orchestration and automation platform, manual environments can erode much of these cost savings due to long cycle times and poor resource utilization.

Solution Benefits

- Increase test efficiency and ROI with improved resource sharing and reduced cycle times
- Empower teams to establish test automation best practices, maximizing resources
- Create self-service, cloud based access to testing processes, technology demonstrations, and proof of concepts
- Deliver an agile and continuous development and test environment
- Speed the time to value of data center build-outs and reference architectures

The TeraVM application emulation and security validation solution with CloudShell enables users to share test resources and their environments, delivering a highly collaborative and integrated virtual test framework.

TeraVM Solution Pack

The TeraVM CloudShell solution pack includes all the components to allow automated deployment of TeraVM within CloudShell and TestShell. The solution pack includes capabilities for configuring and running TeraVM traffic to end devices from within an active CloudShell environment. The TeraVM Shell is the root building block component that provides integration between CloudShell and TeraVM.

Virtual Lab Orchestration

TeraVM within CloudShell provides a flexible test as a service platform for creating user-friendly virtual test labs.

CloudShell provides out of the box business logic that supports testing and DevOps processes enabling a culture of highly productive resource sharing.

Automated provisioning of test environments ensures maximum productivity, leading to shorter development and test cycles.

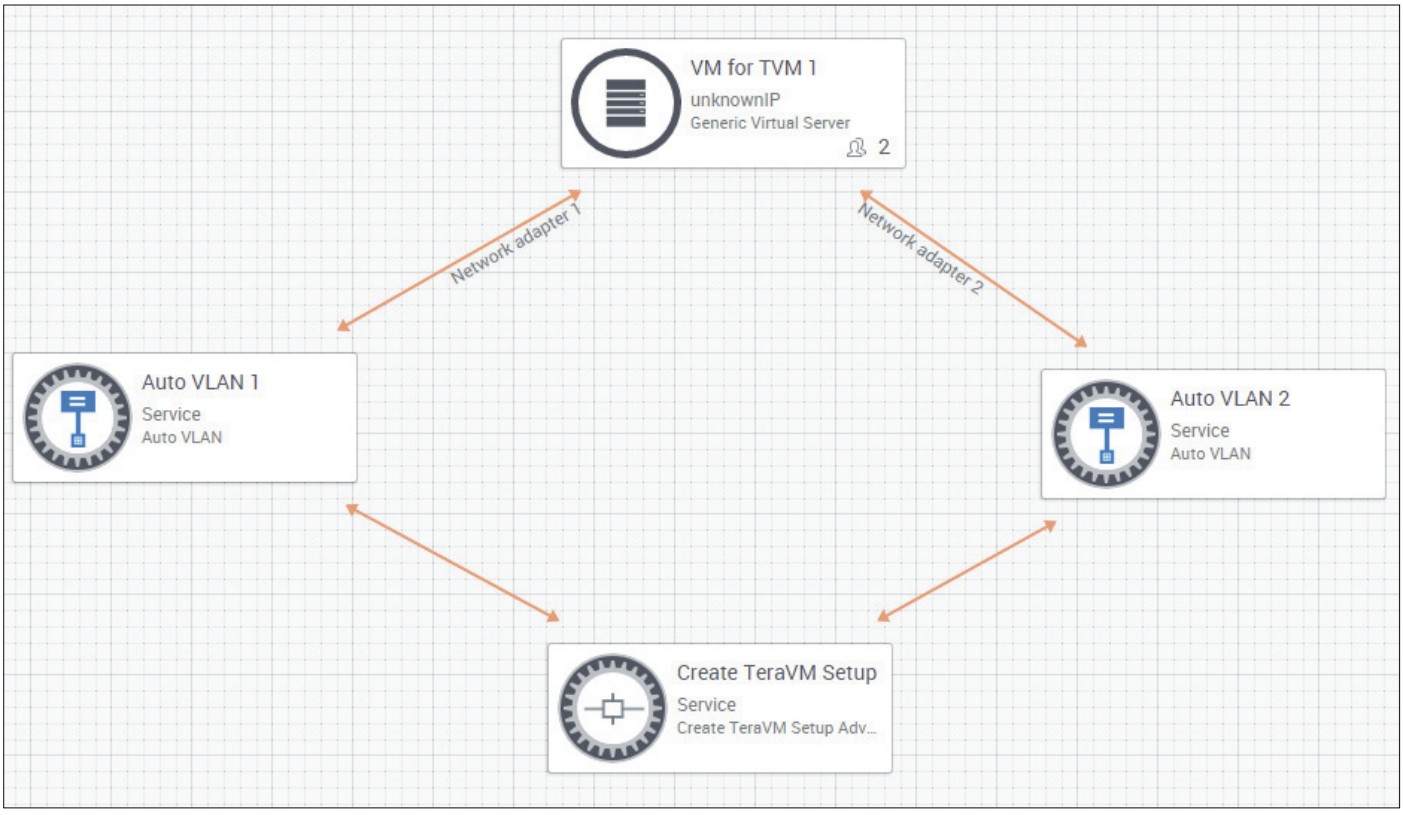


Figure 1. TeraVM with CloudShell test cycle

Test Automation

Network, data center, and cloud test projects are often challenged due to the limitations of traditional script-based approaches.

TestShell's powerful automation features paired with TeraVM enables a breakthrough in testing efficiency and productivity. Combined it optimizes virtual test resources, maximizes automation reuse, and empowers non-programmers to drive the bulk of automation creation and execution.

With TestShell and TeraVM testing teams can deploy automation into their test processes, dramatically speeding test cycles and increasing coverage.

Security Lab Orchestration

The TeraVM Cybersecurity Threat Analysis solution with CloudShell enables rapid time to value for complex network security testing environments, maximizing investments in devices, software and personnel. CloudShell with TeraVM helps testing organizations improve their security resiliency to harden network defenses.

Figure 2. Controller functions

Technical Specification

Capabilities	Description
Deploy/Remove TeraVM Controller	Automate deployment and removal of TeraVM controller as part of a CloudShell environment
Deploy TeraVM Cards and Ports	Automate deployment and configuration of TeraVM cards and port resources. Supports TeraVM cards type 1 and 2
Add TeraVM Cards and Ports	Enables users to add and configure TeraVM cards and ports within CloudShell
Load TeraVM Configuration File	Automate configuration of TeraVM with TeraVM configuration file as specified in CloudShell
Start/Stop TeraVM Test	Allows TeraVM test to be launched or stopped from within CloudShell
Delete TeraVM Test Group	Easily delete TeraVM Test Groups
Remote access to TeraVM Controller	Direct remote access via SSH and/or Web directly from CloudShell environment

*Requires CloudShell 6.2.3 HF11 and above (Supports TMVA Version 11.3, 11.4 and 12.0)

QualiSystems CloudShell offers an integrated automation package for TeraVM, a fully virtualized application emulation and security validation solution. TeraVM provides comprehensive measurement and performance analysis on each and every applications flow with the ability to easily pinpoint and isolate problems flows.

CloudShell is the leading automation and orchestration platform for transforming labs and data centers into purpose-built self-service clouds. CloudShell is deployed by leading service providers, technology manufacturers, enterprise and government IT departments worldwide. TestShell is the test automation component of CloudShell that allows rapid development of object-based test automation processes.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-cloudshell-br-wir-nse-ae
30187511 900 0918

VIAVI Solutions

Brochure

VIAVI

TeraVM Pool Manager

Enabling an Elastic Test Bed TeraVM 12.0

TeraVM™ is an application emulation and security validation solution, delivering comprehensive test coverage for application services, wired and wireless networks.

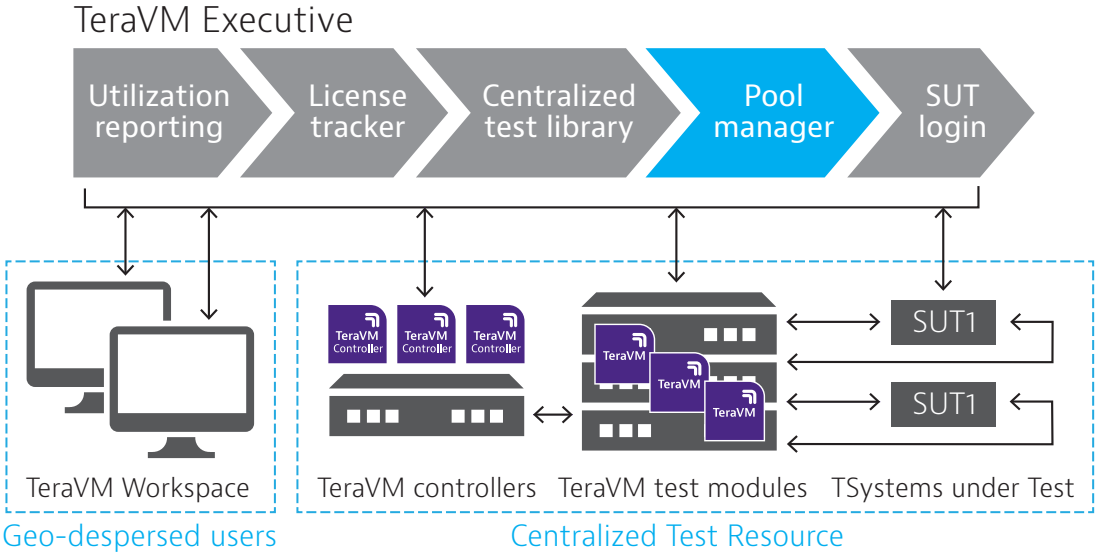
TeraVM is offered as a virtualization solution enabling the flexibility to run anywhere - lab, data center and the cloud, with consistent performance coverage, ensuring that highly optimised networks and services can be delivered with minimal risk.

The TeraVM Pool Manager provides the ability to build an elastic test bed, which optimises compute resources by sharing TeraVM test modules among multiple test beds.

TeraVM test modules are easily managed by the Pool Manager, and allocated to the controller at test run-time. This significant feature enables users to decouple the test modules from the controller.

Key Features and Benefits

- Share virtual test assets to run anywhere, anytime.
- Share test configurations, reducing test time.
- Maximise test utilisation through resource scheduling, reservations and tracking
- Create and assign a category to any interface, independent of topology.
- Easily create functional test pods and aggregate into a single high performance test bed.
- Gain real-time visibility of tests across all users.
- Reduce costs by eliminating multiple labs using proprietary test hardware.



Test Reservation

TeraVM Pool Manger provides visibility to all controllers and modules in use. Users can easily reserve, manage and dedicate TeraVM modules and view operational details, including CPU and IP address. Any TeraVM module not in use is checked regularly by the Pool Manager. If one becomes unresponsive they are highlighted for use, maximizing utilisation.

Operations

The Pool Manager acts as resource manager for TeraVM controllers and test modules. The Pool Manager runs as a service on the TeraVM Executive. TeraVM test modules are assigned by the Pool Manager to the TeraVM controller at test run time. Interface selection is based on a user-defined set of topologies and categories.

Topology Assignment

Newly registered TeraVMs are assigned into a default topology of the system under test. Users can quickly create and assign a topology name to any TeraVM module.

Category Assignment

Based on the TeraVM IP address assignment, the TeraVM modules are assigned a default category of client or server. Users can create and assign a category to any interface, independent of topology.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvmpoolmanager-br-wir-nse-ae
30187442 900 0818

VIAVI Solutions

Brochure

VIAVI

TeraVM Portable Security

Virtualized Application and Security Testing

TeraVM is an application emulation and security performance solution, delivering comprehensive test coverage for application services, wired and wireless networks. TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere – lab, datacenter and the cloud, with consistent performance coverage, ensuring that highly optimized networks and services can be delivered with minimal risk.

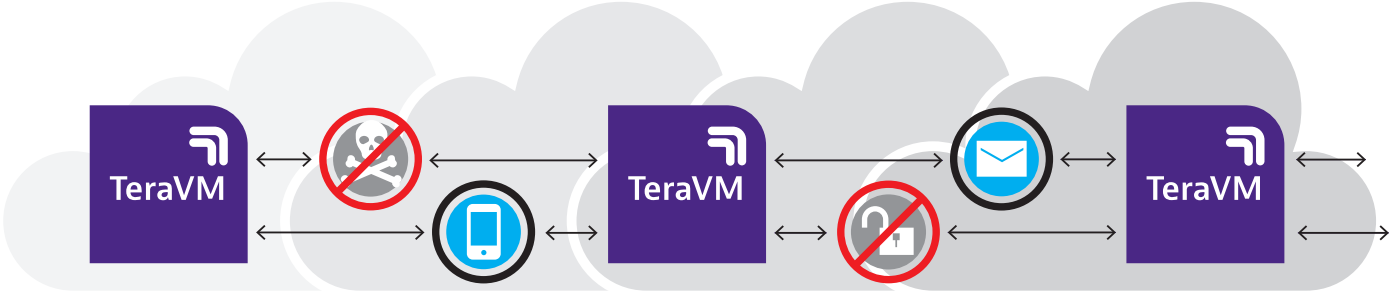
Security threats constantly evolve with new vulnerabilities discovered weekly. Attackers continue to develop new methods and attacks to find undiscovered holes in the most advanced network defenses. Application performance testing and security validation must reflect the latest and most relevant security threats to ensure network security devices will perform and protect the network infrastructure from the most advanced and malicious attacks. TeraVM provides scalable real-world application and threat emulation which leverages veritable internet threats from popular Common Vulnerability and Exposures (CVE) repositories. Frequent updates available ensure users assess their security posture in the landscape of ongoing changes for applications, attacks and standards to stay protected.

Security Hardening

By emulating the latest security threat and exploit profiles, users of TeraVM can assess security vulnerabilities in a safe and contained manner. TeraVM enables users to quickly pinpoint where the weaknesses are in their security counter measures ensuring the appliance or application is patched for any vulnerability.

Benefits

- Ensure the accuracy and validity of network device evaluations and security testing
- Continuous security intelligence with real-world applications and relevant threats
- Comprehensive library of 11,000+ CVE validated threat signatures, with frequent updates
- Realize savings from the only elastic test bed without compromising security
- Maximize security by sharing virtual test assets to run anywhere, anytime



Actionable Insight

TeraVM provides a suite of applications and security threats through a comprehensive cyber security threat database. Together they provide unique, actionable insight into threat activity, its relevance, and how to achieve a desired balance between security cost and business risk.

Performance under Duress

Determine with precision the effectiveness of security counter measures against scaled and targeted attacks. Assess what the impact is on network operations. Using TeraVM, emulate distributed denial of service attacks with known exploits.

Portability

TeraVM's application emulation and cybersecurity solution is deployed on any industry standard hardware with any major hypervisor (e.g. VMware ESXI, Hyper-V, and KVM). With TeraVM you are no longer locked in to proprietary hardware that seems to be obsolete almost the minute you receive it.

Mobility

TeraVM cybersecurity solution is packaged as a virtual appliance on standard hardware and only requires a software license to operate. For geographically dispersed testing and security validation moving a test bed across the world is as simple as checking out a license from a centrally deployed license server.

Cybersecurity Database

TeraVM Cybersecurity Database provides a comprehensive resource and service for proactively protecting and hardening the most advance networks. The TeraVM Cybersecurity Database is frequently updated as new threats are discovered and validated.

TeraVM Cybersecurity Database

See below example of recent threat updates. For a complete list of all threats, contact us.

Vulnerability	Description
Out-of bounds Vulnerability	A successful remote denial of service attack against Google Chrome before 47.0.2526.73.
Microsoft Windows Library Loading Vulnerability	A successful remote code execution attack against Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1.
Microsoft Windows Remote Code Execution Vulnerability	A successful remote code execution attack against Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1.
HTTP WordPress Plugin Vulnerability	WordPress Plugin WP Easy Poll 1.1.3 is vulnerable to a CSRF attack.
HTTP Alcatel Lucent Home Device Manager Vulnerability	Alcatel-Lucent Home Device Manager is prone to multiple cross-site scripting vulnerabilities.
HTTP D-Link DIR-645 Buffer Overflow Vulnerability	D-Link DGL5500 is vulnerable to a buffer overflow, caused by improper bounds checking by UPNP
HTTP AlegroCart 1.2.8 SQL Injection Vulnerability	Alegrocart is vulnerable to multiple SQL injection. A remote attacker could view, add, modify or delete information in the back-end database.

TeraVM Features and Functionality	
General	Real-time isolation of problem flows
	Elastic Test Bed (up to 11Tbps)
Network interface support	Support for 1/10/40Gbps I/0
	Mellanox ConnectX-4 support for 56/100Gbps
Data	TCP / UDP, Teraflow, Ookla speed test
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address assignment	Configurable MAC
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet switch	VLAN and Double VLAN Tagging (Q-Q)
	ACL, 802.1p, DSCP
Data center	VxLAN, SR-IOV
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (VoD)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure access / VPN	Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/v2), Generic remote access
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN
	Cisco ScanSafe
	Juniper Pulse, Juniper Network Connect
	Dell SSO, Fortinet Fortigate and F5
	802.1x EAP-MD5
Securiy attack mitigation	Spam / Viruses / DDoS
	Cybersecurity threat library
Voice	voIP: SIP & RTP (secure & unsecure), SMS
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	EPC and RAN (Rel.8,10,11)
	VoLTE (secure/unsecure), ViLTE
SLA	TWAMP, PING
Automation	CLI, Perl, TCL, XML, Java API
	Python, Jython
	Qualisystems (CloudShell)
	OpenStack

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvmportablesecurity-br-wir-nse-ae
30187439 900 0818

VIAVI Solutions

Brochure

VIAVI
TeraVM
Security Assertion Markup Language (SAML). Performance validation at scale

TeraVM™ supports validation for single-sign on (SSO) applications using Security Assertion Markup Language (SAML), enabling users to measure the capacity of the Identify/Service Provider by emulating millions of unique Web Browser sessions. TeraVM's stateful per-flow architecture enables users of TeraVM to validate SAML performance with unique client credentials (including the use of digital certificates), with each and every emulated client having unique SAML assertions.

TeraVM supports validation of both SAML authentication flow options:

- IdP initiated (Authenticate with IdP and follow redirect to SP service)
- SP initiated (Attempt connection to SP, follow redirect to IdP, authenticate and return to SP)

Validating SAML 2.0 authentication flows at scale

TeraVM is a stateful traffic emulator which enables users validate SAML SSO in a number of unique ways, this includes concurrent validation of both IdP and SP initiated authentication. TeraVM's per flow architecture further enhances the validation methodology by enabling unique SAML assertions per emulated client.

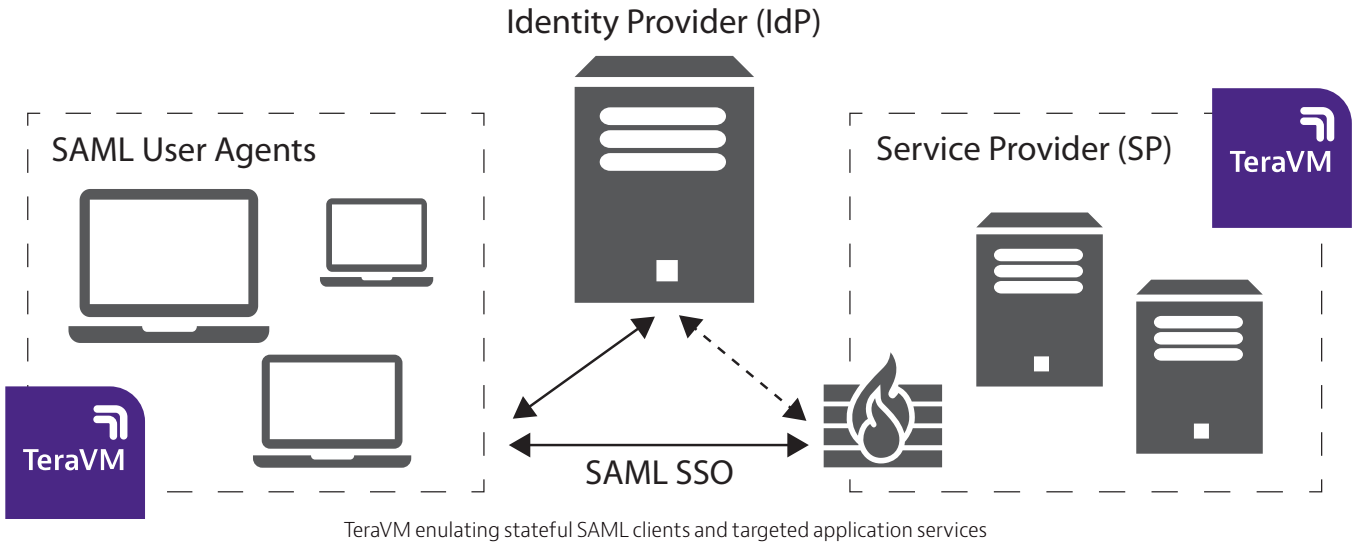
The flexible configuration options means users of TeraVM can assess the reliability of SAML with poorly configured assertions. Furthermore, the per-flow capability enables users to validate performance for more complex SAML scenarios such as realm discovery, using either unique user names, domain names, and/or url associations.

Advantages

- Emulate millions of SAML sessions
- Unique credentials per client, supports the use of digital certificates
- Supports both IdP and SP authentication flow initiation

Features

- Support of proprietary 3rd party authentication flows
- Cloud platform enabled, support for AWS, Azure, and OpenStack
- Out of millions of SAML sessions, easily pinpoint and isolate failed
- SAML sessions



TeraVM enulating stateful SAML clients and targeted application services

Introducing TeraVM

TeraVM is an application-emulation and security-performance solution, delivering comprehensive test coverage for application services, wired, and wireless networks.

TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere - lab, datacenter, and the cloud, with consistent performance coverage, ensuring that highly optimized networks and services can be delivered with minimal risk.

SAML emulation with the most realistic load scenarios

Using TeraVM SAML, users can emulate the most realistic load scenarios for performance validation of throughput, connections, and latency for single sign-on services. TeraVM supports 3rd party SAML flows which includes Citrix and F5.

TeraVM emulates stateful SAML request and responses used for validation of authentication flows originating at either the IdP or SP and/or the targeted application service. After successful authentication, TeraVM's per-flow architecture can be used to validate performance of the targeted service and can be used to validate robustness of SAML by attempting to connect to additional application services, using the assigned SAML security tokens.

TeraVM can be deployed to cloud services such as Amazon Web Services (AWS), Azure, and/or OpenStack; allowing the user validate access privileges, performance of throughput, and latency of core IdP and SP services, alongside the targeted SP application service in the cloud.

TeraVM SAML use cases

Realm Discovery

Validate performance using unique client credentials (username) and/or url requests originating at the emulated client.

SAML Assertions

Validate key SAML assertions such as lifetime of SAML tokens, validate new IdP profiles and/or malformed or with incomplete assertion values

TeraVM Capability Overview	
General	Real-time isolation of problem flows
	Elastic test bed (up to 1Tbps)
Network interface support	Support for 1/10/40Gbps I/0
	Mellanox ConnectX-4 support for 56/100Gbps

TeraVM Capability Overview	
Data	TCP / UDP, Teraflow, Ookla speed test
	HTTP (v1/2, incls. stateful response parser)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
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
Replay	Replay large PCAP files TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunneling (AMT)
	Video on Demand (VoD)
	Adaptive Bit Rate Video (HLS, HDS, MPEG-DASH, smooth)
	Video conferencing, Webex
Secure access / VPN	Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/v2), generic remote access
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN
	Cisco ScanSafe
	Juniper Pulse, Juniper Network Connect
	SAML (F5, Citrix SSO), Dell SSO
	802.1x EAP-MD5
Securiy attack mitigation	spam / viruses / DDoS
	Cybersecurity Database
Voice	VoIP: SIP & RTP (secure & unsecure), SMS
	Dual-hosted UACs, SIP Trunking
	Voice & video quality metric (MOS)
LTE/4G	EPC and RAN (Rel.8, 10, 11)
	VoLTE (secure/unsecure), ViLTE
	Wifi Offload (EoGRE)
SLA	TWAMP, PING
Automation	CLI, Perl, TCL, XML, Java API
	Python, Jython
	Qualisystems (CloudShell)
	OpenStack

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

VIAVI Solutions

Brochure

VIAVI
TeraVM
Teraflow

Run anywhere performance validation for throughput, connections and latency.

TeraVM Teraflow is used to validate key networking metrics of connections, latency and throughput with the abilty to vary bandwidth, packet and session rates, on a per emulated endpoint. The TeraVM Teraflow application supports performance testing with TCP, UDP and DTLS protocols.

A key advantage of Teraflow is the ability to assess throughput and latency performance in a back to back mode and/or against popular web based network performance validation services such as Ookla Speeedtest. TeraVM's Teraflow can emulate both client and/or Ookla equivalent servers, which supports a run anywhere performance validation capability ideal for test sceanrios such as cloud bursting to public/private clouds.

Efficient and Reliable, Run Anywhere Validation

Run Anywhere

TeraVM is delivered as an appliance and/or software only solution, making it the ideal performance validation solution for lab/public/private cloud environments. TeraVM's elastic test bed enables the user to extend their key test case scenarios beyond the lab walls to include live networks connecting with internet enabled 3rd party services and/or public/private clouds. TeraVM enables users to validate performance from inside the cloud service accessing the Ookla Speedtest service.

Advantages

- Highly scalable throughput validation: 1 Gbps to 1 Tbps
- Elastic test bed
- Support for millions of connection rate attempts
- Supports validation against Ookla Speedtest servers
- Supports both unsecure (TCP, UDP) and secure (DTLS) transport layer protocols

Features

- Throughput, Latency and Connection rate test cases
- Emulation and real-time measurement of millions of unique sessions
- Ability to vary packet rate sizes per emulated endpoint
- Per endpoint configuration for bandwidth/ connection rates and session duration
- Out of millions of sessions, easily pinpoint and isolate under-performing sessions

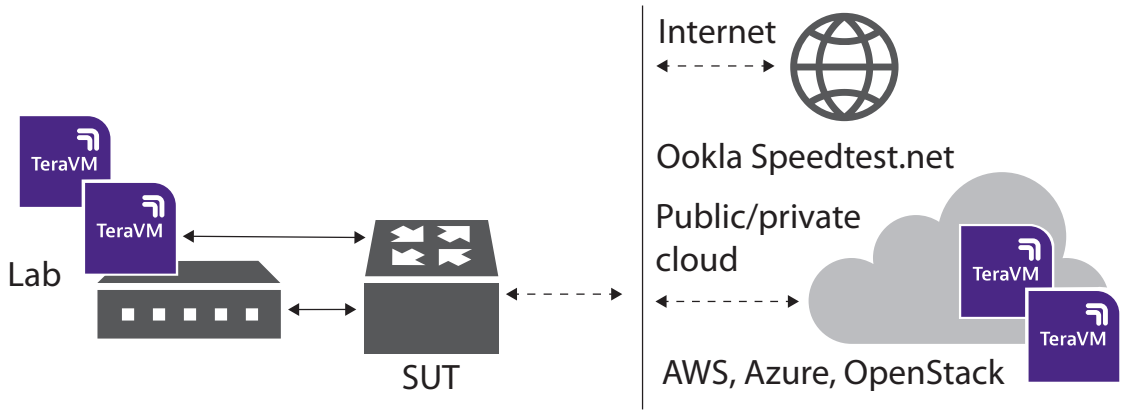


Figure 1: TeraVM Teraflow - Run anywhere throughput and latency performance validation

Ookla Speedtest

TeraVM Teraflow application allows users to emulate on a per endpoint basis, clients behaving in the same manner as the popular Ookla client. Users can elect to test against any number of geo-located Ookla servers, supporting the trio of tests: Latency, Download Bandwidth and Upload Bandwidth.

Emulation with the most realistic load scenarios

TeraVM is an application traffic emulation and security performance measurement solution. Using TeraVM Teraflow, users can emulate the most realistic load scenarios for performance validation of throughput, connections and latency.

TeraVM delivers an integrated configuration and measurement user interface for the core network tests, but also supports the popular internet based speed test service from Ookla. TeraVM enables emulation of Ookla equivalent clients which can access any of the Ookla geo-dispersed servers. TeraVM's per flow architecture enables unique configurations per emulated client endpoint, with support to emulate Ookla equivalent servers.

TeraVM can be deployed to cloud services such as Amazon Web Services (AWS), Azure and/or OpenStack; allowing the user validate throughput and latency performance in the cloud tenancy or validate against the internet based Ookla Speedtest service.

Validation with Ookla Speedtest

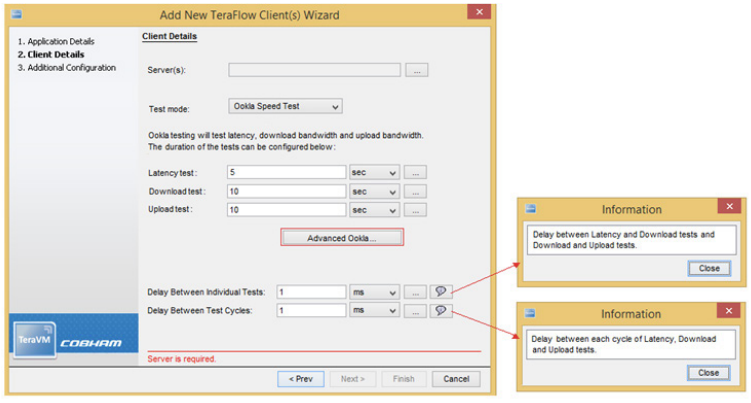


Figure 2: TeraVM GUI supports an integrated Ookla equivalent client

TeraVM features and functionality	
General	Real-time isolation of problem flows
	Elastic test bed (up to 1Tbps)
Network interface cards	Mellanox ConnectX-4 support for 56/100Gbps

TeraVM features and functionality (cont.)	
Data	TCP / UDP, Teraflow (Ookla Speedtest)
	HTTPv1/2 (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
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
Datacenter	VxLAN, GRE, SR-IOV
Replay	Replay large PCAP files TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (VoD)
	Adaptive Bit Rate Video (HLS, HDS, Smooth, MPEG-DASH)
	Video conferencing
Secure VPN	Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/v2), Generic remote access
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN
	Cisco ScanSafe
	Juniper Pulse, Juniper Network Connect
	Dell SSO
	802.1x EAP-MD5
Security attack mitigation	Spam / Viruses / DDoS
	CyberSecurity Database
Voice	VoIP: SIP & RTP (secure & unsecure), SMS
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	EPC and RAN (3GPP Rel. 8, 10, 11)
	VoLTE (secure and unsecure), ViLTE
SLA	TWAMP, PING
Automation	CLI, Perl, TCL, XML, Java API
	Python, Jython
	Qualisystems (CloudShell)
	OpenStack

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

teraflow-br-wir-nse-ae
30187497 900 0918

VIAVI Solutions

Brochure

VIAVI
TeraVM
Testing LTE/4G Evolved Packet Cores

TeraVM™ is used to emulate and analyze unique control plane and bearer sessions with mixed traffic running over bearers. TeraVM's scalability enables efficient load testing of the EPC providing insight into utilization and optimization.

LTE/4G technologies are delivering a greater convergence of voice, video and data to subscribers on the move. Convergence coupled with the subscriber's expectation for always on content, means greater speeds and throughput on a per handset basis. The challenge for service providers is how to scale the Evolved Packet Core (EPC) in order to achieve maximum equipment utilization and to optimize configurations so as to deliver the millions of unique subscriber flows with zero quality issues.

TeraVM is used for Evolved Packet Core (EPC) testing as it can efficiently and reliably scale to the level of load necessary to determine the capacity limitations of the EPC. A key reason to why TeraVM is chosen by many service providers is the ability to emulate stateful subscriber traffic on a granular basis; configure per UE, unique IMSI with multiple application traffic flow types. A significant advantage of stateful per UE emulation is the ability to isolate quickly any impairments based on EPC policy settings.

Features

- Emulate scaled subscriber traffic up to 1 Terabit per second (Tbps)
- Support for GTPv1-U and GTPv2-C
- Stateful UE emulation with configuration for unique IMSI, Bearer ID, TEID and gateway IP addresses
- Per emulated UE performance measurements, with unique performance metrics per application type IPv4 and/or IPv6 enabled traffic flows
- Multiple application types per emulated UE and GTP encapsulation
- Emulate multimedia sessions
- Support VoIP calling with AMR codecs

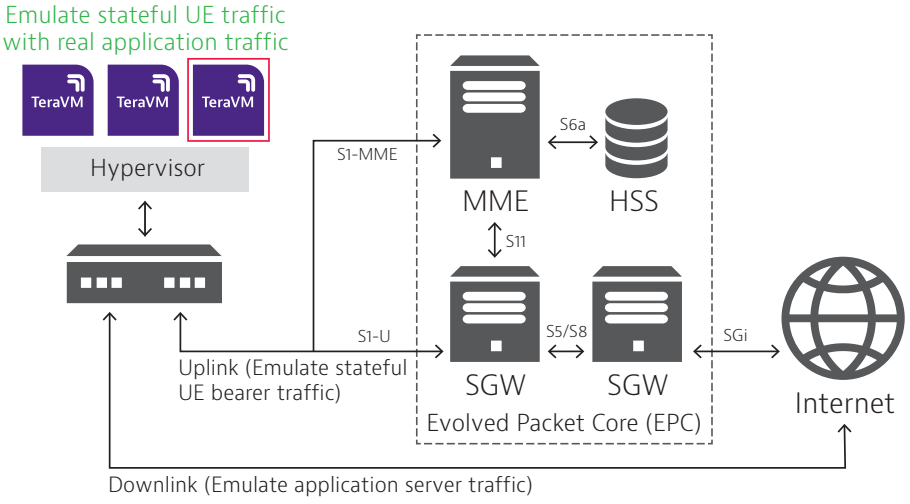


Figure 1: TeraVM testing EPC

Performance testing for the Evolved Packet Core (EPC)

TeraVM is used in two distinct ways to test the performance of the LTE EPC. The first is to generate the application traffic being encapsulated over existing GTP tunnels, in this mode TeraVM provides quality of experience analysis on a per application flow basis. The per flow granularity achieved by TeraVM is necessary to determine the impact any change or optimization of the settings of the EPC has on individual subscribers and application traffic.

A second important use of TeraVM in LTE EPC testing is the ability to load the EPC with a scaled volume of service requests, effectively emulating many enodeBs worth of traffic. TeraVM is used to emulate load conditions on both the control plane and user plane.

TeraVM enables analysis of utilization performance through load testing on all the critical paths in the EPC, which include:

- eNodeB
- MME
- S11(to S/P-GW)
- S1-U
- S11 (to S/P-GW)
- S5/S8 (to P-GW)

Functionality	
SGW/PDN GW	Emulate millions of network connection requests
	Scale test GTP tunnel capacity with millions of flows and IP packets
	Analyze heavy bandwidth usage flow profiles (users using multiple applications)
	Performance test latency with low latency dependent applications of voice and video
Application traffic (QoE testing)	Emulate multiple packet based application flows per GTP tunnel (voice, video and data)
	Test with the latest AMR codec and "OTT" multimedia services (RCS - messaging and video calling)
Device and Usage profiling	Emulate a profile of mixed traffic, emulate multiple application flows per endpoint
	Test with the latest traffic signatures, use packet replay to add the latest device and application traffic types

Comprehensive Test Capability

TeraVM provides the industry's most comprehensive test suite with over 3,000 unique metrics; ranging from application performance to protocol tunneling down to simple port enabled testing with throughput and latency metrics. A user defined threshold can be set on any of these metrics to easily pinpoint and isolate problem flows.

TeraVM provides detailed analysis on each and every emulated flow, the following highlighting some of those key metrics:

- Packets per second
- Dropped/Out of Sequence Packets
- Retransmitted Packets
- Jitter
- Latency
- TCP Connection Rate
- Application Goodput
- Unique Application timings
- Video/ Audio quality score

Features	
General	Real-time isolation of problem flows
Data	TCP / UDP, Teraflow, Ookla speed test
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address	MAC, VxLAN
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet switch	VLAN and double VLAN Tagging (Q-Q)
	ACL, 802.1p, DSCP
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (RTSP)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure VPN	SSL/TLS/DTLS, IPSec (IKEv1/v2)
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN Client
	Juniper Pulse, Juniper Network Connect
	802.1x EAP-MD5
Securiy attack mitigation	Spam / Viruses / DDoS
Voice	VoIP: SIP & RTP (secure & unsecure), H.323
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	GTP tunnel support
SLA	TWAMP
Automation	CLI, Perl, TCL, XML, Java API

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-tle4g-br-wir-nse-ae
30187451 900 0918

VIAVI Solutions

Brochure

VIAVI
TeraVM
Testing Multicast Based Video Services with TeraVM

TeraVM™ is used extensively to test the performance of video over IP services. TeraVM provides both video analysis and feature based functionality performance measurements.

Multicast enables service providers to deliver broadcast video over their IP network. However the challenge faced by many service providers is how to best manage the continued growth in video consumption while maintaining broadcast quality video. Quality of experience for video over IP is not just about video quality testing, but also includes testing the reliability of functions such as channel change. Network optimization for multicast video is a common solution for ensuring quality. However this raises the challenge of how to select the best optimization policy for the broadcast service under varying network load conditions.

Features

- Supports IGMP v1/v2/v3 and MLD v1/v2
- Emulate both multicast clients and/or servers
- Fully stateful clients that can join/leave live broadcast channels
- Channel change capacity testing
- Support for multiple video codec formats (MPEG-4, H.264, VC-1, etc)
- Configurable playout buffers that accurately emulate different viewing device types
- Video and audio quality analysis via mean opinion score (MOS)
- Integrated video quality violation notification
- Dynamic control of emulated multicast clients during live test runs
- Network load generation with a mix of voice, video, and data traffic flows

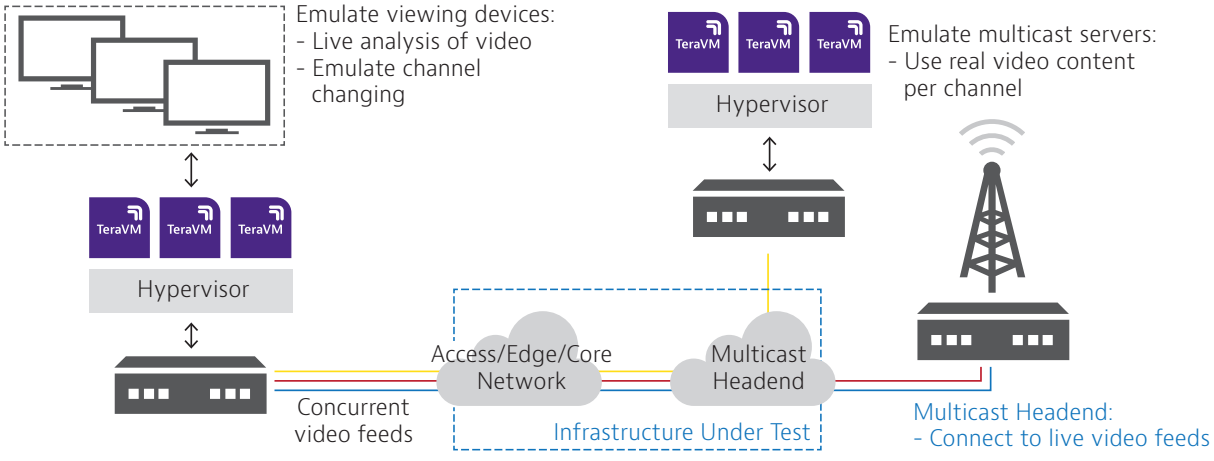


Figure 1: TeraVM testing EPC

TeraVM is the only IP video test and performance measurement solution that provides both endpoint emulation and video quality analysis with performance measurements on functionality such as channel change.

A unique aspect of TeraVM is the ability to measure performance on a per flow or per user basis. This means that for video over IP, TeraVM provides live performance analysis on all available channels in parallel.

Per flow analysis on all available multicast channels is critical to ensuring that the network and policy configuration settings have minimal impact on subscriber viewing quality or usability. Using TeraVM's multicast channel emulation, service providers can also assess the impact that introducing new channels will have on existing services.

Example Test Scenario-Service Scaling:

When a service provider introduces new video channels the existing video service must be tested to make sure there is no negative impact on quality.

With TeraVM, the service provider can emulate multicast subscribers and rate the service delivery quality to establish a baseline. After introducing the new channels, TeraVM is once again used to measure or rate the delivery quality and this can be compared to the baseline measurement to determine if the new channels have had any negative impact on service delivery.

TeraVM is used extensively to test these type of scenarios:

- Per flow measurement on a per emulated subscriber or per channel basis
- Video quality analysis via mean opinion score (MOS) to identify video quality problems
- Timing analysis to emulate channel surfing to determine impact of latency
- Determine accuracy of network policies by using TeraVM load generation

Functionality	
Stateful IGMP/MLD protocol	Concurrent testing with IGMP v1/v2/v3 & MLD v1/v2
	Support membership reports (solicited and unsolicited queries)
	Emulate multicast servers (broadcast real video streams)
Application traffic (QoE testing)	Connect to both standard definition (SD) and high definition (HD) channels
	Configurable buffer sizes to emulate different viewing devices
	Implement channel surfing (joins/leaves) with defined viewing durations
Device and Usage profiling	Media performance of standard definition (SD) and high definition (HD) video streams
	No reference analysis for both video and audio streams (MOS)
	TR 101 290 standard measurements (decodability of elementary video streams)

Features	
General	Real-time isolation of problem flows
Data	TCP / UDP, Teraflow, Ookla speed test
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address	MAC, VxLAN
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet switch	VLAN and double VLAN Tagging (Q-Q)
	ACL, 802.1p, DSCP
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (RTSP)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure VPN	SSL/TLS/DTLS, IPSec (IKEv1/v2)
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN Client
	Juniper Pulse, Juniper Network Connect
	802.1x EAP-MD5
Securiy attack mitigation	Spam / Viruses / DDoS
Voice	VoIP: SIP & RTP (secure & unsecure), H.323
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	GTP tunnel support
SLA	TWAMP
Automation	CLI, Perl, TCL, XML, Java API

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

multicastvideo-br-wir-nse-ae
30187454 900 0918

VIAVI Solutions

Brochure

VIAVI

User Centered Interface Design

Delivering ease of use and collaboration TeraVM 12.0

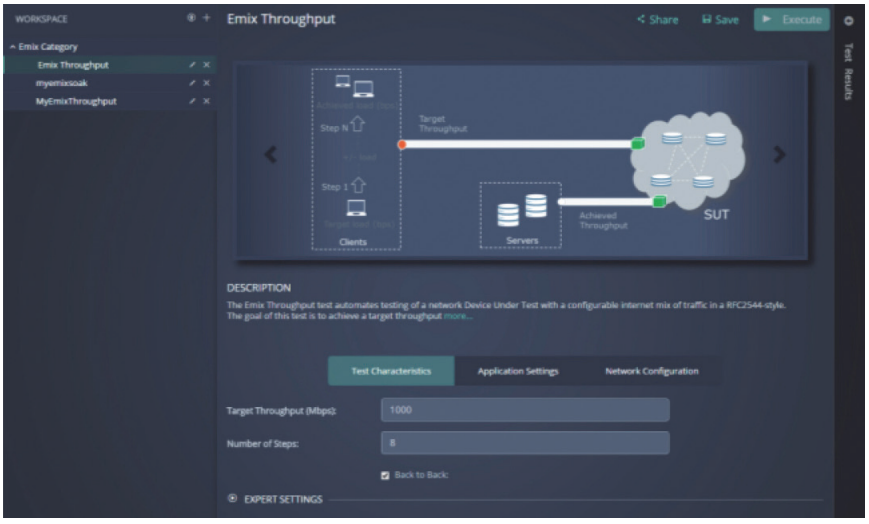
TeraVM™ is an application emulation and security validation solution, delivering comprehensive test coverage for application services, wired and wireless networks.

TeraVM is an application emulation and security validation solution, delivering comprehensive test coverage for application services, wired and wireless networks. TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere - lab, data center and the cloud, with consistent performance coverage, ensuring that highly optimized networks and services can be delivered with minimal risk.

TeravM 12.0 release introduces a HTML5 user interface, and a Centralized Test Library, where many users and TeraVM controllers can easily share and run test cases via an intuitive push button user interface. The centralized library offers a collaborative framework where users can take advantage of TeraVM supplied proven tests or create and share their own test scenarios via a central server.

Key Features and Benefits

- Template driven for enhanced user experience
- Authenticated access to a HTML5 user interface
- Access tests from a centralized test library
- Professional real-time graphing with thresholds
- Multiple user defined metrics per graph
- Easily save data and test results
- Share tests cases to the centralized library



TeraVM HTML5 UI

The TeraVM HTML5 user interface enables up to ten real-time charts, each containing up to ten unique metrics. A significant enhancement is the ability to see event notifications based on threshold crossing events in each of the charts. Test cases created in the user interface are cross-compatible with, and can be viewed and managed in the TeraVM Java Client. The Java Client continues to be available for running tests at a host/application level.

Test Results in the UI

Test Results in the UI

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

usercenter-interfacedesign-br-wir-nse-ae
30187441 900 0818

VIAVI Solutions

Brochure

VIAVI
TeraVM

Voice, Video and MPEG Transport Stream Quality Metrics

The ITU-T published J.144, a measurement of quality of service, for the transmission of television and other multimedia digital signals over cable networks. This defines the relationship between subjective assessment of video by a person and objective measurements taken from the network.

The correlation between the two are defined by two methods:

- Full Reference (Active) – A method applicable when the full reference video signal is available, and compared with the degraded signal as it passes through the network.
- No Reference (Passive) – A method applicable when no reference video signal or information is available.

VIAVI believes that a combination of both Active and Passive measurements gives the correct blend of analysis with a good trade off of accuracy and computational power. TeraVM provides both voice and video quality assessment metrics, active and passive, based on ITU-T's J.144, but are extended to support IP networks.

For active assessment of VoIP and video, both the source and degraded signals are reconstituted from ingress and egress IP streams that are transmitted across the Network Under Test (NUT).

The VoIP and video signals are aligned and each source and degraded frame is compared to rate the video quality.

For passive measurements, only the degraded signal is considered, and with specified parameters about the source (CODEC, bit-rate) a metric is produced in real-time to rate the video quality.

This combination of metrics gives the possibility of a 'passive' but lightweight Mean Opinion Score (MOS) per-subscriber for voice and video traffic, that is correlated with CPU-expensive but highly-accurate 'active' MOS scores.

Both methods provide different degrees of measurement accuracy, expressed in terms of correlation with subjective assessment results. However, the trade off is the considerable computation resources required for active assessment of video - the algorithm must decode the IP stream and reconstitute the video sequence frame by frame, and compare the input and outputnframes to determine its score. The passive method is less accurate, but requires less computing resources.

Active Video Analysis

The active video assessment metric is called PEVQ – Perceptual Evaluation of Video Quality. PEVQ provides MOS estimates of the video quality degradation occurring through a network by

analysing the degraded video signal output from the network. This approach is based on modelling the behaviour of the human visual tract and detecting abnormalities in the video signal quantified by a variety of KPIs. The MOS value reported, lies within a range from 1 (bad) to 5 (excellent) and is based on a multitude of perceptually motivated parameters.

To get readings from the network under test, the user runs a test with an video server (TeraVM or other) and an IGMP client, that joins the stream for a long period of time. The user selects the option to analysis the video quality, which takes a capture from both ingress and egress test ports.

Next, the user launches the TeraVM Video Analysis Server, which fetches the video files from the server, filters the traffic on the desired video channel and converts them into standard video files. The PEVQ algorithm is run and is divided up into four separate blocks.

The first block – pre-processing stage – is responsible for the spatial and temporal alignment of the reference and the impaired signal. This process makes sure, that only those frames are compared to each other that also correspond to each other.

The second block calculates the perceptual difference of the aligned signals. Perceptual means that only those differences are taken into account which are actually perceived by a human viewer. Furthermore the activity of the motion in the reference signal provides another indicator representing the temporal information. This indicator is important as it takes into account that in frame series with low activity the perception of details is much higher than in frame series with quick motion.

The third block in the figure classifies the previously calculated indicators and detects certain types of distortions.

Finally, in the fourth block all the appropriate indicators according to the detected distortions are aggregated, forming the final result – the mean opinion score (MOS). TeraVM evaluates the quality of CIF and QCIF video formats based on perceptual measurement, reliably, objectively and fast.

In addition to MOS, the algorithm reports:

- **Distortion indicators:** For a more detailed analysis the perceptual level of distortion in the luminance, chrominance and temporal domain are provided.
- **Delay:** The delay of each frame of the test signal related to the reference signal.
- **Brightness:** The brightness of the reference and degraded signal.
- **Contrast:** The contrast of the distorted and the reference sequence.
- **PSNR:** To allow for a coarse analysis of the distortions in different domains the PSNR is provided for the Y (luminance), Cb and Cr (chrominance) components separately.
- **Other KPIs:** KPIs like Blockiness (S), Jerkiness, Blurriness (S), and frame rate the complete picture of the quality estimate.

Passive MOS and MPEG Statistics

The VQM passive algorithm is integrated into TeraVM, and when required produces a VQM, an estimation of the subjective quality of the video, every second. VQM MOS scores are available as an additional statistic in the TeraVM GUI and available in real time. In addition to VQM MOS scores, MPEG streams are analysed to determine the quality of each "Packet Elementary Stream" and exports key metrics such as Packets received and Packets Lost for each distinct Video stream within the MPEG Transport Stream. All major VoIP and Video CODECs are support, including MPEG 2/4 and the H.261/3/3+/4.

Voice over IP call quality can be affected by packet loss, discards due to jitter, delay, echo and other problems. Some of these problems, notably packet loss and jitter, are time varying in nature as they are usually caused by congestion on the IP path. This can result in situations where call quality varies during the call - when viewed from the perspective of "average" impairments then the call may appear fine although it may have sounded severely impaired to the listener. TeraVM inspects every RTP packet header, estimating delay variation and emulating the behavior of a fixed or adaptive jitter buffer to determine which packets are lost or discarded. A 4- state Markov Model measures the distribution of the lost and discarded packets. Packet metrics obtained from the Jitter Buffer together with video codec information obtained from the packet stream to calculate a rich set of metrics, performance and diagnostic information. Video quality scores provide a guide to the quality of the video delivered to the user. TeraVM V3.1 produces call quality metrics, including listening and conversational quality scores, and detailed information on the severity and distribution of packet loss and discards (due to jitter). This metric is based on the well established ITU G.107 E Model, with extensions to support time varying network impairments.

For passive VoIP analysis, TeraVM v3.1 emulates a VoIP Jitter Buffer Emulator and with a statistical Markov Model accepts RTP header information from the VoIP stream, detects lost packets and predicts which packets would be discarded – feeding this information to the Markov Model and hence to the TeraVM analysis engine.

PESQ Support

Finally, PESQ is available for the analysis of VoIP RTP Streams. The process to generate PESQ is an identical process to that of Video Quality Analysis.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contacts.

tvm-vv-mpeg-br-wir-nse-ae
30191143 900 0620

VIAVI Solutions

Brochure

VIAVI
TeraVM
Testing Telepresence with TeraVM

TeraVM™ emulates stateful Telepresence endpoints, which are used to assess a network's suitability to host collaborative meetings and also to determine the meeting capacity limitations.

Telepresence is a widely deployed technology which uses a rich video, audio and data experience to improve collaboration between online meeting participants in geographically dispersed locations. The challenge faced when preparing to deploy Telepresence is how to accurately assess the performance of the underlying network to host collaborative meetings from a number of remote sites. A further complexity is how to accurately measure performance and functionality without deploying expensive hardware or large numbers of soft clients to each site.

TeraVM is chosen by service providers and network equipment manufacturers to test Telepresence meeting places because it's a virtual solution which can be easily deployed and distributed. A further benefit of TeraVM is the ability to emulate the leading vendor's Telepresence endpoints which include room encoders and/or software based PC clients. As an integrated solution TeraVM provides detailed performance analysis on the control signaling and the media, which includes analysis of each and every video and audio stream associated with the meeting. TeraVM is used to join live or scheduled meetings in which TeraVM impersonates the speaker, enabling analysis of Telepresence voice detection functionality. Other meeting functionality which can be assessed using TeraVM includes call hold and call mute.

Features

- Emulate 3rd party Telepresence endpoints: Cisco CTS series, Cisco Movi, Cisco Jabber, Tandberg E, EX, C series
- Supports TIP (Telepresence Interoperability Protocol)
- Participate in actual live meetings
- Impersonate a live speaker with varied speaker loudness
- Test call functions (e.g. call mute and call hold) live during the meeting
- Input auxiliary feeds such as presentation files per emulated meeting participant
- Register with 3rd party meeting and scheduling servers
- Configure call media per endpoint: frame rate, bitrate, audio codec
- Video and audio quality analysis per emulated meeting participant
- Dynamic call control during live tests on a per emulated participant basis

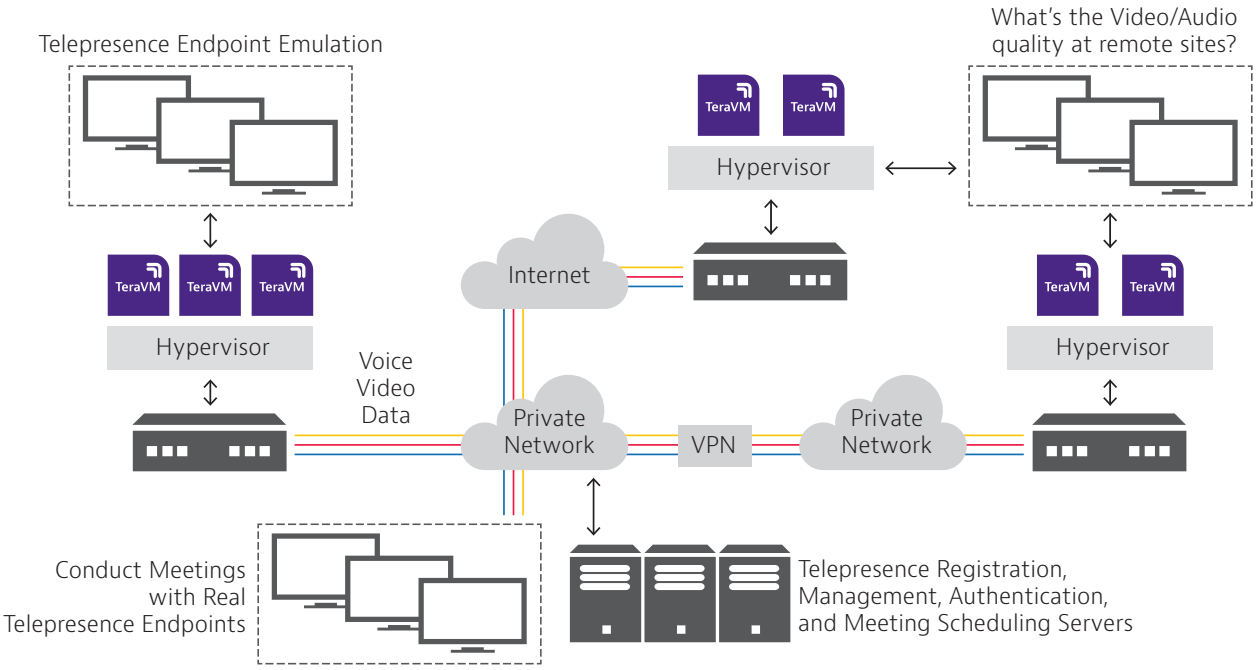


Figure 1: Example TeraVM deployment

Example Test Scenario

If a service provider is rolling out a "walk in" Telepresence service, in order to scale the service the provider must be able to quickly test and select locations that have the optimum network performance required for high quality Telepresence meetings. TeraVM is an ideal solution to test and select service locations because of the following attributes:

- Virtual solution: no transportation of physical equipment, same day roll-out and test
- Endpoint variation: test Telepresence hardware and/or software clients (e.g. Jabber)
- Concurrent site testing: test a number of remote sites concurrently in real time
- Content assessment: test with standard definition and high definition (HD) content
- Meeting control/management: assess access to the centralized servers

Functionality	
TeraVM Telepresence	Emulate 3rd party Telepresence endpoints (encoder and/or soft clients)
	Interoperate with 3rd party management systems: registration, scheduling, authentication and management servers
	Supports Telepresence Interoperability Protocol (TIP)
Analysis per endpoint	Analysis on each and every media stream on a per emulated endpoint or per meeting basis
	Analysis of both the signaling and media flows
	Subjective quality scoring or Mean Opinion Scores (MOS) for both video and audio streams
Meeting room functionality	Test call hold and call mute functionality
	Test voice detection and floor control, impersonate speakers with varied loudness
	Test auxiliary services including file sharing

For telepresence TeraVM measures over 50 metrics. Below are a few example metrics:

- QMVIdeo MOS
- QMAudio MOS
- RTP Video Frame Jitter
- Buffer Overrun/Underrun
- Call Time Ringing
- Time to First Media FrameOut of Sequence packets
- Endpoint Registration Success
- SIP Control Message Rates
- RTCP Packet Rates

Features	
General	Real-time isolation of problem flows
Data	TCP / UDP
	HTTP (headers, substitution, attachments)
	SMTP / POP3 (incl. file attachments)
	FTP (Passive/Active), P2P applications, DNS
Address	MAC, VxLAN
	DHCP, PPPoE (IPv4 & IPv6)
	Dual Stack (6RD, DS Lite)
Ethernet switch	VLAN and double VLAN Tagging (Q-Q)
	ACL, 802.1p, DSCP
Replay	Replay large PCAP files - TCP, UDP and raw data playback
	Amplify and dynamically substitute data into PCAP files
Video	Multicast: IGMP v1/v2/v3 & MLD v1/v2
	Automatic Multicast Tunelling (AMT)
	Video on Demand (RTSP)
	Adaptive Bit Rate Video (HLS, HDS, Smooth)
	Video conferencing
Secure VPN	SSL/TLS/DTLS, IPSec (IKE v1/v2)
	Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN Client
	Juniper Pulse, Juniper Network Connect
	802.1x EAP-MD5
Securiy attack mitigation	Spam / Viruses / DDoS
Voice	VoIP: SIP & RTP (secure & unsecure), H.323
	Dual Hosted UACs, SIP Trunking
	Voice & Video quality metric (MOS)
LTE/4G	GTP tunnel support
SLA	TWAMP
Automation	CLI, Perl, TCL, XML, Java API

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-telepresence-br-wir-nse-ae
30187452 900 0918