VIAVI
NetSecOPEN™ on TeraVM™

With our market leading, fully virtualized security test tool TeraVM, VIAVI delivers the full suite of NetSecOPEN test cases.

What is TeraVM?

TeraVM is a software based L2-7 test tool running on off the shelf hardware & in the Cloud (Amazon AWS, Azure, Google Cloud, Oracle OCI etc.) to test security devices, networks and services at scale.

What is NetSecOPEN?

NetSecOpen is a non-profit, membership driven organization that provides open and transparent testing standards for Network Security Device Performance. NetSecOpen defines a suite of standards that can be used for the evaluation and/or certification of network security protocols.

NetSecOpen Compliant Test Suite

In the market leading easy to use web GUI, TeraVM delivered NetSecOPEN compliant test cases following these criteria:

• Page Size: various page sizes were defined

• IPV4 and IPv6 Hosts: hosts that use IPv4 or IPv6

• Traffic Flow: TCP connection, preform 10 HTTP GET transactions of different page sizes

• Test Phases: default values for test phases are defined.

NetSec⊘PEN

NetSecOPEN Test Case List

HTTP Throughput Test – measure throughput of HTTP transactions varying the HTTP response object size

HTPP CC – determine the maximum number of concurrent TCP connections that he DUT sustains when using HTTP traffic

HTTP CPS – using HTTP traffic determine the maximum sustainable TCP connection establishment rate supported by the DUT for different load conditions

HTTP Transaction Latency - using HTTP traffic determine the average transaction latency of the DUT

HTTPS Throughput Test - measure throughput of HTTPS transactions varying the HTTPS response object size

HTTPS CC - determine the maximum number of concurrent TCP connections that he DUT sustains when using HTTPS traffic

HTTPS CPS – using HTTPS traffic determine the maximum sustainable TCP connection establishment rate supported by the DUT for different load conditions
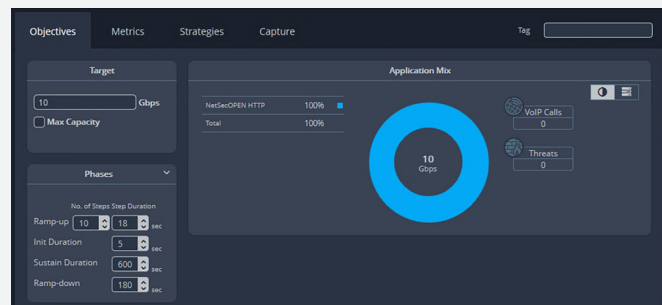
HTTPS Transaction Latency – using HTTPS traffic determine the average transaction latency of the DUT

NetSecOPEN Traffic Mix – using NetSecOPEN traffic mix determine the maximum sustainable throughput performance supported by the DUT

Note: there are 20+ additional variants of these 9 tests.

Watch video of the TeraVM web GUI at:
https://bcove.video/31BXNAi

Web UI – screenshot

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 1/10/40/100 GE ports

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 Multiple streams/Multiplexing support

- SMTP / POP3 (incl. file attachments)

- FTP (Passive/Active), P2P applications, DNS

- FTP client session count limit

- DNS client (with HTTP/S applications) incl. host name into 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 sub data into PCAP

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 with EVS (Enhanced Voice Services)

- VoIP client scaling with auto generated unique AKA authentication 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), Generic remote access

- VPN clients: Cisco AnyConnect, Fortinet, Juniper Pulse, Juniper Network Connect, 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 publicIP address assigned to TeraVM in publiccloud environments

- PPTP VPN Client & Server supported

Security

- 40,000+ Malware attacks & CyberSecuritythreats, 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

- Good and Bad mixed traffic flows

- Statefully scale Cisco specific threats

- Ability to use 3rd party threat libraries

- Ability to turn on /off Extended MasterSecret (RFC 7627) support flag to test CiscoFTD, ASA and other security solutions

- Support for TLS1.3, TLS1.2 simultaneously on Client & Server

- TLS SNI Support incl. unique certificate perFQDN

SLA Monitoring

- TWAMP-RFC 5357, PING

- 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 @ 1,000s of RANs

- Core Emulation:

  - 5G (NSA & SA), 4G-LTE, 3G, 2G with Mobility @ 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

- Oracle OCI

- Containerized TeraVM (docker)

Hypervisors

- VMware ESXi

- KVM Ubuntu

- Amazon AWS

- Microsoft Azure

- KVM Redhat

- Openstack

Specific Test Coverage

TeraVM includes Cisco 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 802.1X

Client

- Cisco AnyConnect ECDSA, EdDSA Cert authentication

- Cisco Umbrella

- Captive Portal testing

- Cisco TelePresence

- Cisco Video Clients

- Cisco WebEx

- Cisco Phones

- Mobile phones for Security Gateway

- IoT Device