TeraVM Security

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

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
PCAPNG format support for troubleshooting TLS flows
Same test profile can be used for multiple platforms
Faster setup, faster testing, faster results
Distributed multi-cloud deployment support

Network Interface Support

Support for 1/10/40/100 Gbps I/O

Data

Jumbo Frame support with max MTU/Segment configurable
TeraFlowUDP Out-of-Sequence Statistics, reverse flow support
Latency/TCP RTT distribution view with bucket configuration
TeraFlow TCP/UDP, Ookla Speed Test, VR/Gaming (with Burst Profile)
CCDF plotting of TWAMP One Way Delay metric and per packet latency reporting
HTTP, HTTPS, HTTP 2.0 ALPN, HTTP/3, HTTP over QUIC (per stream bitrate control and statistics)
HTTP with SAML 2.0 authentication (IdP emulation)
HTTP websocket emulation
HTTPS Client with SAML 2.0 Auth |Explicit Proxy-SWG validation
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 Client with UDP/TCP/TLS(DoT) and HTTP(DoH) with support for 1 milllion user supplied DNS queries using random ports
DNS server emulation with configurable domain name mappings
Post Quantum Cryptography for TLS - HTTPS with PQC KEMs
SaaS Application Profiles

Address Assignment

Configurable MAC
DHCP, PPPoE (IPv4 and IPv6)
Dual Stack (6RD, DS Lite)

Ethernet Switch

VLAN Tagging (up to 8 concurrent tags)
ACL, 802.1p, DSCP
Enable path MTU discovery

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 and stateful TCP Replay: Ability to dynamically change content
Replay large PCAP files: TCP, UDP and raw data playback
IP Replay (w/ DHCP): multiple TCP/UDP streams
Amplify and dynamically substitute data into PCAP files

Video

CMTS, CDN, Multicast: IGMP v1/v2/v3 and 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
H.265 codec support

Voice

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

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 and 32)), Generic remote access, CSFR support

802.1x EAP-MD5, EAP and PEAP with MS CHAPv2 Authentication

RADIUS client EAP-TLS/EAP-FAST support with configurable custom AVPs

802.1X Accounting Start and Stop Records

Scalable Site to Site VPN - IPV6/V4

Additional security to limit access to public IP address assigned to TeraVM in public cloud environments

IKE/IPSec VPN with PPK (RFC8784)

IKE/IPSec VPN with Post Quantum Preshared Key (PPK)(RFC8784)

IKE/IPSec VPN with Post Quantum Cryptography (PQC)KEMS | RFC9370 RFC9242

HTTPS SAML Authentication - Zero Trust Network validation at Scale

PPTP VPN Client and Server supported

Cisco AnyConnect SSL and Cisco AnyConnect IPsec VPN Clients

Cisco Umbrella SWG, session resumption

Cisco AnyConnect for Secure Firewall Cloud Native (SFCN)

Cisco AnyConnect SAML 2.0 authentication, SSO, AD based login

Cisco AnyConnect for VTK, Meraki with SAML

Cisco AnyConnect STRAP (Session Token Re-Use Anchor Protocol)

Cisco Umbrella Chromebook Client emulation

Cisco AnyConnect SSL and IKE certificate based authentication with multiple user provided ECDSA EdDSA certificates

Cisco Secure Access Client with MASQUE

Cisco Secure Access Client - Hybrid ZTNA

PaloAlto GlobalProtect VPN client emulation

Security

65,000+ Malware attacks and Cybersecurity threats, updated monthly

Spam / Viruses / DDoS / Malware

Malware Application Profiles

TCP CUBIC congestion control

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 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

Chained certificates for HTTP server

SLA Monitoring

TWAMP-RFC 5357, PING-RFC 792

Cisco Netflow Records/Exporter emulation at scale

Internet of Things (IoT)

Client emulation

CoAP-RFC 7252

NIDD over SCEF, S11-U, S1-U

SCEF Emulation Including Protocol Relay

Cloud Platform Support

Amazon AWS

Google Cloud (GCP)

Oracle Cloud (OCI)

Microsoft Azure

Alibaba Cloud

Hypervisors

VMware ESXi

KVM Ubuntu

KVM Redhat

Openstack

Kubernetes Cloud Platforms (Containerized TeraVM)

Google GKE

Amazon EKS

NetSecOPEN Tests

NetSecOPEN Test Suite