

# TeraVM Security

TeraVM Security 是一个基于软件的 L2-7 测试工具，运行在标准 x86 服务器和云（Amazon、Azure、Openstack 等）中，提供完全虚拟化的应用仿真和安全验证解决方案，用于测试和保护设备、网络及其服务。

## 应用支持

<b>常规</b>	<b>数据中心</b>
系统利用率报告（位置、用户、测试平台、使用中的许可证、使用统计信息）	VxLAN、GRE、SR-IOV
许可证签入默认计时器	<b>自动化</b>
自适应引擎 - 动态自动查找被测设备的最大容量	REST、CLI、Perl、TCL、XML、Java API
用于 TLS 流故障排查的 PCAPNG 格式支持	Python、Jython
相同测试配置文件可用于多个平台	Cisco LaasNG、Qualisystems (CloudShell)、Luxoft 软件定义实验室 (SDL)、Openstack、Cisco pyATS
更快设置、更快测试、更快获得结果	<b>重放应用程序存储库</b>
分布式多云部署支持	智能 UDP 和有状态 TCP 重放：能够动态更改内容
<b>网络接口支持</b>	重放大型 PCAP 文件：TCP、UDP 和原始数据回放
支持 1/10/40/100 Gbps I/O	IP 重放（带 DHCP）：多个 TCP/UDP 流
<b>数据</b>	将数据放大并动态替换到 PCAP 文件中
支持巨型帧，最大 MTU/段可配置	<b>视频</b>
TeraFlowUDP 乱序统计，反向流支持	CMTS、CDN、组播：IGMP v1/v2/v3 和 MLD v1/v2
具有存储桶配置的延迟/TCP RTT 分布视图	自动组播隧道 (AMT)
TeraFlow TCP/UDP、Ookla 速度测试、虚拟现实/游戏（带突发模式）	视频点播 (VoD)
TWAMP 单向延迟度量和每个分组延迟报告的 CCDF 绘图	自适应比特率 (HLS、HDS、MPEG-DASH、SMOOTH)
HTTP、HTTPS、HTTP 2.0 ALPN、HTTP/3、HTTP over QUIC（每流比特率控制和统计）	视频会议、WebEx、网真
使用 SAML 2.0 身份验证的 HTTP (IdP 仿真)	基于 HTTP 的视频
HTTP websocket 仿真	支持 H.265 编解码器
具有 SAML 2.0 Auth 的 HTTPS 客户端   显式代理 SWG 验证	<b>语音</b>
SMTP/POP3（包括文件附件）	在 HTML5 UI 中保护 VoIP 和 WebEx 通话
FTP（被动/主动）、P2P 应用程序、DNS	双栈 VoIP 网关仿真
FTP 客户端会话计数限制	Cisco CUCM、CUBE
DNS 客户端（带有 HTTP/S 应用程序，包括 IP 地址解析）	VoIP：SIP 和 RTP（安全和非安全），SMS
具有 UDP/TCP/TLS(DoT) 和 HTTP(DoH) 的 DNS 客户端，使用随机端口支持 100 万个用户 DNS 查询	VoIP 客户端扩展，自动生成唯一的
具有可配置域名映射的 DNS 服务器仿真	采用 EVS（增强型语音服务）的 VoIP
用于 TLS 的后量子加密 - 使用 PQC ML-KEM 的 HTTPS (FIPS-203)	每个客户端的 AKA 身份验证请求
SaaS 应用程序配置文件	VoLTE 紧急呼叫支持
<b>地址分配</b>	双托管 UAC、SIP 中继
可配置 MAC	语音和视频质量指标（同时支持 MOS）
DHCP、PPPoE (IPv4 和 IPv6)	EVS 编解码器支持，各种比特率，静音抑制
双栈 (6RD, DS Lite)	G.711 支持 SID-RFC3889
<b>以太网交换机</b>	IMS 的 SIP 更新，包括 PANI 信息
VLAN 标记（最多 8 个并发标记）	MCPTT 组呼叫（包括 KPI 支持）
ACL、802.1p、DSCP	MCPTT 客户端和应用程序服务器仿真
启用路径 MTU 发现	

<b>安全访问/VPN</b>
SSLv2/3、TLSv1.0/1/2/3 和 DTLSv1.0/2
TLS 客户端密码套件选择
AnyConnect VPN 客户端的动态 IPv6 分配
无客户端 VPN (SSL/TLS/DTLS)、IPSec (IKEv1/v2 (DH 组 31 和 32))、通用远程访问、CSFR 支持
802.1x EAP-MD5、EAP 和 PEAP, 带 MS CHAPv2 身份验证
RADIUS 客户端 EAP-TLS/EAP-FAST 支持可配置的自定义 AVP
802.1X 记帐开始和停止记录
可扩展站点到站点 VPN - IPv6/V4
在公共云环境中限制对分配给 TeraVM 的公共 IP 地址的访问, 提供额外安全性
带 PPK 的 IKE/IPSec VPN (RFC8784)
具有后量子预共享密钥 (PPK) 的 IKE/IPSec VPN (RFC8784)
使用后量子加密 (PQC) 的 IKE/IPSec VPN ML-KEM FIPS-203 RFC9370 RFC9242
HTTPS SAML 身份验证 - 大规模零信任网络验证
支持 PPTP VPN 客户端和服务端
Cisco AnyConnect SSL 和 Cisco AnyConnect IPSec VPN 客户端
Cisco Umbrella SWG, 会话恢复
Cisco AnyConnect for Secure Firewall Cloud Native (SFCN)
Cisco AnyConnect SAML 2.0 身份验证、SSO、基于 AD 的登录
Cisco AnyConnect for VTK, 带有 SAML 的 Meraki
Cisco AnyConnect STRAP (会话令牌重用锚定协议)
Cisco Umbrella Chromebook 客户端仿真
Cisco AnyConnect - 通过 IKE_SA_INIT 传递 FQDN/SNI
Cisco AnyConnect 基于 SSL 和 IKE 证书的身份验证, 由多个用户提供 ECDSA 和 EDDSA 证书
带有 MASQUE 的 Cisco Secure Access 客户端
Cisco Secure Access Client - 通用 ZTNA
PaloAlto GlobalProtect VPN 客户端仿真
带有 PQC ML-KEM 密码的 Cisco AnyConnect
OKD 密钥管理系统测试
<b>安全性</b>
超过 65000 个恶意软件攻击和网络安全威胁样本, 每月更新
垃圾邮件/病毒/DDoS/恶意软件
恶意软件应用程序配置文件
TCP CUBIC 拥塞控制
L4S - TCP Prague 拥塞控制



北京 电话: +8610 6539 1166  
 上海 电话: +8621 6859 5260  
 上海 电话: +8621 2028 3588  
 (仅限 TeraVM 及 TM-500 产品查询)

深圳 网站:

DDoS 攻击应用:
<ul style="list-style-type: none"> <li>洪水: SYN、反射 SYN、复位、UDP、PING、ARP</li> <li>攻击: TearDrop; UDP 分片; 可配置速率, 开始和停止</li> <li>欺骗 Mac 寻址</li> </ul>
好坏混合流量流
有状态地扩展 Cisco 特定威胁
能够使用第三方威胁库
能够打开/关闭扩展主密钥 (RFC 7627) 支持标志, 以测试 Cisco FTD、ASA 和其他安全解决方案
在客户端和服务端上同时支持 TLS 1.3 和 TLS 1.2
可配置的 TLS 记录大小
TCP 延迟确认 (基于计时器)
HTTP 严格传输安全 (HSTS) 标头支持
TLS SNI 支持, 包括每个 FQDN 的唯一证书
HTTP 服务器的链式证书
<b>SLA 监控</b>
TWAMP-RFC 5357, PING-RFC 792
Cisco NetFlow 大规模记录/导出器仿真
<b>物联网 (IoT)</b>
客户端仿真
CoAP-RFC 7252
NIDD over SCEF、S11-U、S1-U
包括协议中继的 SCEF 仿真
<b>云平台支持</b>
Amazon AWS
Google Cloud (GCP)
Oracle Cloud (OCI)
Microsoft Azure
Alibaba Cloud
<b>虚拟机管理程序</b>
VMware ESXi
KVM Ubuntu
KVM Redhat
Openstack
<b>Kubernetes 云平台 (容器化 TeraVM)</b>
Google GKE
Amazon EKS
<b>NetSecOPEN 测试</b>
NetSecOPEN 测试套件

电话: +86 755 8869 6800  
 www.viavisolutions.cn