SHENICK SOLUTION BRIEF

SSL/TLS/DTLS VPN client emulation with TeraVM

OVERVIEW

TeraVM is used for performance testing the leading VPN appliances as it emulates stateful SSL/TLS/DTLS VPN clients encapsulating real application traffic, enabling performance measurements on both the VPN tunnel and the application traffic inside the tunnel.

FEATURES

- ✓ Test VPN appliances from the leading vendors: Cisco, Fortinet or Juniper
- ✓ Test multiple VPN appliance types concurrently
- ✓ Unique authentication detail (username, password or certificate) per emulated VPN client
- ✓ Unique tunnel duration and re-connection delay per VPN client
- ✓ Support mixed tunnel encapsulation of IPv4 and/or IPv6 enabled flows
- ✓ Dedicated VPN performance metrics
- ✓ Performance analysis on each of the encrypted application flows

SHENICK

www.shenick.com

A key challenge faced by all computer network administrators is to select the correct VPN appliance for the specific user environment and applications being secured. Network administrators are under pressure to implement the highest level of security whilst maintaining the performance of the user connectivity and the applications being secured. In addition, network administrators are required to do this using theoretical analysis of the VPN appliance brochure.

TeraVM is the only IP test solution which offers testing of all the leading VPN appliances. Network administrators use TeraVM to verify the performance and the scalability of the VPN appliance. In addition, network administrators are using TeraVM to understand how the various VPN appliance settings impact the performance of the applications being secured. Network administrators no longer rely on theoretical results and are adopting a pragmatic approach to ensuring the highest levels of security are achieved, by testing with TeraVM.

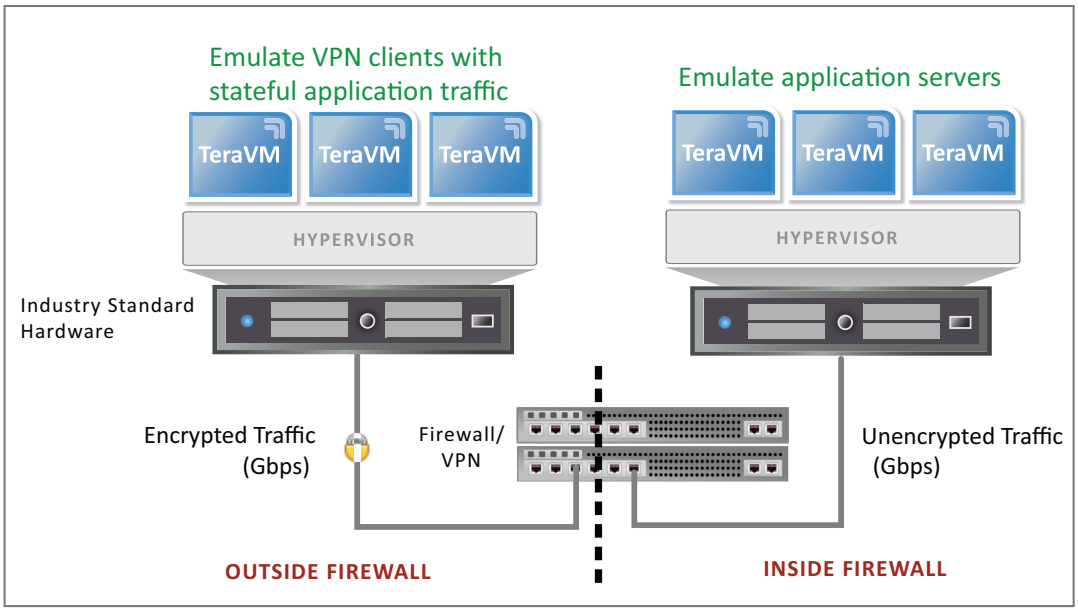

Figure 1: TeraVM emulates stateful VPN clients for a number of leading VPN appliances. TeraVM is used to test the scalability and performance of both the VPN session numbers and the applications being secured.

SSL/TLS/DTLS VPN performance

TeraVM's emulated SSL/TLS/DTLS VPN clients are used to test the leading VPN appliances because it enables performance testing on both the VPN tunnel and the application traffic encapsulated by the tunnel. TeraVM provides real time analysis on both the secure tunnel with dedicated performance metrics and also on the application with its own set of metrics, for each and every emulated application in the tunnel.

VPN client test scenarios

TeraVM's emulated VPN clients are used to test connectivity and access performance of a wide range of network components which require secure connections, these include VoIP Call Managers, Firewalls to IMS Session Border Controllers. TeraVM's real-time performance analysis of both the VPN client and the application flow in the secure tunnel, ensure the correct levels of security are applied for the configured network quality of service settings.

TeraVM SSL/TLS/DTLS VPN client emulation

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 enables mixed testing of IPv4 and IPv6 SSL/TLS/DTLS tunnels and application traffic. The following is a sample set of tunnel specific metrics available as part of the integrated solution:

- ✓ Tunnels Attempted
- ✓ Tunnels Established
- ✓ Mean Tunnel Establishment Time
- ✓ Tunnels Erred
- ✓ Tunnels Rejected
- ✓ Tunnels Completed
- ✓ Number of Control Frames
- ✓ In Tunnel IP bits/second
- ✓ Out Tunnel IP bits/second

Functionality Overview

TeraVM's SSL/TLS/DTLS functionality

- ✓ Support Cisco(AnyConnect), Fortinet (Fortigate) and Juniper (Network Connect and Pulse) VON clients
- ✓ Ciphers:DES, RC2, RC4, RC5, IDEA, AES, Blowfish, Camellia
- ✓ Cryptographic hash functions : MD5, MD2, SHA, MDC-2
- ✓ Public-key cryptography : RSA, DSA, Diffie-Hellman key exchange, Elliptic curve
- ✓ Authentication Mechanism - Username/Password or Certificates
- ✓ Certificate Authority: generate and sign certificates/keys
- ✓ Digital Certificates: X509
- ✓ Dead Peer Detection
- ✓ Auto DTLS fall back to TLS, plus fall forward from TLS to DTLS
- ✓ VPN addressing - IPv4-in-IPv4, IPv6-in-IPv4, IPv4-in-IPv6, IPv6-in-IPv6
- ✓ Define Tunnel Duration and Login Durations
- ✓ Unencrypted packet captures

TeraVM Software 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 & Double Tagging (Q-Q)
- ACL, 802.1p, DSCP

REPLAY
- Replay large PCAP files
- Amplify and dynamically substitute data into PCAP files
- TCP, UDP and raw data playback

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 VPN
- SSL/TLS/DTLS
- IPsec (IKE v1/v2)
- Cisco AnyConnect SSL VPN Client
- Cisco AnyConnect IPsec VPN Client
- 802.1x EAP-MD5

SECURITY ATTACK MITIGATION
- Spam / Viruses / DDOS

VOICE
- VoIP: SIP & RTP (secure & unsecure)
- Dual Hosted UACs, SIP Trunking
- H.323
- Voice & Video quality metric (MOS)

LTE/4G
- GTP tunnel support

SLA
- TWAMP

AUTOMATION
- CLI, Perl, TCL, XML, Java API

SHENICK

NORTH AMERICA
1900 McCarthy Blvd, Suite 301
Milpitas, CA 95035, USA
TEL: 408-385-7630

EUROPE
Brook House, Corrig Avenue,
Dun Laoghaire, Dublin, Ireland
TEL: +353-1-236-7002

www.shenick.com
info@shenick.com