SHENICK SOLUTION BRIEF

IPSec VPN client emulation with TeraVM

OVERVIEW

TeraVM is used to assess the performance of IPSec policy settings of the leading VPN appliances. TeraVM provides detailed, real time analysis on each application being secured by the appliance, enabling a pragmatic approach to IPSec policy settings.

FEATURES

- ✓ Supports Cisco AnyConnect
- ✓ Test with highly scaled levels of encrypted traffic
- ✓ Dedicated performance measurements per IPSec tunnel
- ✓ Security Association: IKEv1 or IKEv2
- ✓ Encryption algorithms: DES, 3-DES, AES-xxx-yyy
- ✓ Integrity algorithms: SHA1, SHA2-xxx and MD5
- ✓ Diffie-Hellman Groups: 1 to 26
- ✓ Address Encapsulation: IPv4/IPv6/ dual-stack
- ✓ Dead Peer Detection: Variable time delays
- ✓ Unencrypted application packet capture

SHENICK

www.shenick.com

A key challenge faced when deploying IPSec VPN appliances is to correctly configure the IPSec policy to suit the user and the application types in use. The complexity of the challenge increases when the number of users are scaled and each user with a unique set of applications. Incorrectly configuring the IPSec policy will come at a cost; set too restrictive the service is unusable, set too weak and the potential for a security breach is high.

TeraVM is the only solution available which enables users test security robustness reliably with the widest range of scenarios. Use TeraVM for testing VPN appliance scalability and to assess the suitability of IPSec policy settings on a wide range of applications. A key differentiator of TeraVM's IPSec VPN client emulation is the ability to emulate and measure performance on a range of application traffic types which are encapsulated by varying strengths of IPSec encryption policies.

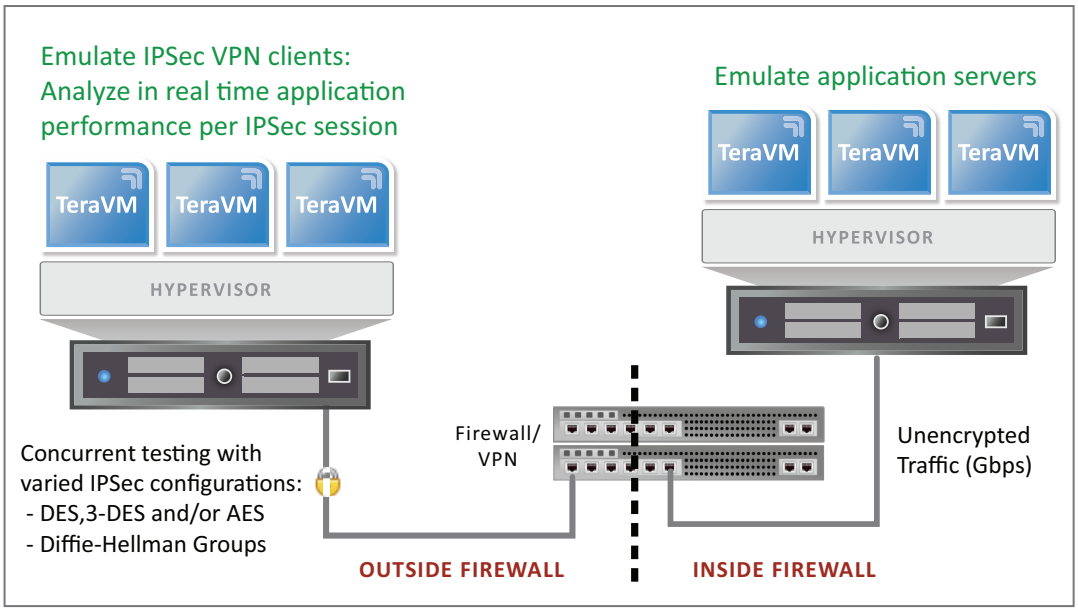

Figure 1: TeraVM emulates IPSec (IKEv1 & IKEv2) VPN clients. TeraVM enables VPN scalability testing with varied policy settings with a focus on deriving the best security policies for a wide range of application types.

Select the right IPsec policy

Test the performance of IPSec policy configurations; vary policy settings to define efficient tunnel setup and the correct level of encryption to deliver applications of video, voice and data with zero quality issues. Use a distributed TeraVM to test performance from remote sites.

Per IPSec tunnel, per application performance measurements

Use TeraVM's per flow performance measurements to determine the performance on a per IPSec tunnel, per application flow basis. Automatically isolate poorly performing applications, use TeraVM un-encrypted packet captures for debugging application traffic.

With TeraVM IPSec VPN client emulation achieve:

- ✓ Optimal IPSec policy settings for session establishment in the network
- ✓ Optimal IPSec throughput from the VPN appliance
- ✓ High levels of application throughput in IPSec tunnels

TeraVM IPSec VPN client emulation

TeraVM IPsec VPN client use cases

IPSec VPN initialization and capacity testing	Vary Diffie-Hellman Groups for optimum tunnel initialization performance. Test throughput using a number of encryption algorithms. Define the capacity of the secure appliance to deliver highly scaled levels of encrypted traffic.
Encrypted Application performance testing	Examine each and every IPSec tunnel and the quality on each and every unique application flow in the VPN tunnel. Use integrated tools for unencrypted packet captures, useful for verifying the actual application flow transactions.
Security Breach Attacks	Emulate IKE Denial of Service (DoS) attacks, determine the impact on capacity at the secure appliance. Test the secure appliance's resiliency with a mix of legal and illegal attack traffic flows.

Functionality Overview

TeraVM's IPsec functionality

- ✓ Support IKEv1 and IKEv2
- ✓ Tunnel Protocol Mode
- ✓ Diffie Hellman - 1 through to 26
- ✓ Encryption Algorithms - DES/3DES, AES-CBC/GCM-256, AES-CBC/GCM-192, AES-CBC/GCM-128
- ✓ Authentication Algorithms - SHA-1, MD5, SHA2-512/384/256
- ✓ Authentication Mechanism - Pre-shared Keys
- ✓ Dead Peer Detection
- ✓ IPSec addressing - IPv4-in-IPv4, IPv6-in-IPv4, IPv4-in-IPv6, IPv6-in-IPv6
- ✓ Application Traffic secured by IPSec - Voice (SIP& RTP), Video (RTSP), Data (HTTP, SMTP, POP3)
- ✓ Unencrypted packet captures

Sample IPSec performance measurements

- ✓ 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

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