TeraVM VPN FAQ

VIAVI Solutions

This document serves as a guide to provide background on Virtual Private Network (VPN) testing with an emphasis on failover functionality.

For additional Cisco details re Cisco AnyConnect VPN see:
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116312-qanda-anyconnect-00.html#anc14

WHAT IS TeraVM?

We refer to TeraVM as a "Virtualized IP Test and Measurement Solution". The key word in this description is "Virtualized". TeraVM does not require any propriety hardware and can be run on industry-standard hardware. By this we mean any x86 based server from the likes of Dell, Cisco, IBM, HP, Huawei or others. The only requirement is that the industry-standard server have a hypervisor (e.g. VMware ESXi, KVM, etc.) installed on it. It also runs in Amazon and Microsoft Azure clouds.

TeraVM is used to emulate client and/or server traffic for the purposes of testing a discrete device (e.g. VPN firewall, video server, router, VoIP gateway etc.) or network to determine performance characteristics, limitations of features/functionality or any other similar type of testing.

TeraVM is also a mobile network emulator emulating either the RAN or Mobile Core for all generations of 3GPP standards.

VPN SPECIFICS

Q. Can TeraVM Emulate Virtual Private Network Traffic?

Yes, TeraVM can generate Remote Access VPN and Site-to-Site VPN traffic to test VPN headends and access points for performance and capacity

Q. What VPN Protocols does TeraVM Support?

TeraVM supports SSL/TLS based VPNs using numerous vendor specific implementations, for example, Cisco AnyConnect, Pulse Secure, F5 etc. TeraVM also support IKE/IPsec based VPNs under the generic IKE/IPsec VPN Client application and also under the Cisco AnyConnect Client application. In addition, TeraVM supports DTLS on the Cisco AnyConnect VPN Client Application.

Q. What authentication methods are supported?

Depending on the specific VPN application type TeraVM can support Certificate based, username/password based or PreSharedKey based authentication.

The Cisco AnyConnect VPN Client and the IKE/IPsec VPN Client application support the use of RSA Certificates and ECDSA Certificates, in addition to EdDSA signature algorithms.

IKE ECDSA authentication supports the following certificate/key types:

- ECDSA-256 - Cert/Key secp256r1 (prime256v1)
- ECDSA-384 - Cert/Key secp384r1
- ECDSA-521 - Cert/Key secp521r1

The AnyConnect VPN client supports:

- DTLS - IKE ECDSA when using ECDSA certs for Multiple Certificate Authentication
- SSL/TLS - IKE ECDSA when using ECDA certs for Multiple Certificate Authentication
- IKE/IPsec - IKE ECDSA when using ECDSA certs for both Certificate and Multiple Certificate Authentication

The IKE/IPsec VPN Client supports:

- IKEv2 - IKE ECDSA when using ECDSA certs for signature authentication

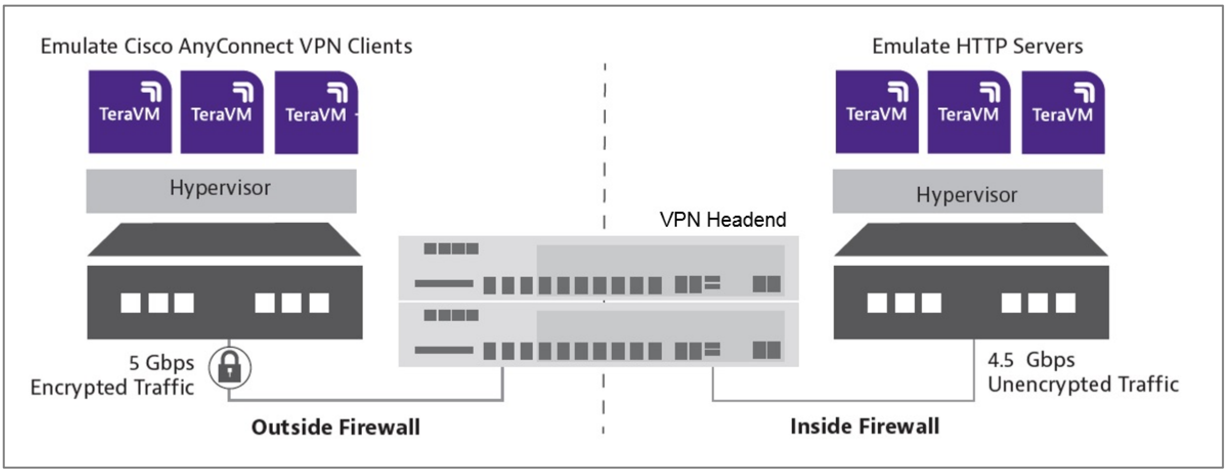

Figure 1: Typical VPN Headend Test Setup

Q. TeraVM is used to generate Application Traffic. Can TeraVM Generate Application Traffic over VPNs?

Yes. The architecture of the VPN client facilitates the definition or creation of a Tunnel object, when the VPN client Application has been authenticated. This tunnel object can then be used assign application traffic profiles to transport between the 'Outside' client-side entities and the 'Inside' server-side resources to generate application traffic. e.g. HTTP/HTTPS, FTP, VoIP etc. Multicast Traffic is NOT supported, unicast traffic only.

Q. Does TeraVM Support VPN Failover?

Yes. TeraVM supports the mechanisms to facilitate VPN failover in a VPN headend setup that initiates the failover between Primary and Backup/Standby VPN Headend. This is supported in the Cisco AnyConnect VPN Client Application.

Q. What Failover Mechanisms are supported?

TeraVM provides the Client-side mechanisms to track and participate in a failover activity. This is achieved by ticking the 'VPN Failover' tick-box on the Cisco Anyconnect VPN Client application. This is supported for IKE/IPsec and also SSL/TLS and DTLS based VPN clients.

Q. How is Failover Achieved?

Failover depends mainly on Dead Peer Detection (DPD) messages which detect messages being lost due to failure scenario. Another key detection mechanism used is a shorter rekeying interval.

For SSL/TLS when a tunnel disconnection is detected the VPN emulation engine will trigger a reconnection using the same tunnel 'cookie'. After 3 attempts it will close the tunnel and restart the connection from scratch. The reconnection will be directed to whichever is the active VPN headend.

Q. Are there any other factors to consider for VPN failover?

Another important aspect is the tunnel establishment rate. For example, if tunnel rate for 1,000 tunnels is 30 seconds, we recommend increasing to 60 seconds. This applies to the VPN Client application.

Some guidance on scaled configurations:

- 300 Reconnect per second is acceptable level 100-150 for Certificate Authenticated
- DPD intervals should also be revised accordingly for scale

When testing scale, (thousands of VPNs) loss of traffic on a tunnel is a real possibility. A feature on ASA can reset a tunnel if no traffic persists and therefore re-initialises the session by tearing down for no traffic. vpn-idle-timeout – The default value is '30 minutes'.

Q. How many Tunnels have been tested?

Site-to-Site VPNs - ~35,000 Tunnels

Remote Access - 10,000 Tunnels