ACL Digital
an ALTEN group company

VPN Gateway
(vVPN)-3.0

Overview

Increasing global footprint of enterprises and mobility of workforces has increased the demand for enhanced network security and data protection at high packet processing speed. Various hand held devices other than computers now connect to rough public data infrastructure. Securing the sensitive data transmitted to these remote devices has become mission critical in the world with ever increasing security threats.

ACL VPN provides organizations, NEMs and service providers a scalable IPsec VPN solution in various deployments along with high performance.

ACL IPSec VPN Gateway solution provides IPSec tunnel establishment, termination and service gateway functionality that can be deployed as direct application on a Native, Bare metal server or as a Virtual Network Function in Cloud Infrastructure.

Solution

This solution is developed to run on Intel x86 based platforms, using DPDK (Data Plane Development Kit) Software Development Kit (SDK). Software and Hardware architecture of this solution allows achieving 25X performance over the solutions from Traditional Network Equipment Manufacturers. A Cloud VPN Gateway solution can be used to provide VPN connectivity to Wi-Fi users or wired residential/enterprise broadband subscribers. It can also be used for securely connecting mobile small cells or HeNBs to EPC. It also can become a VNFC of a Virtual CPE (vCPE) solution with the addition of Firewall, IDS/IPS and other services along with the IPsec VPN Gateway. ACL IPSec VPN Gateway solution provides IPSec tunnel establishment, termination and service gateway functionality that can be deployed as direct application on a Native, Bare metal server or as a Virtual Network Function in Cloud Infrastructure.

VPN Features

- DPDK based, optimized IPsec for high performance Fast path processing
- Runs as VNF on the Cloud Platforms – GCP and AWS
- Supports jumbo frames as well as unicast and multicast features for voice, video, and data traffic in diverse, large-scale applications.
- Leverages Suite B cryptographic algorithms like AES (CBC, CTR & GCM) for encryption and XCBC & SHA2 for Authentication
- Diffie-Hellman groups from 1(MODP-768) to group 18 (MODP-8192)
- Deployable as Site to Site, Remote access VPN and Hub & Spoke
- GRE Over IPSec for Transport mode
- IKE-v2 with Rekey (Parent and Child Rekey)
- Pre-Shared Key (PSK), X.509 Certificate based authentication (PKI)
- Client Authentication using CRL, OCSP & EAP.
- Support 3GPP TS 33.320 V10.5.0
- IKE fragmentation
- Virtual IP pool, DHCP
- NAT-T Support
- Dead Peer Detection(DPD)
- Various IKE, ESP and system statistics collection and logging
- VPN Gateway package installation solution on Cloud platform (RPM, Debian)
- Openstack based Orchestration and Life Cycle Management
- CLI based fault monitoring and status information
- REST API support for remote configuration and monitoring

Detailed Feature List

Keying Methods

- IKEv2

IPSec Methods

- Policy Based
- Route Based

Authentication Algorithms

- HMAC-MD5 key size – 128 bits
- HMAC-SHA1 key size – 160 bits
- HMAC-SHA2 key size – 128, 192 & 256 bits
- HMAC-XCBC key size - 96 bits

Crypto Algorithms

- NULL
- 3DES key size - 168
- AES-CBC key size - 128, 192 & 256
- AES-CTR key size - 128, 192 & 256
- AES-GCM key size - 128 (ICV 8, 12 & 16)

Pseudo-Random Functions

- HMAC-MD5
- HMAC-SHA1
- HMAC-SHA2
- HMAC-CMAC

Diffie-Hellman (DH) Group

- DH-01 (MODP-768)
- DH-02 (MODP-1024)
- DH-05 (MODP-1536)
- DH-14 (MODP-2048)
- DH-15 (MODP-3072)
- DH-16 (MODP-4096)
- DH-17 (MODP-6144)
- DH-18 (MODP-8192)

Solution Features

Client Support List

- Strongswan, Windows OS native, Apple iOS native, Android (via strongswan)

PARENT SA Support

- Tunnel Mode
- Transport Mode
- Perfect Forward Secrecy (PFS)
- PFS and Non-PFS mode
- NAT-T Detection and Negotiation
- NAT-T (UDP Encap ESP) for both tunnel & transport
- IKE Fragmentation
- Certificate Request Payload
- CIPHER and HASH algos negotiation

Authentication Method

- Pre-shared key(PSK)
- RSA X.509 Certificate based authentication (PKI)
- Chained Certificates
- Extensible Authentication Protocol (EAP)

CHILD SA Support

- CIPHER and HASH algos negotiation for data security
- Encapsulating Security Payload (ESP)
- Crypto Multi Buffer Support (CMB) for Data Encryption /Decryption Authentication in Fast path
- Multiple Traffic selectors (IKE v2), Traffic selector narrowing
- Configuration payload for roaming user IP address(DHCP/Local Pool)

Certificate Management

- CRL (Certificate Revocation List)
- OCSP (Online Certificate Status Protocol)
- Complete PKI architecture

Tunnel Control

- Dead Peer Detection (DPD)
- Lifetime negotiation
- Re-keying
- Re-Auth
- Tunnel Statistics
- PKI (CRL/OCSP for certificate revocation)

Management Features

- CLI based device configuration and Statistics information
- REST API based Management – For configuration and Stats
- Graphical User Interface for configuration and monitoring
- Centralized Management: Openstack based Orchestrator
- Package based distribution for different platforms
- Extensive logging support

Supported RFCs

- RFC 5996, RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7383: Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- RFC 6818: Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
- RFC 4806: Online Certificate Status Protocol (OCSP) Extensions to IKEv2
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3602: The AES-CBC Cipher Algorithm
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use with Ipsec
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec

VPN – Scalability & Performance

Licensing model support for different scalability, capacity and performance need. Depending upon the environment chosen, the maximum possible numbers are

- High performance IPsec VPN, scalable IPsec tunnels and throughput traffic
- Tunnel establishment rate is up to 1,000 tunnels/second
- Maximum capacity of 128K tunnels is supported on 1RU server
- 4-port 10 GbE in line IPsec traffic (Bi-Directional) at wire speed
- VPN throughput can scale up linearly with the increase in the number of CPU cores, providing unparalleled performance in a compact form factors, as well as Rack Servers

VPN – Platform Support

Support for different virtual environments

- Deployable on a VM or bare metal with
- Intel X86 COTS platforms
- As VNF on Google Compute Platform (GCP) and AWS provided by cloud operators
- OpenStack

Architecture

- Designed and Developed fast path processing using latest versions of DPDK
- Scalable architecture based on the needs. IPsec Fast path can scale on

a. Standalone software instance as Virtual Machine(VM)

b. Cloud deployment

- IPsec Fastpath can scale from one core to Multiple cores based on requirement and performance needs

c. Bare metal

d. Virtualization Support for VirtIO, SR-IOV, PCI Pass-through

Deployment Diagram