Zentera ZCA for Secure Private Line

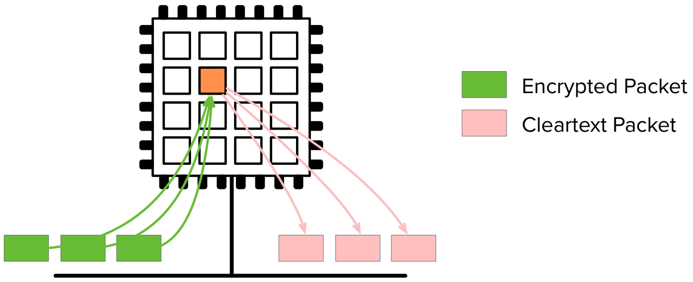
Multi-Gigabit Security through Overlay Application Proxy Networks

MPLS Encryption in Cloud: The Throughput Problem

Cloud Service Providers like AWS and Microsoft Azure offer dedicated network connection services to establish high-speed MPLS links from private on-premises or colocation environments to one of the AWS Direct Connect or Azure ExpressRoute supported peering points. MPLS does not encrypt traffic and under the shared responsibility model for security and compliance, protecting the data remains customer's responsibility, implemented and managed by customers in the VPC.

Enterprises have traditionally used IPSec VPNs to address network encryption between sites. The design and security implementation for IPSec VPN is complex, with site-to-site persistent connection shared by multiple applications. IPSec VPNs lack host / application level security as well as end-to-end data encryption, as the tunnel terminates at the VPN concentrator.

High-speed IPsec is provided by hardware VPN concentrators at each end of the tunnel, but for cloud deployments, software VPN gateways running on a cloud VM must be used. There is a "speed limit" of about 1.25Gbps for software-based implementations of IPsec. IPsec is a Layer 3 protocol without any knowledge of Layer 4 sequence numbers; as a result, packets from all flows through a single CPU core to prevent reordering. Software VPNs from all vendors, including AWS and Microsoft Azure VPN gateways face this limitation in IPsec throughput. Not only does this limit application flow bandwidth, it also impacts the transport utilization. For example, a 2 Gbps Azure ExpressRoute circuit limited to 1.25 Gbps operates at 62.5% utilization. This is a fundamental limitation of IPsec technology on modern multicore CPUs which cannot be improved with a faster network transport.



Zentera ZCA for Secure Private Line

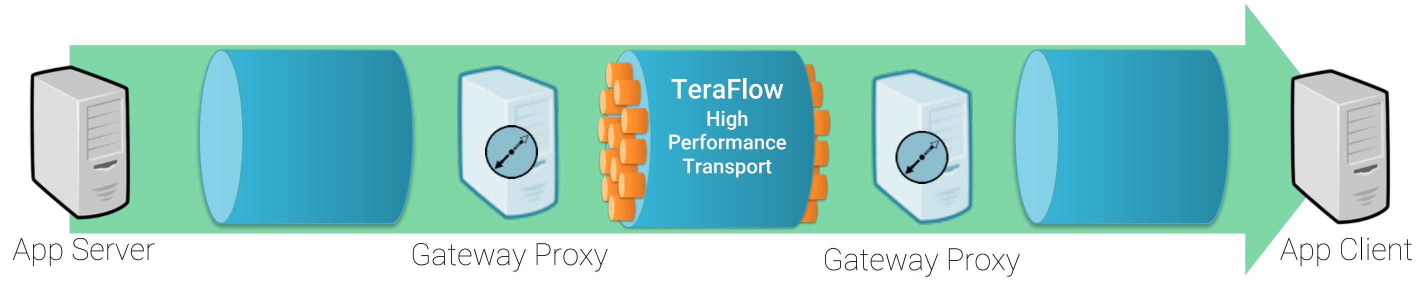
- TeraFlow™ encryption multi-gigabit single-flow performance and TLS 1.3-strength protection
- Security Filter Table built-in for firewalling function
- Works on any private line, including Azure ExpressRoute and AWS Direct Connect
- Implements without touching existing network and security infrastructure

97 E Brokaw Road Suite 360 • San Jose, CA 95112
www.zentera.net

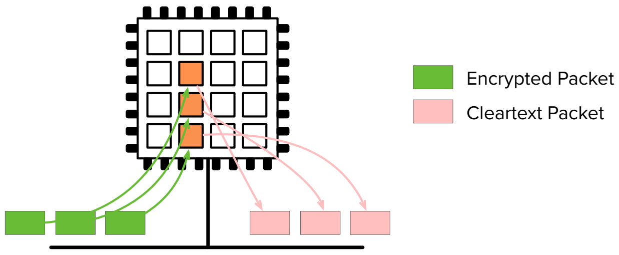
Illustration of the IPsec "Speed Limit" – network performance throttled by a single CPU core

Zentera TeraFlow™ Encryption

Zentera Cloud Access (ZCA) zCenter release 5.2.1 and up supports a new feature called TeraFlow, which enables for high speed transport between pairs of Gateway Proxy machines.



The fundamental CoIP® proxy technology is implemented at TCP/IP Layer 5, and as a result the Gateway Proxy machines are aware of Layer 4 flow concepts. TeraFlow can distribute packets from a single application flow to multiple CPUs while ensuring packet ordering, allowing much more efficient utilization of the Gateway Proxy CPU and higher throughput. Zentera has demonstrated single flow performance (application to application) of 6Gbps, and aggregate performance with multiple flows exceeding 10Gbps on a single Gateway Proxy.



	VM Instance	Single Flow	8 Flows
US West (Oregon)	c5.xlarge	3.84	5.29
	c5.2xlarge	4.72	8.01
	c5n.4xlarge	6.00	13.50

TeraFlow Encryption results in AWS demonstrate more efficient CPU utilization for encryption

Multiple Gateway Proxy machines can be clustered in parallel to achieve 20Gbps or higher aggregate link encryption over an MPLS WAN transport.

Security Filter Table

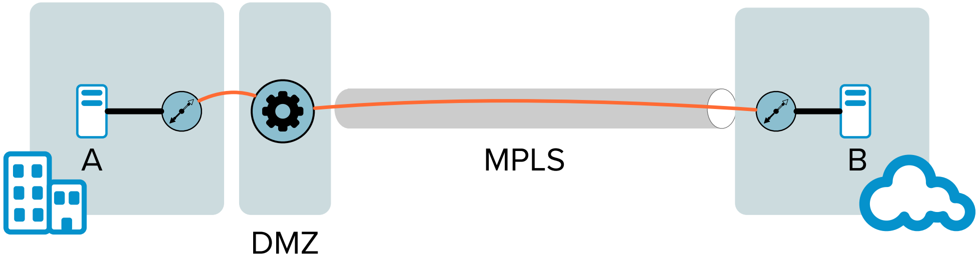
The original implementation of Zentera zCenter supported a whitelist model for security enforcement; applications or endpoints were admitted to the overlay network by whitelist policy, defined in an Application Profile. Zentera zCenter release 6.1.1, that model has been revised and now supports firewall-style permit and deny rules; this enables administrators to define both whitelist and blacklist policies, based on L3 and L4 (Endpoint and Gateway Proxy), and application (Endpoint Proxy only).

Remote Database Replication with Zentera ZCA

The power Security Filter Table function can be combined with TeraFlow encryption to enable secure high-speed database replication to the cloud. Database replication is frequently a critical part of backup or disaster recovery services, and are required to meet certain operational targets. Databases with large change rates need high per-flow performance to enable replication while delivering the required Recovery Point and Recovery Time Objectives (RPO/RTO). For example, a database with a 1TB daily change rate will require >2Gbps single flow throughput to achieve a 1-hour RPO – not achievable with IPsec VPN and a software-based VPN gateway.

Single Flow Throughput	Time to Transfer 1TB	Time to Transfer 10TB
1Gbps	2.2h	22h
2Gbps	1.1h	11h
4Gbps	33m	5.5h
6Gbps	22m	3.7h

The diagram below illustrates database replication using Gateway Proxy machines to provide a high-speed, filtered and encrypted connection between machine A (database machine) in an on-premises environment, and machine B (replication target) in a cloud environment. To start the replication, Host A makes a connection to the on-premises Gateway Proxy, which then initiates the CoIP setup to create a TLS 1.3 tunnel to the cloud Gateway Proxy, which in turn forwards traffic to Host B. Because all communications are with the Gateway Proxy server, neither Host A nor Host B are aware that the other machine is remote.



For security, the TLS 1.3 tunnel is built on-demand, and if database replication stops, the tunnel is automatically torn down until it is needed again.

The Security Filtering Table can be programmed to whitelist specific servers ("only Host A can talk to Host B"), specific ports/protocols (TCP with port numbers), and to blacklist known protocols/ports for extra security (e.g. TCP port 22). To make the filtering as effective as possible, and to minimize cleartext traffic in the network, it is recommended to deploy the Gateway Proxy machines as close as possible to the database servers – ideally, within the same DMZ as part of a *Deep Segmentation* strategy to minimize the attack surface.

This basic configuration has been used in customer production traffic to saturate multi-gigabit Microsoft Azure ExpressRoute links.

Zentera ZCA vs IPsec Comparison

	Zentera ZCA	IPsec with Cloud VPN Gateway
Technology	Layer 5, Proxy	Layer 3, Network
Network Component	Gateway Proxy	Router/VPN Gateway
Transparent to Routers/Firewalls	Yes	No
Encryption Tunnel	TLS 1.3	IPsec
Tunnel Termination	At Gateway Proxy, near Endpoint application edge	At VPN Gateway/Concentrator, near corporate edge
TeraFlow Performance	Yes; 6Gbps per flow 10+ Gbps aggregate	No; 1.25Gbps max
Host-Based Controls	Yes	No
Application-Based Controls	Yes (Endpoint Proxy)	No
Built-in Firewall	Yes, SFT	No

For More Information

On the Web:
https://www.zentera.net

Email:
sales@zentera.net

Phone:
+1 (408) 436-4811

Copyright© 2020 Zentera Systems, Inc. All rights reserved. Zentera®, Zentera CoIP®, CoIP®, Cloud over IP®, and certain other marks are registered trademarks of Zentera Systems, Inc., in the U.S. and other jurisdictions, and other Zentera names herein may also be registered and/or common law trademarks of Zentera. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Zentera, and Zentera disclaims all warranties, whether express or implied, except to the extent Zentera enters a binding written contract with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Zentera. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Zentera's internal lab tests. In no event does Zentera make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Zentera disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Zentera reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.