CERTES NETWORKS

White Paper

Certes Networks' Layer 4 Encryption

Network Services Impact Test Results

Executive Summary

One of the largest service providers in the United States tested Certes Networks' Layer 4 payload encryption over their MPLS network. In each test, the encrypted traffic traversed the MPLS network as expected. The PBR test was designed to bypass normal routing (via routing table). Interesting traffic was successfully routed after encryption using port-based PBR rules.

The tests clearly demonstrated that the Certes Networks encryption solution passes packets with Layer 2 through Layer 4 headers in clear text while encrypting the data payload and without disrupting network services or applications. The unique capabilities of the Certes Networks Layer 4 encryption solution also makes troubleshooting an encrypted network easier.

The Certes Networks Layer 4 encryption solution is designed to be completely agnostic to the WAN. If you have a working network, then the solution can surround and protect the network without impacting network services or applications.

Note: *The following encryption capabilities are not possible with traditional, appliance-based IPsec encryption solutions because all of the Layer 4 header information would be encrypted.*

Introduction

Certes Networks has deployed multiple network encryption solutions on various types of networks around the world. When you need to encrypt your data in motion, Certes Networks makes it easy. Whether you need to protect a single link, or your entire network, Certes Networks eliminates the complexity of encrypting today's networks.

Certes Networks has extended their encryption capabilities to include the ability to encrypt Layer 4 payload data while the Layer 4 header information remains in the clear. This functionality allows for Layer 4 network services to run while the data payload is encrypted.

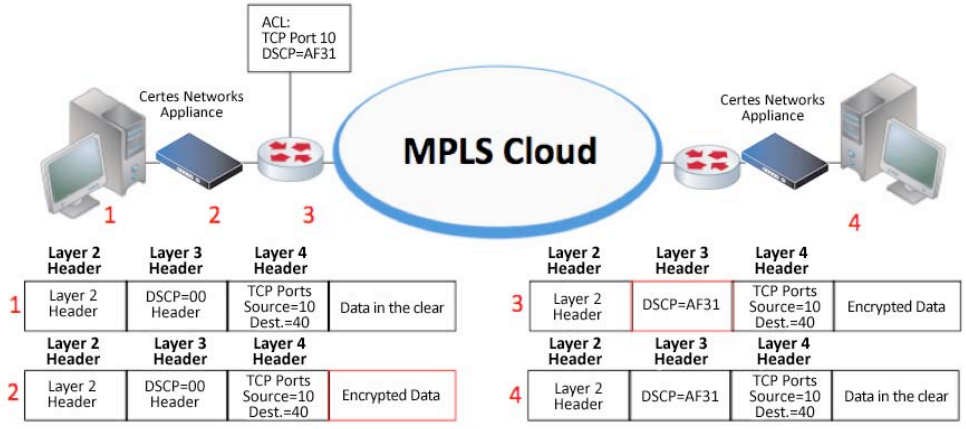
The Service Provider tested the Certes Networks Layer 4 encryption capabilities to measure the impact of the Certes Networks solution on CoS markings, Network Address Translation (NAT), Policy Based Routing and Netflow.

The Tests

In order to fully test the performance of the Certes Networks Layer 4 encryption solution, the following tests were performed.

Class of Service (CoS) Markings after Encryption

Test Setup: Two data streams were generated between two endpoint PCs using TCP ports 10 and 20. These TCP streams were sent with default DSCP (00) marking. They passed through the Certes Networks device with Layer 2, 3 and 4 headers in clear text. This was verified through packet capture on the remote side of Certes Networks appliance.



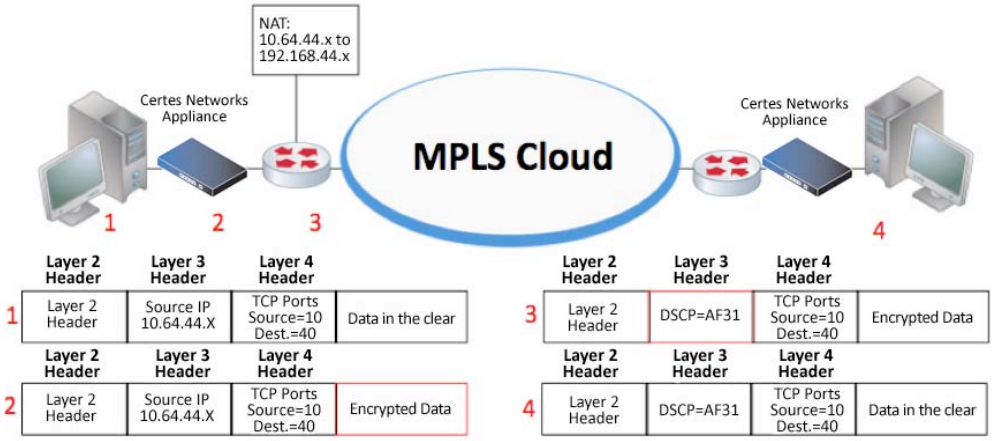
On the Customer Edge (CE) router, an extended Access Control List (ACL) was configured to match on specific IP and TCP ports. TCP port 10 traffic was marked and classified into the Class 2 queue or DSCP AF31. TCP port 20 was classified into the Class 1 queue or DSCP EF. Classifications and markings were verified through "sho policy-map int" command.

In addition, packets were captured on the far-end CE router (off the remote end of the Certes Networks appliance). TCP ports 10 and 20 traffic was clearly marked with DSCP AF31 and EF.

Test Results: The markings were set correctly after encryption, passed through the MPLS network and were present after decryption.

Network Address Translation (NAT) after Encryption

Test Setup: NAT was enabled on the CE router to NAT the source IP address. Packets were sent from 10.64.44.x address. As they passed through the Certes Networks appliance, the data payload was encrypted while the address was preserved. The packets were then switched to the CE router. On the CE router, the 10.64.44.x address was translated to a 192.168.44.x address.

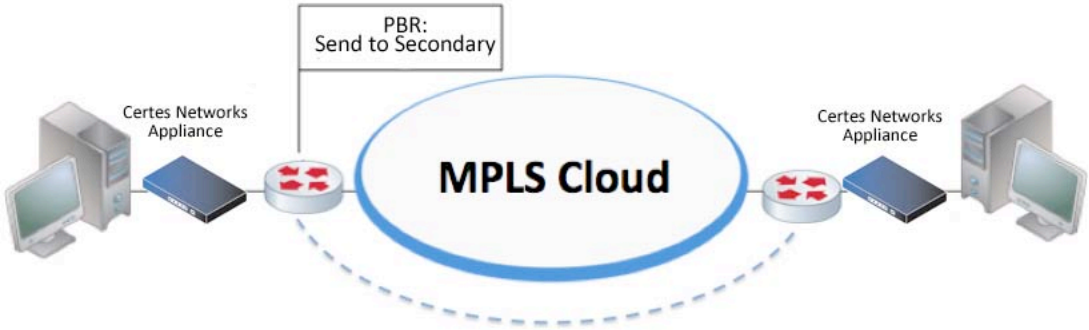


Test Results: Even though the address translation occurred after encryption, Certes Networks was able to successfully decrypt the NAT'd packets. Traffic was properly decrypted at the other end with the NAT'ed IP address on the clear packet after decryption.

Policy Based Routing (PBR) after Encryption

Test Setup: On the CE router, PBR was set up to re-route packets based on Layer 4 port information. An extended ACL was setup to match on a specific IP

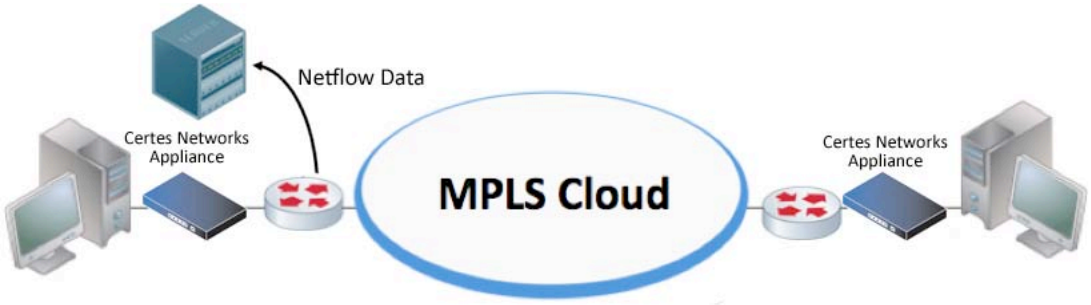
and TCP port to redirect packets as it entered the router. Instead of following the normal routing (via routing table), interesting packets were routed based on PBR policies.



Test Results: Although the data was encrypted, the traffic successfully bypassed the MPLS network based on the PBR port based rule. The CE router had no problem applying PBR rules based on the Layer 4 information of packets encrypted by CipherEngine.

Capturing Netflow Statistics after Encryption

Test Setup: Depending on the physical and logical placement of Netflow monitored devices, Netflow packets may or may not be encrypted. For this test, Netflow configuration and monitoring was set up on the CE routers beyond the encryption appliances. The 10.64.36.20 PC was configured as the Netflow collector and data was sent through the network.



Test Results: The Netflow analyzer successfully collected address, protocol and port information after the data was encrypted using Layer 4 encryption.

Layer 4 Encryption Tests Summary

The tests clearly demonstrate that the Certes Networks encryption solution successfully passes packets with Layer 2 through Layer 4 headers in clear text while encrypting the rest of the packet over any network. They also prove that

Certes Networks' solution can encrypt data without disrupting network services or application performance. This allows customers to run Class of Service, Network Address Translation, Policy Based Routing, Netflow and any other router commands that may require Layer 4 information.

Troubleshooting Benefit

With traditional IPsec encryption, all packets are encrypted and marked as ESP (protocol 50) packets. If there is a problem with an application, network engineers are not able to identify the applications because the application port information is encrypted. This makes troubleshooting an encrypted network difficult.
With the Certes Networks Layer 4 encryption solution, the information needed to identify the application remains in the clear on the packet, while the data itself is encrypted. This allows network engineers to troubleshoot a network that is encrypted using Layer 4 encryption with the same methodology as they normally do.

About Certes Networks

Certes Networks (formerly CipherOptics) is the leader in developing scalable security solutions for high performance networks. We provide advanced encryption and policy and key management solutions for securing wide area networks, and enable secure connectivity to private and public clouds. Certes Networks helps organizations improve security, decrease risk, and reduce the cost of compliance with data privacy regulations while enabling high performance and secure connectivity to critical infrastructures in the branch office, data center or in the cloud.