AppEx CloudWAN
Ultimate Enterprise Security

Abstract

Enterprises often have an illusion that it is more secure with a private network, like MPLS VPN. But in reality, security is gained mainly through strong encryption, well managed authentication and authorization. In terms of data transmission, encryption is the key element of security, so this whitepaper focuses mainly on the encryption aspect of enterprise information security.

Using MPLS as WAN links, enterprises still need to apply the right encryption mechanism if security is a concern. Hackers can easily sniff traffic on MPLS as long as they can tap the fiber somewhere on the path, and not to mention that MPLS service provider and authorized government agencies (and sometimes other countries' counterparts) can always tap the fiber and sniff traffic flowing through MPLS VPN. So the private links like MPLS do not necessarily provide secure data transmissions, and the burden is still on enterprises to apply encryptions to their sensitive data.

Taking care of encryptions can be a pain to many enterprises. The good news is that with the emerging trend of SD-WAN, there is finally a possibility to have encryption embedded in connectivity itself. AppEx CloudWAN is such a SD-WAN implementation that embeds strong and flexible data encryption and take enterprise security as its highest priority.

Customer Managed CloudWAN and End to End RTT

Most of AppEx customers are using AppEx managed CloudWAN, as illustrated by Figure 1. As the most common use case, when a customer's branch office connects to its headquarter with CloudWAN, there are three RTT (Real-Time TCP) tunnels involved in the data transmission. The branch office connects to a close-by CloudWAN edge POP (Point

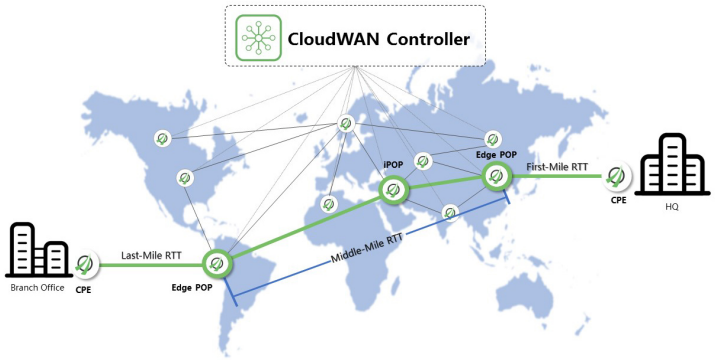

Figure 1. AppEx Managed CloudWAN

Of Presence) via RTT, illustrated as Last-mile RTT. The headquarter does the same with the First-Mile RTT. Both RTT tunnels can choose to use IPSec to encryption traffic, in which case the customer allows AppEx to manage keys. Meanwhile, IPSec encryption can also be applied on the Middle-Mile RTT tunnel between two edge POPs, with keys also managed by AppEx.

The main advantage of the three RTT tunnel approach is that there can be advanced application optimization features enabled at the edge POPs, like object cache, which provides local responses to client requests and hence significantly reduce the response time.

For customers with rigid security requirement, they can choose end to end RTT with IPSec encryption between two CPEs, in which case, the data is in encrypted tunnel along the path, and even AppEx cannot decrypt the data in CloudWAN POPs. This end to end RTT approach is further discussed below together with customer managed CloudWAN option.

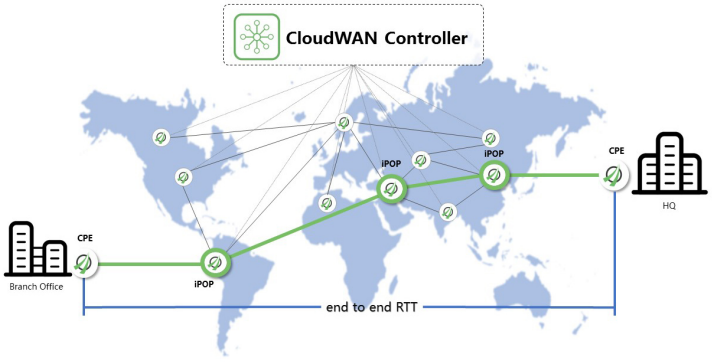

Figure 2. Customer Managed CloudWAN

Besides AppEx managed CloudWAN, AppEx provides another option for customers who want to gain full control of data security, which is called customer managed CloudWAN. With this option, AppEx builds a CloudWAN network with POPs dedicated for this customer, and hand the management to the customer. Use the same case of the connectivity between the branch office and the headquarter, the customer can now gain full control of IPSec encryptions for all three RTT tunnels.

To make it even more secure, there can be a single end to end RTT tunnel established directly between the branch office and headquarter, illustrated by Figure 2. With this end to end RTT, the IPSec encryption and key exchanges happen directly between the branch office and the headquarter, and CloudWAN POPs along the path becomes intermediate POPs (iPOP), which only apply route optimizations

and are not able to decrypt the traffic. Hence the original data is never exposed on public domain.

Besides, CloudWAN RTT tunnel does not assume any packet encapsulation and data type inside it. Customers can always keep their existing security mechanism and put the already encrypted traffic into RTT tunnel, in which case IPSec encryption on RTT tunnel provides an extra layer of security.

CloudWAN – Software Defined Security

The customer managed CloudWAN option together with the end to end RTT unlocks the full potential of SDN (Software Defined Network) in terms of security. The following discussion is based on this combination.

Figure 3 shows the encapsulation of RTT tunnel packets. IPSec is a layer inside RTT tunnel header, and the original packets are completely encrypted by IPSec, including IP and TCP/UDP headers. Meanwhile, this encapsulation design allows the separation of security and CloudWAN data transmission optimization (RTT acceleration and route optimization). This allows data/network security to be separately managed, and enables Software Defined Security in the following ways:

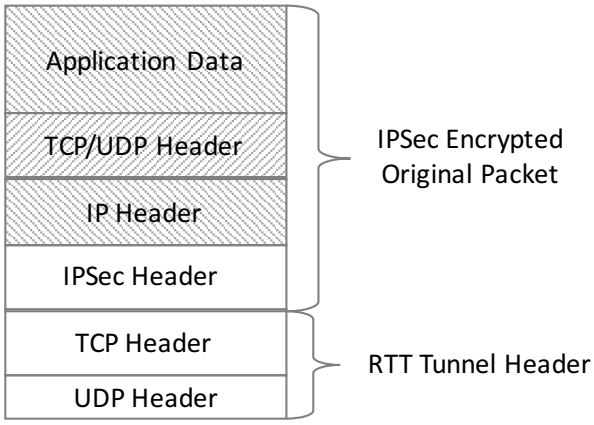

Figure 3. RTT tunnel encapsulation

1. Each RTT tunnel can carry different IPSec encryption, which means that the customer can choose different encryption algorithms and key sizes, or no encryption, for different locations and applications according to the level of the sensitivity of the data. CloudWAN will put the data into different RTT tunnels in case their security requirements are different.
2. For highly sensitive data, to avoid any breach of data on POPs that reside on public Cloud, end to end RTT can be used to connect two CPEs (or virtual CPEs) directly, so there is no exposure of clear text data on public domain. In general, a 128-bit symmetric key (by default in CloudWAN) is computationally secure against any brute-force attack. The customer can also choose a 256-bit key size for even more sensitive data.

3. The key management is completely controlled by the customer, and even AppEx has no access to the keys, and hence cannot decrypt the traffic.
4. Some customers, especially these multi-national corporations, may have concerns on the locations their data may traverse for security or government regulation reasons. With customer managed CloudWAN, they can have full control of the route of any RTT tunnel, hence provision the geographic locations of the POPs and physical links for some of their highly sensitive data.

The above Software Defined Security capabilities are unmatched by any existing WAN infrastructures, private circuit based or SD-WAN based.

Conclusion

AppEx managed CloudWAN provides an easy way to use SD-WAN solution with AppEx managed encryption embedded in the RTT tunnels. Meanwhile Customer managed CloudWAN together with the end to end RTT option provides an ultimate enterprise security solution that no other WAN infrastructure can match. It fully releases the power and flexibility of Software Defined Security, and put enterprises in full control of their information security.

