Obtaining Egress Savings using Private Connections to Cloud Service Provider

Anurag Singh Mandhar
Principal Architect

Ghassan Semaan
Sr Mgr-Solutions Architect

If you would like to discuss this
further with Verizon, please email
us at tech-expert@verizon.com.

verizon✓
business

Contents

1. Executive Summary

An increasing number of enterprises have migrated or are in the process of migrating their applications to be hosted in the cloud, motivated by benefits such as cost savings, scalability, and flexibility. To access those applications, most of those enterprises rely on the Internet, driven by the assumption that the Internet provides a cheaper network alternative to private networks. What is sometimes overlooked during the cost comparison is the cost of transferring data out from the Cloud Service Providers (CSPs). While transferring data to CSPs (called "ingress data") is typically free, data charges for transferring data out from CSPs (called "egress data") can be a considerable cost that is often overlooked. Because the CSPs charge significantly more for egress data over their Internet gateways versus a private connection, the aforementioned assumption about the Internet being cheaper is not always true.

In this document, we compare the cost between Internet-based and private connection-based network alternatives, and we show when each alternative is the best suited for a lower egress cost. For the private network alternative, we used Verizon's Secure Hybrid Network service for the private WAN connectivity and Verizon Software Defined Interconnect (SDI) for the connection to the cloud. Please note that Verizon has other private network services, such as Private IP and Secure Cloud Interconnect, that can be used as well to connect an organization's network to a cloud hosted service and deliver similar saving results.

2. On Prem to Cloud Connectivity Options

Before we get into the cost comparison, let's quickly review the two connection options at a high level.

2.1. Internet-based

Enterprises can connect to CSPs using a combination of Public Internet and IPSec VPNs. This involves enterprises accessing the Internet using broadband connectivity and then configuring a site-to-site IPSec VPN service between their remote locations and a VPN gateway provided by the CSPs. The IPSec tunneling provides an encrypted and secure tunnel between the enterprise's network and the CSP's network.

**Figure 1: On Prem to CSP using internet**
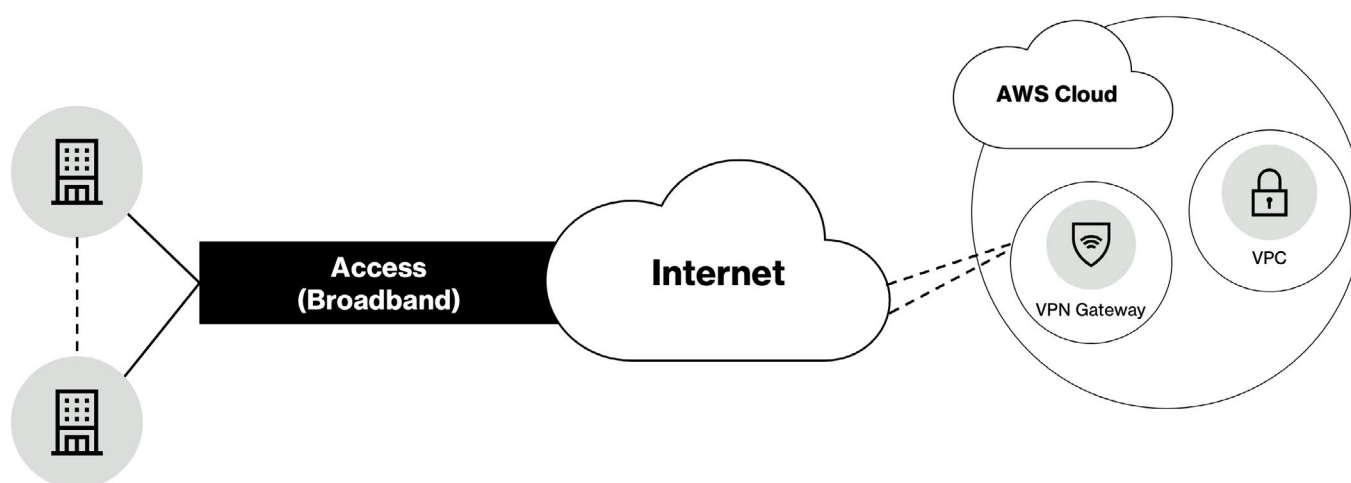
2.2. Private Connection

Enterprises can opt to use a private connection alternative from the CSP, such as Amazon Web Services (AWS) Direct Connect or Azure Express Route. When such a solution is selected, a private network will be required to connect the enterprise remote locations to that CSP private connection.

One such possible private network could be the Verizon Secure Hybrid Network which can utilize the same broadband access the enterprise uses for the Internet access but to connect to Verizon Private IP MPLS based backbone network. Verizon Software Defined Interconnect is then used to connect the MPLS backbone network to the private construct from the CSP (for example, in the case of AWS, that would be establishing a connection to an AWS Hosted Direct Connect). A short description of both Secure Hybrid Network and Software Defined Interconnect is provided in the Appendix.

Figure 2: On Prem to CSP using Secure Hybrid Network & Software Defined Interconnect

Figure 2: On Prem to CSP using Secure Hybrid Network & Software Defined Interconnect
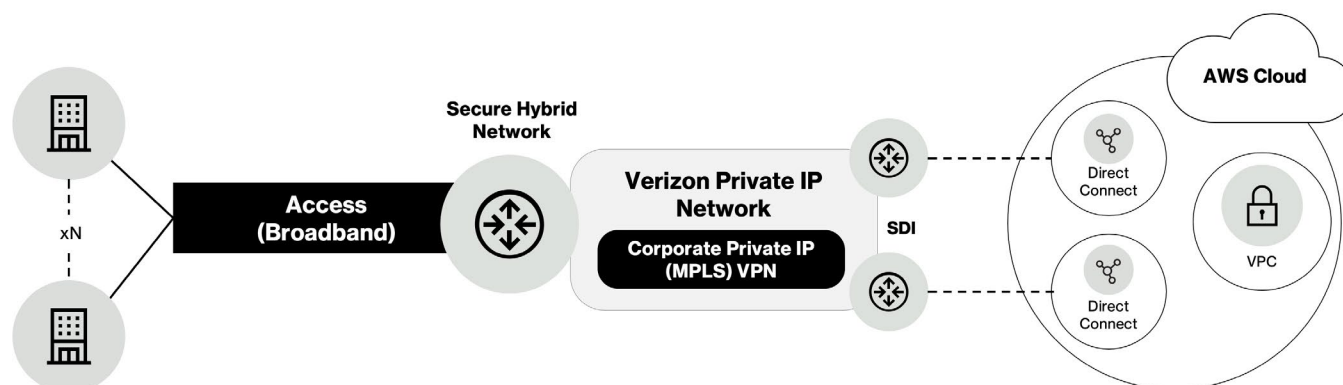
3. Understanding the Data Egress Cost

Almost all CSPs don't charge their customers for data that is transferred to the cloud (i.e., "ingress data"). On the other hand, the CSPs charge their customers for the data they transfer out from the cloud (i.e., egress data). These charges can vary depending on the amount of data being transmitted, the CSP region or geographic location used, whether an Internet or a private connection is used and other factors. Egress charges can become significant if the enterprise users are accessing a lot of data from the cloud.

One of the key factors impacting that cost is the type of connection being used: an Internet-based connection or a private-based one. Examples of private-based connections would be AWS Direct Connect, Azure Express Route or Google Partner Interconnect. If we consider the AWS example, for the US East 1 region, AWS charges can be as high as $0.09[1] per GigaByte (GB) for egress traffic over the Internet but only $0.02 per GB on a Direct Connect connection (https://calculator.aws/#/addService/DirectConnect). As a result, there can be considerable savings that can be achieved if an enterprise uses private connections versus the Internet when the egress data volume is high.

4. Cost Comparison Analysis

In this paper, we are comparing the egress fees associated with AWS[2], using the following two network alternatives:

• IPSec tunnels over the Internet, using AWS Internet Gateway

• Direct Connect with a Private WAN (Verizon's Secure Hybrid Network + Software Defined Interconnect using an AWS private connection)

4.1 Internet Gateway

With Internet Gateway (IGW), AWS egress charges are dependent on the AWS Region used as well as the amount of egress traffic. The egress cost per GB decreases as the amount of egress data increases. We will refer to this cost as C_Internet which is calculated as:

C_Internet = Egress Data in GB x Egress charges in USD per GB

The Cost of the Internet option is equal to the cost of egress data in GB times the cost per GB over the IGW.

AWS provides a calculator that facilitates the calculation of egress cost based on the expected egress traffic (https://calculator. aws/#/addService/VPC).

4.2 Private Connection

The cost of a private connection involves two components: (i) AWS charges for the private connection plus egress traffic and (ii) the private WAN connection.

For the private WAN, we are proposing to use Verizon Secure Hybrid Network service to provide the connection to the remote offices and Verizon Software Defined Interconnect to connect the WAN to the cloud. Both Secure Hybrid Network and Software Defined Interconnect have port charges per connection. The number of Secure Hybrid Network ports is dependent on the number of remote locations to connect and its cost is dependent on the port speed (Mbits/s). The number of Software Defined Interconnect ports is also dependent on the number of connections to the cloud and are also charged on the port speed (Mbit/s). For our comparison, we assumed a combination of port number and port speed that can accommodate the amount of the egress traffic from the cloud (i.e., 10 TeraBytes(TB) to 500 TB).

We will refer to this cost as C_private and is calculated as:

C_Private = C_PrivateWAN+C_AWSDirectConnect

C_PrivateWAN = [Cost of private network (Secure Hybrid Network+Software Defined Interconnect)]. Both Secure Hybrid Network and Software Defined Interconnect charges are based on port speed and not traffic usage.

C_AWSDirectConnect= C_PortSpeed+C_EgressTraffic

C_EgressTraffic= Egress Data in GB x 0.02 USD per GB

This is shown in the diagram below using AWS as the CSP.
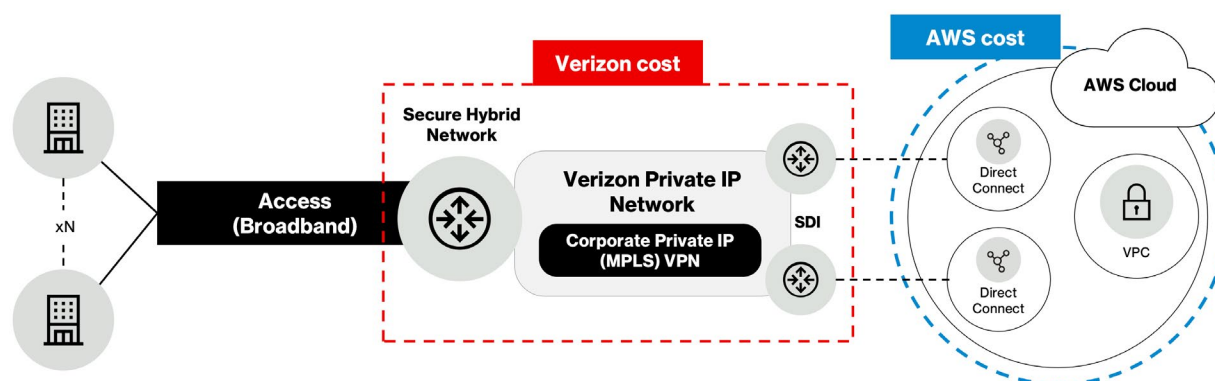
The pricing for AWS component was taken from their publicly available calculators and price lists (https://calculator.aws/#/addService/DirectConnect) and is subject to change. For all the calculations we picked the cheapest AWS region which at this time is US-east-1
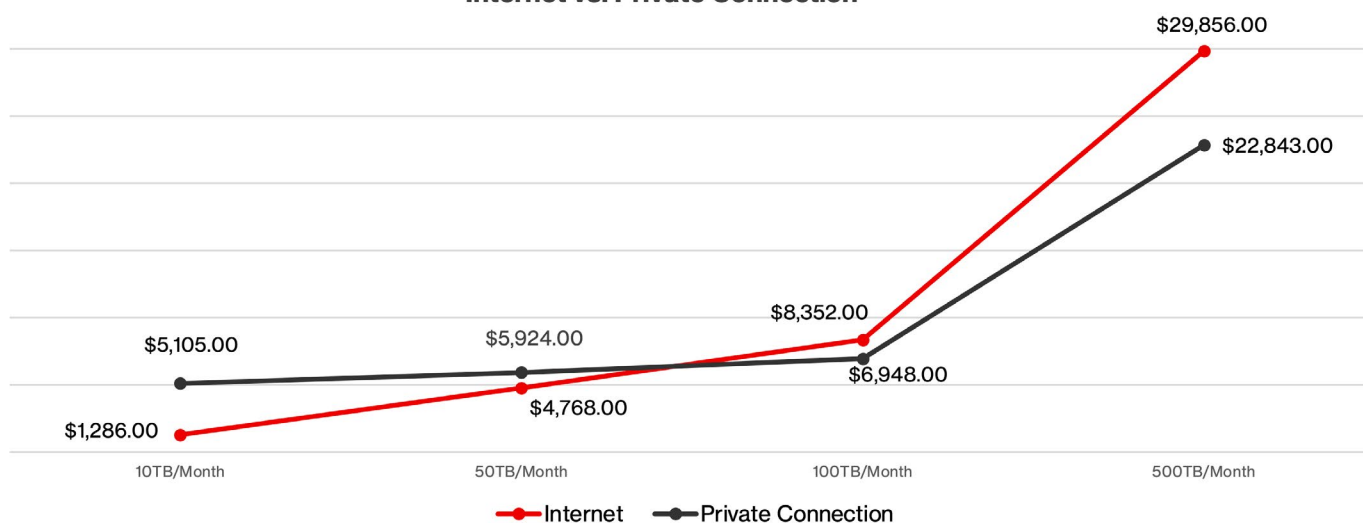
4.3 Cost Comparison

We wanted to compare the cost of the two networking options to determine when

C_Internet > C_Private

We estimated the monthly cost for both options for egress traffic between 10 TB to 500 TB. The results are reflected in the graph below.

AWS Egress charges
Internet vs. Private Connection

Chart values:
- 10TB/Month: Private Connection $5,105.00; Internet $1,286.00
- 50TB/Month: Private Connection $5,924.00; Internet $4,768.00
- 100TB/Month: Internet $8,352.00; Private Connection $6,948.00
- 500TB/Month: Internet $29,856.00; Private Connection $22,843.00

Legend: Internet — Private Connection

As reflected in the table, the better alternative is dependent on the amount of egress traffic. When that amount is relatively small, the Internet option may be cheaper. However, as the amount of egress traffic increases, the private alternative becomes more appealing. The actual breakpoint is dependent on the actual network configuration, CSP and region used, special pricing enterprises have, etc., However, the calculations indicate that in the range of approximately 50 TB, using a private connection starts to become more attractive then the public Internet. There are also other advantages, including performance and security, that a private network will provide.

5. Summary

As you consider the alternatives to connect your remote users to applications hosted in the cloud, it is imperative that you pay attention to the amount of egress traffic from the cloud that the application will generate. Based on that amount, a combination of Verizon Secure Hybrid Network with a private cloud connection such as Verizon Software Defined Interconnect might be financially more attractive, owing to the difference in the cost of egress traffic over the Internet versus over the Private gateway. Ignoring that factor might result in a design where the cost of the connections themselves may be cheaper over the Internet but, when the cost of the egress traffic is added, the total cost of an Internet-based solution will be greater than a Private network based one.

Contact Us

If you have any questions or need additional support with your specific design, please email to us on tech-expert@verizon.com.

Appendix A: Verizon Secure Hybrid Network

Secure Hybrid Network combines the cost and availability benefits of the public Internet with the consistency of performance and security offered with private networking.

Secure Hybrid Network allows the enterprises to use public/Internet access as the last mile to connect to Verizon's Secure Hybrid Network PoP securely and access the Verizon private backbone via broadband. With Secure Hybrid Network PoPs present globally in a distributed high availability manner, it allows enterprises to connect to Verizon MPLS network in a secure fashion enabling access to enterprise VPNs. The benefits of Verizon's MPLS backbone include: dedicated bandwidth, comprehensive SLAs, prioritization of critical traffic, and secure, non-public traffic.
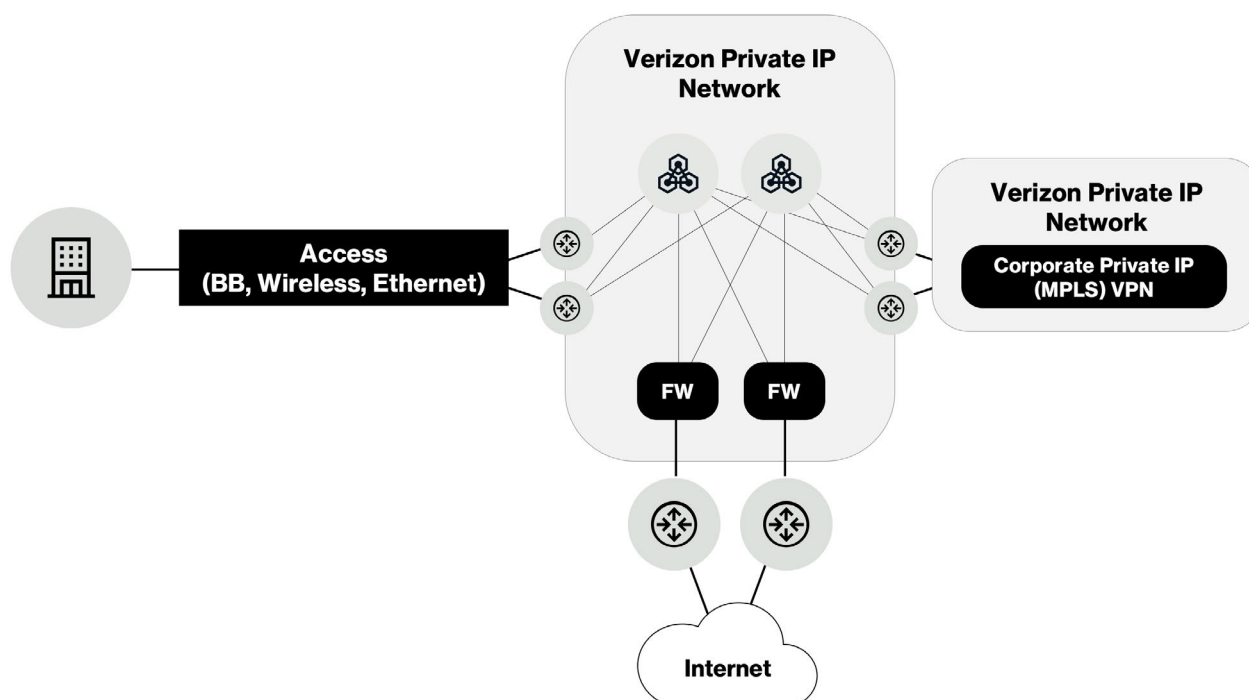

Secure Hybrid Network allows enterprises to have different port speeds from 3Mbps to 1Gbps.

https://www.verizon.com/business/products/networks/connectivity/hybrid-network-solutions/

Appendix B: Software Defined Interconnect

With Software Defined Interconnect, Verizon has deployed two physical L2/L3 capable devices at a number of Equinix data centers across the globe. Direct 10 Gbit/s (and in some locations 100 Gbit/s) cross connects are then configured between those devices and Equinix Fabric (primary and secondary Fabric for redundancy). Verizon can then extend our Layer 2 and Layer 3 network to any other CSP (or customer CPE) that is connected to the Equinix Fabric.
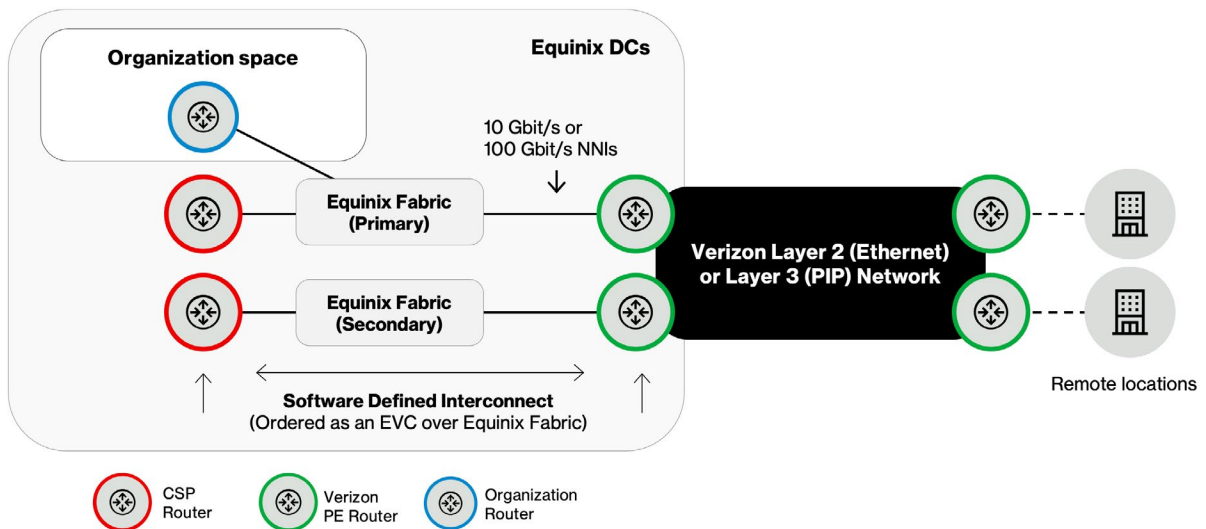
When an organization wants to connect to a CSP with Software Defined Interconnect, a Software Defined Interconnect access is (software) configured on the Verizon colocated devices and is then attached to the user Private IP VPN (when the Layer 3 option is used) or to the user ELINE or ELAN EVC (when the Layer 2 option is used) on one side and to the CSP routers on the other side.

When the Layer 3 option is used, Verizon will then manage the Border Gateway Protocol (BGP) session between the Software Defined Interconnect access and the CSP. The logical Software Defined Interconnect access is then used to route traffic between the two entities.

When the Layer 2 option is used, Verizon then provides only a medium to connect the organization routers to the CSP routers and it is the organization's responsibility to initiate and manage the BGP session with the CSP routers.

Software Defined Interconnect access characteristics are:

- It is supported with both Verizon Private IP (Layer 3 VPN) and ELINE/ELAN (Layer 2 VPN) services.
- Software Defined Interconnect access is configured on a single Verizon device. However,two devices are available at each peering point so two diverse Software Defined Interconnect accesses can be ordered.
- It is a speed-based service (i.e., organizations are charged for the amount of Mbit/s they ordered).
- It can be bundled with Verizon hosted firewall and SD WAN services.
- It is supported by Verizon industry leading Private IP SLAs and QoS.
- User traffic is provided with a committed information rate (CIR)) and is policed to the ordered speed.
- It is available in the U.S. and internationally.

https://www.verizon.com/business/verizonpartnersolutions/products/cloud/software-defined-interconnect/

verizon✓
business