Private/Public WAN Virtualization Using Ecessa Solutions

ECESSA

Worry-Proof Internet
2800 Campus Drive · Suite 140 · Plymouth, MN 55441
Phone (763) 694-9949 · Toll Free (800) 669-6242

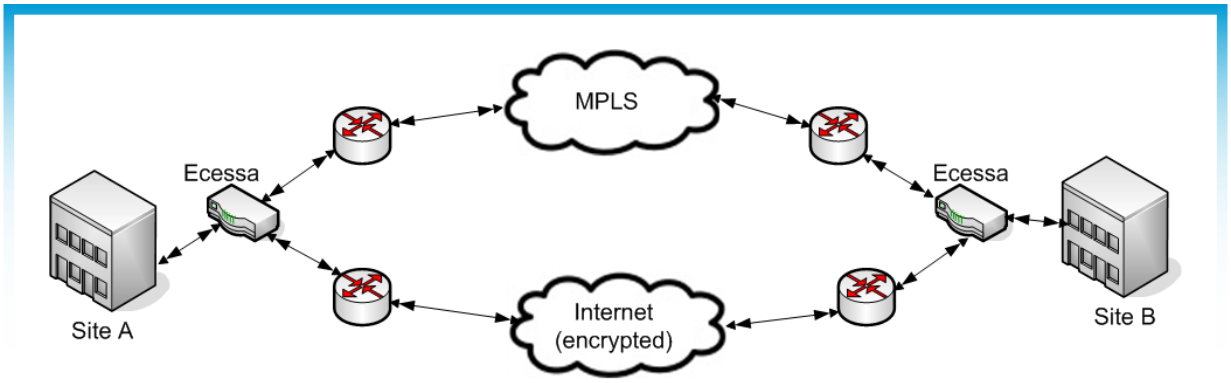
Private/Public WAN Virtualization Using Ecessa Solutions

Many businesses have remote offices spread out both within state lines and out-of-state. Data transfer between these locations is usually critical — sharing resources and in some cases, communications which are a requirement for executing day-to-day business functions. Typical network topologies for these setups include: a "hub and spoke," where a central headquarters site (or sites) support a variety of smaller remote sites, or a mesh setup, where each site communicates with each other.

One of the technologies often employed to facilitate this kind of connectivity is Multiprotocol Label Switching (MPLS). An MPLS network offers a number of benefits; the traffic typically takes a defined, efficient route through the ISP's network thus offering privacy, guaranteed throughput, and typically a low latency. Many ISPs also apply Quality of Service (QoS) to specific types of traffic throughout the network, providing the best performance possible to sensitive traffic types (VOIP, Citrix, etc.). However, utilizing an MPLS network can be expensive for the amount of bandwidth offered and it can also present a single point of failure. While the routes between sites may be self-healing within the ISP's cloud, connection disruptions at any one of these sites – especially an HQ site – could be disastrous.

There are a few options to address the issue of redundancy. One option is to set up multiple MPLS connections using diverse physical connectivity at each site. However, the expense involved often makes such an option unfeasible for many small and medium-sized businesses. Another option is to fail the traffic over to a site-to-site VPN over a backup using a less expensive public Internet connection at each site in the event MPLS connectivity is lost. While this works in a pinch, it can be very disruptive. Additionally, it may result in paying for a backup connection which sits unused unless an emergency occurs. Some network administrators will alleviate the second issue by statically routing specific traffic types over the backup line continuously (utilizing some of the bandwidth of this spare service), however this can be difficult to properly configure and is not necessarily making use of the bandwidth efficiently, and failover is still disruptive and messy.

Ecessa's solutions address these challenges, providing a seamless failover and efficiently utilizing the bandwidth while giving administrators a high level of control over the traffic to address their specific needs. With Ecessa's WAN Virtualization functionality, testing is constantly performed between the sites over the various paths, allowing an outage to be detected instantaneously. Traffic is then re-routed automatically over any remaining paths between the locations. Over public circuits, this traffic is encapsulated and encrypted (for security purposes), and then de-encapsulated and de-encrypted at the other end. The traffic would then appear exactly as if it had gone over the MPLS path… the nature of the session is not changed, and the disruption is minimal. Specific traffic can be configured to take a preferred path by default (latency sensitive traffic might be sent over the MPLS to take advantage of the benefits outlined above) but otherwise the default behavior would be to intelligently load-balance the traffic on a per-packet basis over the multiple WAN connections, thus making efficient use of all the available bandwidth between the locations.



Additionally, Ecessa's solutions have the option of duplicating specific traffic types over multiple connections. With this functionality enabled for a particular type of traffic, each packet is sent over multiple connections simultaneously – the appliance at the other end simply accepts the first packet to arrive and then discards any duplicates. This creates an even more seamless level of failover (there is no disruption at all if a connection goes down), and can potentially optimize performance for latency-sensitive traffic types. Since the other end always accepts the first packet to arrive, the best path is always achieved. The downside to this approach however, is that obviously there is no load-balancing for the duplicated traffic types – indeed, the bandwidth is used on each line – so Ecessa's solutions allow users to be very specific about which approach (load-balanced, single path with failover, or duplicated) to take with each traffic type.

The benefits of these functionalities are considerable. MPLS connections can be expensive, and it might not be feasible to have redundant MPLS connections to ensure uptime. Also, the ability to supplement MPLS connectivity with less expensive public broadband connectivity can offer not only peace of mind but easier access to more bandwidth as required. The ability to control the traffic on many levels can help to ensure the highest quality levels possible for critical traffic between locations. Ecessa's site-to-site WAN Virtualization functionality allows businesses to achieve the necessary uptime and performance levels without breaking the bank.