VPN (IPsec) Services

Solution Brief

Overview

To support hybrid cloud and extended data center environments, KEMP LoadMaster implements IPsec VPN tunnels to secure and route traffic to remote locations. This capability supports a number of operational scenarios such as dynamic scaling via 'cloud bursting' and application delivery from multiple data centers. IPsec is an industry standard and is offered as a secure connectivity option on cloud services from Microsoft, Amazon and Google. IPsec is also available on server platforms such as Windows and Linux and also on network routing appliances..

Example Scenario - Cloud bursting to Microsoft Azure

Cloud bursting allows organizations to dynamically scale applications by utilizing resources on cloud services that can be brought in and out of service as required to complement the on-premise application capacity. In the following cloud bursting environment, the application virtual service on LoadMaster is configured to forward traffic both to local servers and to servers located in the Microsoft Azure Cloud so that the application workload can be balanced between on-premise and cloud.

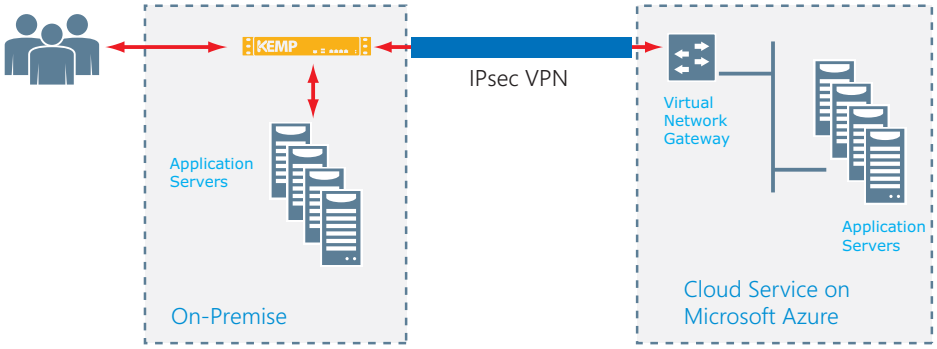

Figure 1- LoadMaster to Azure VPN topology

Under a light workload, the servers in the Azure cloud are turned off and the LoadMaster will not forward any traffic to these servers. When the traffic load increases, the Azure servers can be spun up and once operational, the LoadMaster will balance the workload across local and Azure servers. The IPsec VPN provides secure routing of traffic to any host in the connected Azure 'Cloud Service'.

VPN (IPSec) services are included in all LoadMaster load balancers and VPN connections are easily configured via the web management interface. LoadMaster includes diagnostic logs to troubleshoot VPN connectivity issues while the packet trace facility can capture VPN traffic (IKE, AH, ESP) for more in-depth diagnostics.