Programmable Network

Use Case: Secure Internet Access

A secure, scalable and cost-efficient pathway to cloud

Traditional approach to networking

Many enterprises that rely on traditional networking use private connectivity from their branch to the head office, which requires them to maintain a private network. However, a direct internet connection may be a more efficient solution and represent a better use of their network investment.

Under a traditional networking approach, traffic flows from the customer site to the data centre, where it is then directed to the Internet. The network is protected with security policies applied at a single point, to ensure traffic is secure and to prevent cyber-attacks.

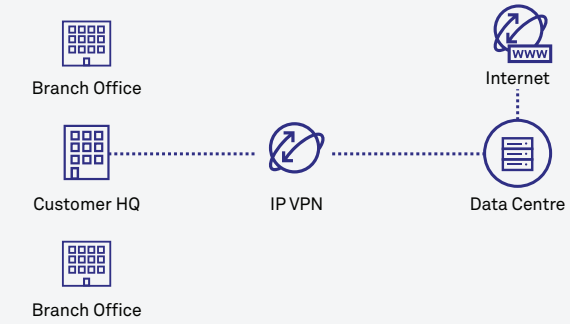

Figure 1: Current WAN setup to the Internet

Current limitations

Enterprises that set up their own connectivity have to find a data centre to host their networking equipment, use lengthy procurement processes to order hardware such as routers and firewalls, and arrange for manual installation and provisioning.

Once set up, subsequent changes require a lot of time to implement, with limited access to the data centre facility, and the request access having to conform with the data centre security policy. This makes maintenance or troubleshooting difficult.

What can the Programmable Network do?

With Telstra's Programmable Network, enterprises can connect securely to the Internet from a NextIP/IPVPN service in near real time, while paying only for what they use.

The Programmable Network allows you to securely connect your WAN to the Internet through the use of network function virtualisation (NFV).

Virtual network functions such as virtual routers and virtual firewalls will be deployed to replace physical hardware, with a choice of vendors available on the Programmable Network portal.

The virtual firewall blocks unauthorised traffic from the Internet and secures the organisation's WAN.

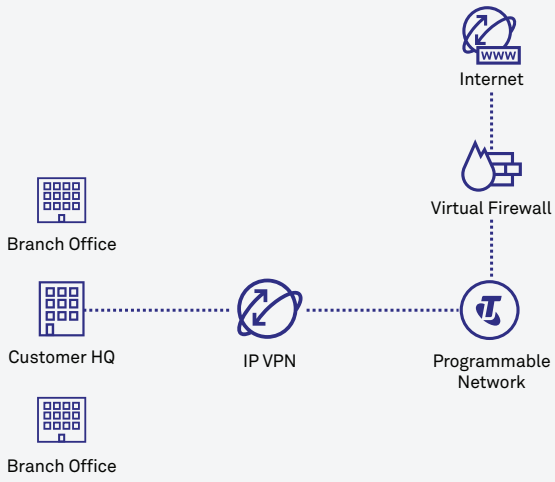

Figure 2: Breakout to the Internet via the Programmable Network

Outcomes

No need for data centre space or hardware

As there is no physical hardware deployed by the organisation, no data centre hosting space is required.

Operating expenses instead of capital expenses

There will not be any depreciation or amortisation of physical assets due to their virtual nature. Instead of a hefty upfront CAPEX to procure network services, organisations will shift to an OPEX model, paying only for the bandwidth they use.

More control

Maintenance and modifications to network functions can be performed through an online portal in near real time, doing away with the need to implement changes physically at the data centre. New patches can be done remotely to keep the software updated.

Speed of deployment

Deployment of the virtual network functions can take place within minutes, reducing provisioning time.

Telstra

Contact your Telstra account representative for more details.

Australia

1300 telstra (1300 835 787)

telstra.com/enterprisesecurity

International

Channel Partners partners@team.telstra.com

Sales tg_sales@team.telstra.com