Telefónica Tech

The challenges of *traditional* networks in a *digital* business environment

Challenges of the traditional paradigm

Prior to the proliferation of Public Cloud, the traditional network architecture supported the hosting of workloads in a providers' data centre. Traffic was typically routed over MPLS networks and firewalled at a central breakout. As customers move workloads to Public Cloud and SaaS, these architectures are inherently secure, but inflexible and inefficient.

The network design needs to adapt to the new customer strategies of "Cloud First" and "Internet First".

Companies transforming their IT to Cloud are recognising these challenges:

1

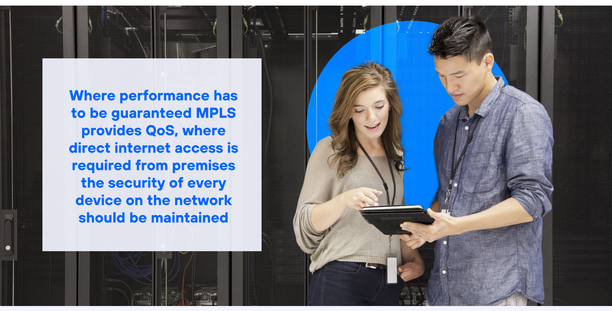
Lack of flexibility: Networks are increasingly heterogeneous and dynamic, for example the need to connect directly between cloud instances and support mobility and SaaS.

2

Lack of visibility and management: The traditional network router offers limited control capabilities, no pro-active visibility of possible security threats or incidents, and no measurement of performance metrics.

3

Lack of customisation and integration between networking and security, which is complicated exponentially by multi-cloud deployments.



Where performance has to be guaranteed MPLS provides QoS, where direct internet access is required from premises the security of every device on the network should be maintained

New *hybrid* architectures

To address the challenges of traditional networks the enterprise network has to transform. The edge device needs to recognise the application in order to replace the static route with policy-based decisions and enable insightful reporting. The management domain needs to extend into the Public Cloud and to all the end user devices, reporting on the extended network edge without compromise.

The price of bandwidth to premises has been falling for several years, driven by increased competition and the proliferation of new transmission technologies.

SDWAN technology allows multiple interfaces to be used at any time.

With secondary and tertiary connections no longer passive; more bandwidth becomes available without increasing the op-ex.

Customers want to connect to the new hybrid network now, to take immediate advantage of the benefits that new technology can bring without waiting for incumbent contracts to expire or approval of capital expenditure. This requires a brown-field approach to the transformation.

Evolving to *secure* network architectures

Manufacturers' edge devices should offer granular licenses for both hardware and virtual appliances, that are reportable and integration-ready through open APIs. Performance of security and networking in the core and at the edge should be visible and reportable from the same platform, irrespective of the device format.

Network providers need to enable the customers' evolution to new architectures and Software-Defined Networking by delivering solutions which converge advanced networking and cyber security capabilities.

Edge devices need to be capable of enabling the transformation between connectivity technologies and adapting to the SaaS and Public Cloud models.

To enable secure mobility, end-user devices should be protected from threats on and off the corporate LAN with the same set of policies. Any suspicious activity on a device should initiate a quarantine of that device pending investigation and sandboxing.

Telefónica Tech