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:

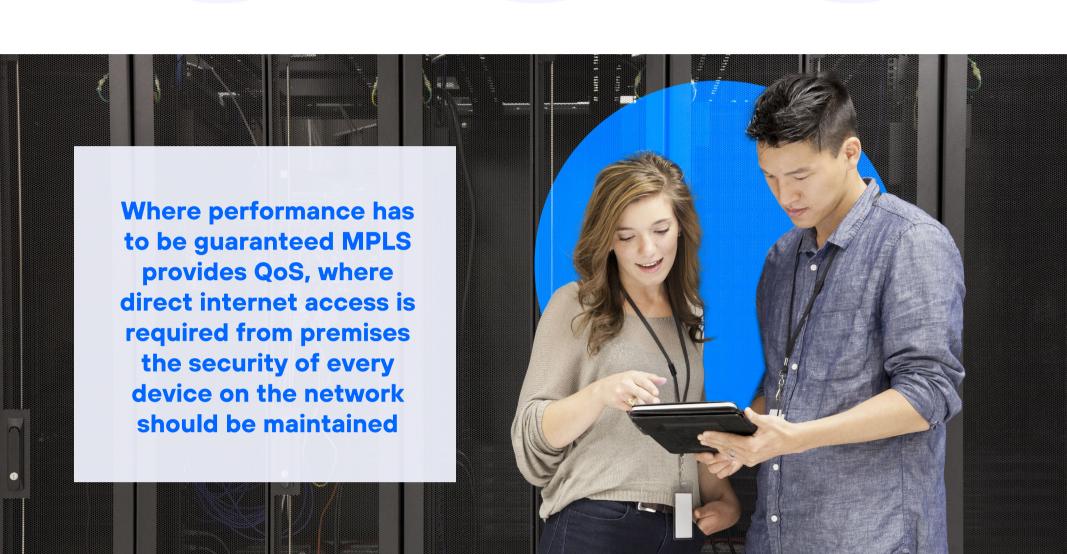
Lack of flexibility:

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

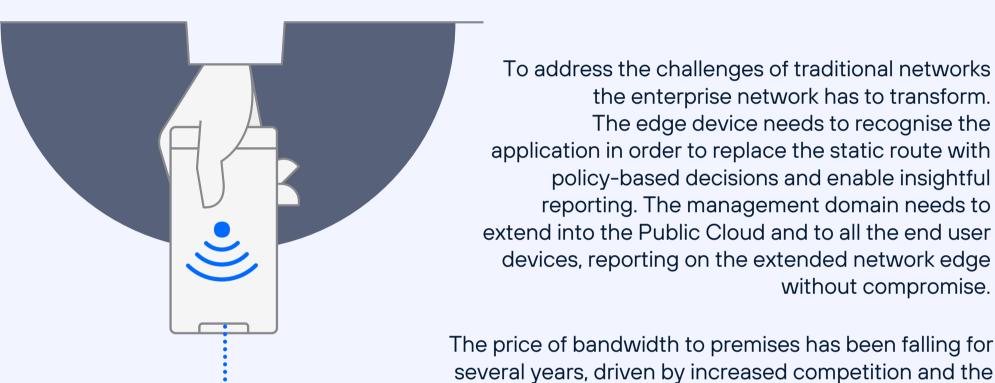
Lack of visibility and management:

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

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



New hybrid architectures

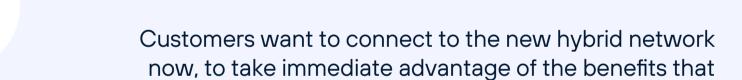


The edge device needs to recognise the application in order to replace the static route with policy-based decisions and enable insightful reporting. The management domain needs to extend into the Public Cloud and to all the end user devices, reporting on the extended network edge without compromise. The price of bandwidth to premises has been falling for

To address the challenges of traditional networks

the enterprise network has to transform.

proliferation of new transmission technologies. SDWAN technology allows multiple interfaces to be used at any time.



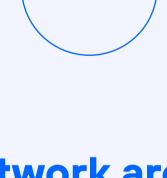
With secondary and tertiary connections no longer passive; more

bandwidth becomes available without increasing the op-ex.

incumbent contracts to expire or approval of capital expenditure. This requires a brown-field approach to the transformation.

new technology can bring without waiting for







Manufacturers' edge devices should offer granular licenses for both hardware and virtual appliances, that are reportable and integration-ready through open APIs. Performance of

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

security and networking in the core and at the edge should

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.

Group) are registered trademarks. Telefónica Tech and its subsidiaries reserve all rights therein.

2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. All rights reserved. The information contained herein is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. (hereinafter "Telefónica Tech") and/or any other entity within the Telefónica Group or its licensors. Telefónica Tech and/or any Telefónica Group company or Telefónica Tech's licensors reserve all intellectual property rights (including any patents or copyrights) arising out of or relating to this document, including the rights to design, produce, reproduce, use and sell this document, except to the extent that such rights are expressly granted to third parties in writing. The information contained in this document may be subject to change at any time without prior notice. The information contained in this document may not be copied in whole or in part, distributed, adapted or reproduced in any form without the prior written consent of Telefónica Tech. The sole purpose of this document is to support the reader in the use of the product or service described herein. The reader agrees and undertakes to use the information contained herein for the reader's own use and not for any other use. Telefónica Tech shall not be liable for any loss or damage arising from the use of the information contained herein or for any errors or omissions in the document or for the incorrect use of the service or product. Use of the product or service described herein shall be

governed by the terms and conditions accepted by the user of this document for use. Telefónica Tech and its brands (as well as any brand belonging to the Telefónica

You can read our privacy policy here