Telefónica Tech

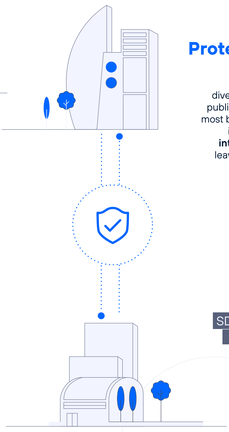
Steps to *connect* and *secure* an enterprise network

With application-aware devices at each network edge and an insightful Management platform, SD-WAN technology makes it possible to offer a much more flexible, dynamic and manageable WAN and creates new network architectures.

Connecting every edge device directly to the internet makes efficient use of bandwidth and introduces substantial improvements to the user experience.

However, with this broader attack surface, companies need to show improvements in network security mechanisms in order to keep the network protected.

To converge cyber security into the SD-WAN network solution customers should consider the following guidelines:



01

Protect inter-branch traffic:

An SD-WAN network may use multiple and diverse transport media, often accessing links to public networks such as the Internet and 5G. The most basic level of security in an SD-WAN solution is one **that ensures the confidentiality and integrity of inter-site traffic** - the information leaving each site must be encrypted so that it is not vulnerable to interception.

02

Protect direct access to the internet:

SD-WAN solutions enable efficient use of low-cost (i.e. internet) bandwidth.

This creates new points of vulnerability to cyber-attacks and requires each site to have security protection in place.

03

Enable secure communication with the public cloud:

Access to applications and services hosted in the Public Cloud must be encrypted to the same standard as traffic on physical networks.

In this way, communication with the Public Cloud will be protected through the SD-WAN.

04

Consider internal segmentation:

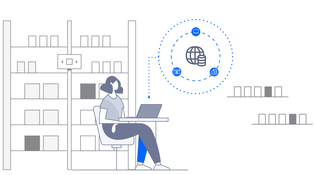
Within each site, it is important to keep traffic segmented, so that there is a secure "air gap" between the user network and hosted services. This will help to ensure that if a compromised user device enters the network, it is not able to propagate the attack to services on the network.

05

Ensure centralised visibility and management:

Without a management platform, controlling each site's SDWAN is unmanageable. A unified platform ensures consistency between site configurations and

makes it easier to detect vulnerabilities and incidents.



06

Ensure convergence between SD-WAN and cyber security:

Check that the SD-WAN service and cyber security functionalities are fully converged and not simply integrated.

Expert life-cycle analysis of the consistency of configurations and policies of both network and security technologies

will be key to ensuring that the enterprise network is protected from vulnerabilities. In addition, being able to correlate SD-WAN and security incidents speeds up identification and resolution.

"To facilitate this journey, vendors offer solutions to connect, secure and manage the enterprise network through a single service, offering converged SD-WAN technologies with cyber security features.

Designed and managed by expert teams to ensure policy consistency between the two solutions."

Telefónica Tech