Publication date:
24 Feb 2023
Author:
Pablo Tomasi,
Principal Analyst, Private Networks and Enterprise 5G

Mobile VPN enables a new **nomadic workforce**

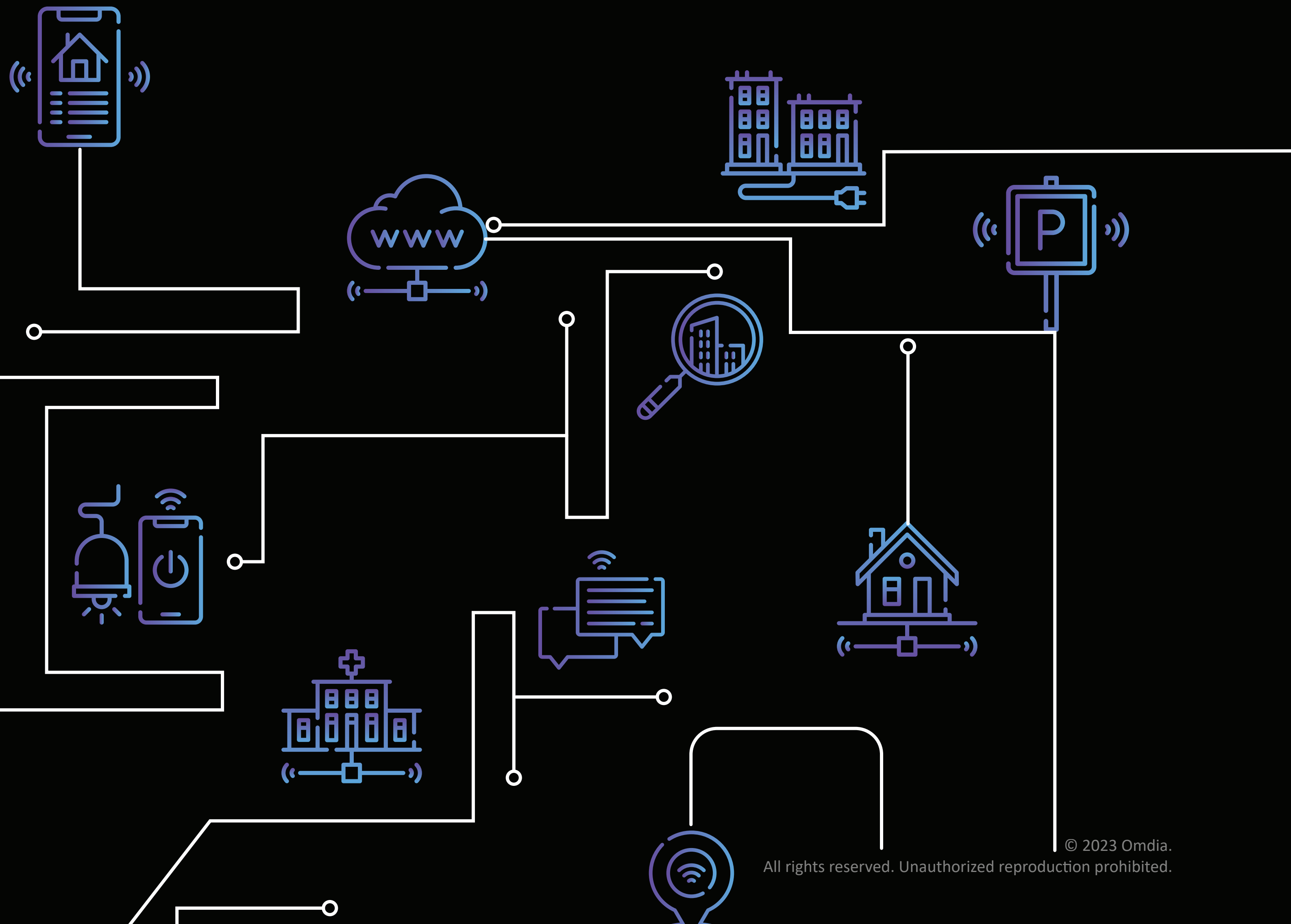
Mobile VPN for Smooth Network Switching and Verticals' Transformation

OMDIA

Commissioned by: HUAWEI

Brought to you by Informa Tech

Contents



Executive summary

The enterprise market has been developing shaped by the needs of supporting a mobile workforce which needs to access both the company’s intranet as well as the internet in a secure and efficient way. Vertical markets such as government, healthcare, and education, as well as enterprises of all sizes, need to provide secure connectivity to their employees, whether they are inside the enterprise campus or outside of it.

The mobile VPN solution is a key application of private 5G as it tackles the enterprise challenges delivering a seamless connectivity for both intranet and internet without the need for manual login or traffic passing through the public internet before reaching the enterprise servers.

Furthermore, it can serve enterprises with different sizes and investment capabilities thanks to different deployment options, including a shared UPF and a dedicated one. The solution has currently been used by customers such as the Zhejiang University, the Shenzhen government, and an enterprise in UAE.

Mobile VPN delivers value to the enterprise by providing an improved experience versus traditional VPN in areas such as security and data throughput, but also in terms of cost saving as the enterprise does not need to incur in operations and maintenance (O&M) costs. From a telecoms operator perspective, mobile VPN enables the carrier to gain new customers, drive the sale of 5G connections and deliver enterprise solutions.

Industry background

Industry developments

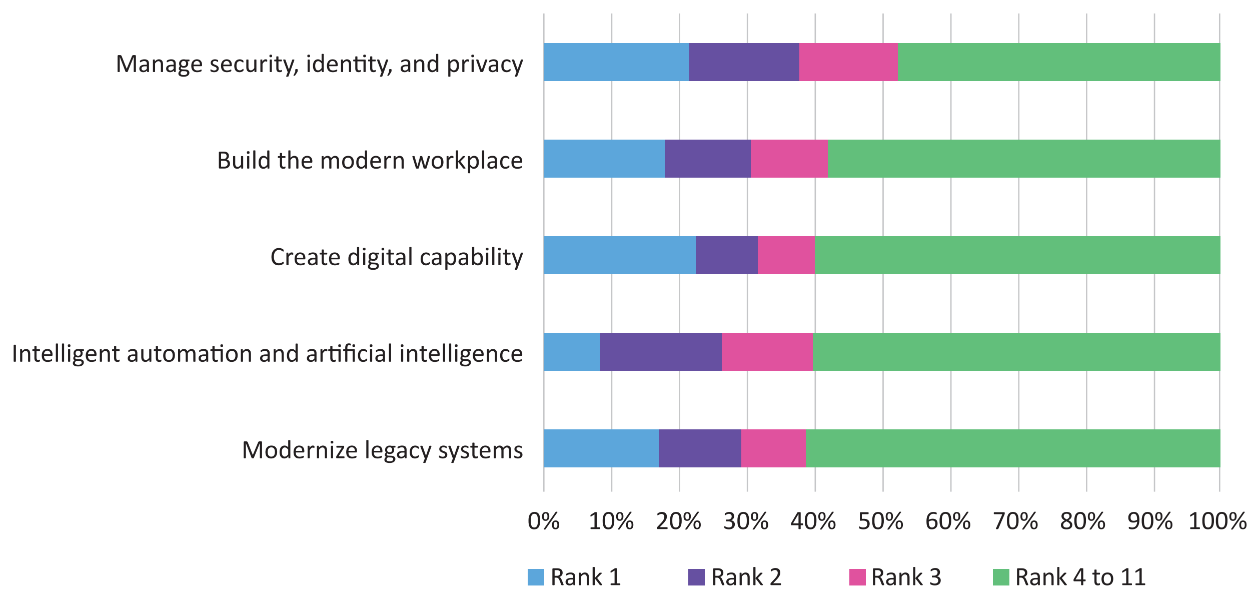
At a glance it would appear that each vertical market is unique from others. For instance, a factory wants to increase production, a port wants to move more containers per hour, and a city wants to improve the user experience. Yet, all these goals which are driving the transformation of industries are based on a set of common underlaying trends.

Key trends consistent across all vertical markets include connecting assets and driving a digital transformation, integrating new transformative technologies, such as AI or AR/VR, into existing solutions, and supporting an increasingly dispersed workforce. Digital transformation—or for specific industries industry 4.0—is about digitizing assets and workforce, in other words securely connecting them while enabling access to intranet resources, as well as supporting new ways of working.

Among all these trends, the common requirements of supporting an ever mobile and dispersed workforce in a secure way is the foundational layer for any enterprise transformation. Enterprises expected to access their intranet and applications securely from their campus network but also more and more often from any dispersed location at any time. According to Omdia's Enterprise 5G Survey 61% of workers connected to 5G are nomadic or hybrid workers showing a clear change in worker habits.

The workforce must be connected securely. According to another survey conducted by Omdia, including a range of different verticals and enterprises of all sizes, when enterprises were asked about their most important technology priorities, they ranked managing security, identity, and privacy as the most important priority for their IT teams. This need shows how a connectivity solution capable of meeting this requirement will be the first priority for any enterprise.

Figure 1: Top 5 IT trends for the enterprise



Notes: n = 4769
Source: IT Enterprise Insights: IT Drivers and Technology Priorities – 2023

Enterprises from all verticals demand access to the internet and intranet dual domain

No enterprise is an isolated island and the digitization of an enterprise and the increase in connected devices and personnel bring the requirement of a secure connection from any location.

The evolution of different industries is shaped by new trends and technologies all requiring larger bandwidth, reliability, and security. For instance, in the healthcare sector, researchers need to access an ever-large number of datasets, and they need to use AI or ML to optimize research or patient monitoring. Security, privacy, and confidentiality is a cornerstone of this vertical. Health experts need to be increasingly mobile (and therefore connected) to move around different health institutions but also beyond those institutions in the case of remote patient visits or remote consultations. The transport and logistics vertical also have many trends which require a mobile force connected with a secure and reliable connectivity. In a port or airport environment different companies working there need to be connected securely while moving around the environment for troubleshooting for instance or to support customers and cargos.

Examples of demand for dual connectivity for different verticals:

Education: The education sector has been undergoing a revolution in the way that classes and research is conducted. This was also accelerated by COVID-19 which prompted the need to facilitate secure remote learning and teaching for staff and students. For instance, teachers must be able to connect to use university tools safely and efficiently and to access research and database while being both inside and outside the campus. Students also need to securely connect to online classes as well as having remote access to library resources such as scientific journals.

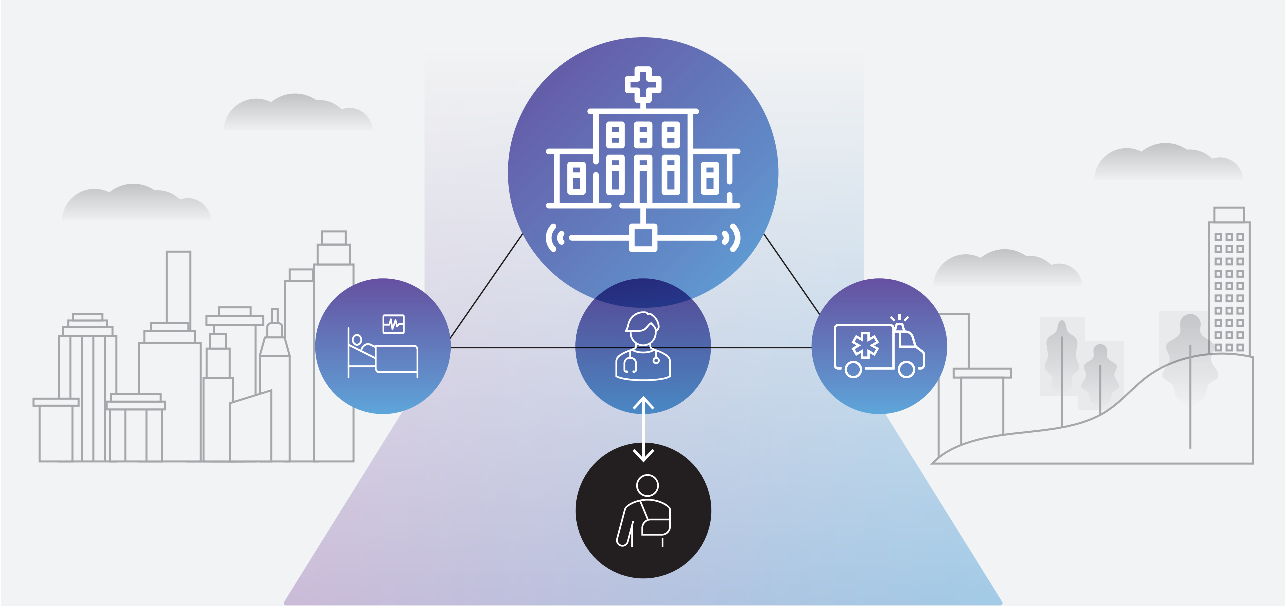
Smart cities: Smart cities including government services are a prime candidate for the use of secure remote dual connectivity. Most public workforce is remote by nature and given the fact they need to connect to city's programs and software, for instance while monitoring city infrastructure, their connection must be secure. Providing public services, uploading or processing city documents, and interacting with video conferencing or even pandemic prevention, are all tasks that the city workforce may need to do from various locations.

Enterprises: Whether an enterprise is from the transport, manufacturing, or other vertical market there is no doubt that remote and nomadic workers are becoming critical to the successful completion of day-to-day jobs. An expert could be working remotely, engaging with a remote team from a different site via a video conferencing, or helping with online engineering process and design simulation and file transfer.

Healthcare: The need to expand and adapt health services to bring healthcare both into more remote or countryside areas, as well as easing access to healthcare for people in urban centers are key priorities for the vertical. This requires a reliable secure connectivity as an essential tool. Doctors may need to conduct remote consultations, including remote video conferencing. Mobile medical devices, as part of mobile health services are of increasing relevance to meet the need of segments of population that because of work habits or living locations may prefer remote care.

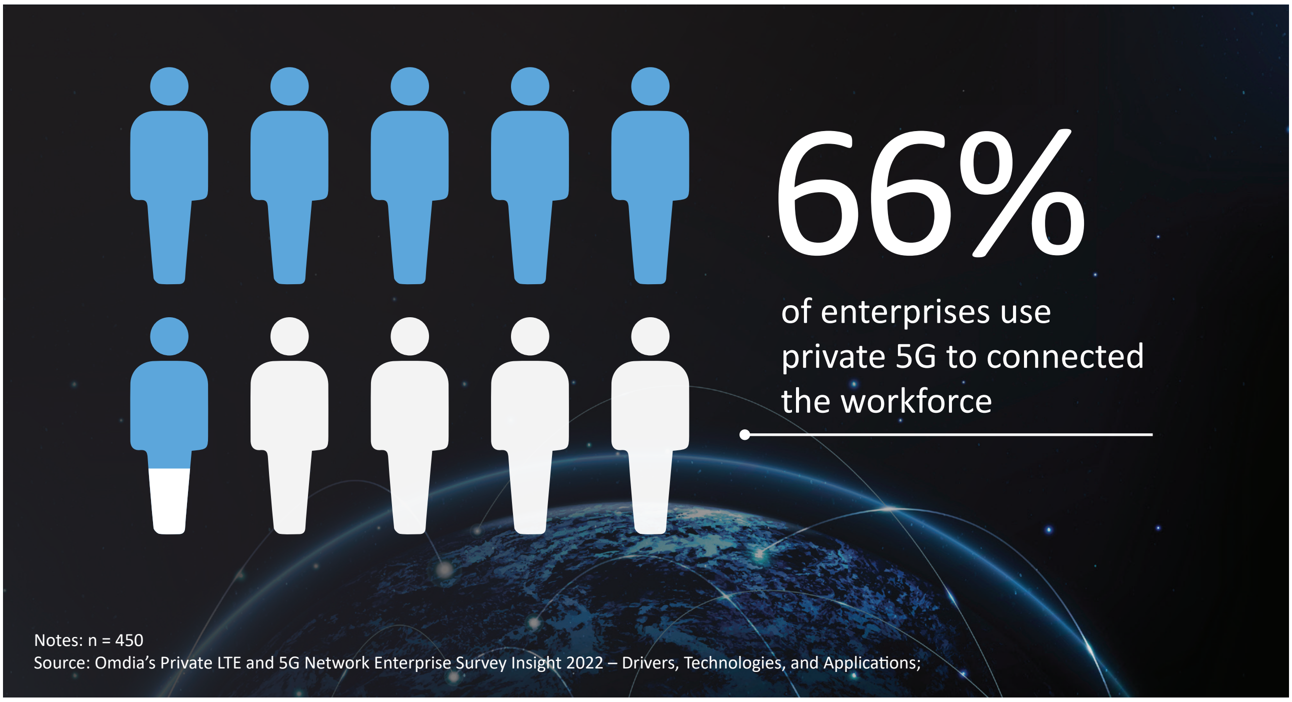
Overall, with many enterprises having multiple sites, or having a workforce that is roaming, for instance, to different customer sites, a simple, secure, and wide coverage connectivity option is needed.

Figure 2: Connectivity needs in healthcare



Mobile VPN introduction: solutions that can address different scenarios

Figure 3: workers are the main asset connected by private 5G



Notes: n = 450
Source: Omdia's Private LTE and 5G Network Enterprise Survey Insight 2022 – Drivers, Technologies, and Applications;

The mobile VPN solution is one of the leading private 5G applications as it addresses the enterprise needs for security and the connected workforce, which are key cornerstone of any enterprise.

Improving workforce productivity is one of the main drivers for many verticals and for instance, according to Omdia's *Private LTE and 5G Network Enterprise Survey Insight 2022 – Drivers, Technologies, and Applications*, this was a key driver for the deployment of a private 5G network for one in every four enterprises in the government sector. Overall, 66% of enterprises use private 5G to connect their workforce.

5G with mobile VPN can deliver a better experience as private 5G connectivity's reliability, quality of service (43%), and security and privacy (42%) were identified by respondents as the main advantages of a private 5G network versus other technologies.

Mobile VPN has two architectural options that make the solution adapted to different customer requirements. It is also a solution that can run on both a 4G and 5G converged network, and this is a critical feature as some countries are still in the first phase of their 5G journey. Significantly, compared to existing legacy VPN solutions, mobile VPN is more secure as the data does not go through the open internet before reaching the enterprise servers but is transmitted only on the carrier's transport network.

From an architectural point of view, the solution can be delivered leveraging an on-premises UPF architecture, or a shared UPF architecture. Details on the two architectural options are provided below.

Mobile VPN service scenario

1. **The users access the service within a city.**

Details: Any user who is inside the campus can directly access the intranet though the campus private network. The identification of the user information is done in the edge UPF which is also integrated with the distributed gateway (DGW). This allows a user inside the campus to directly access the enterprise intranet though the campus private network. However, even in the case when the user is outside of the campus network, he can still securely connect as all the internet data will still be transmitted through the edge UPF. There is continuous indoor and outdoor coverage.

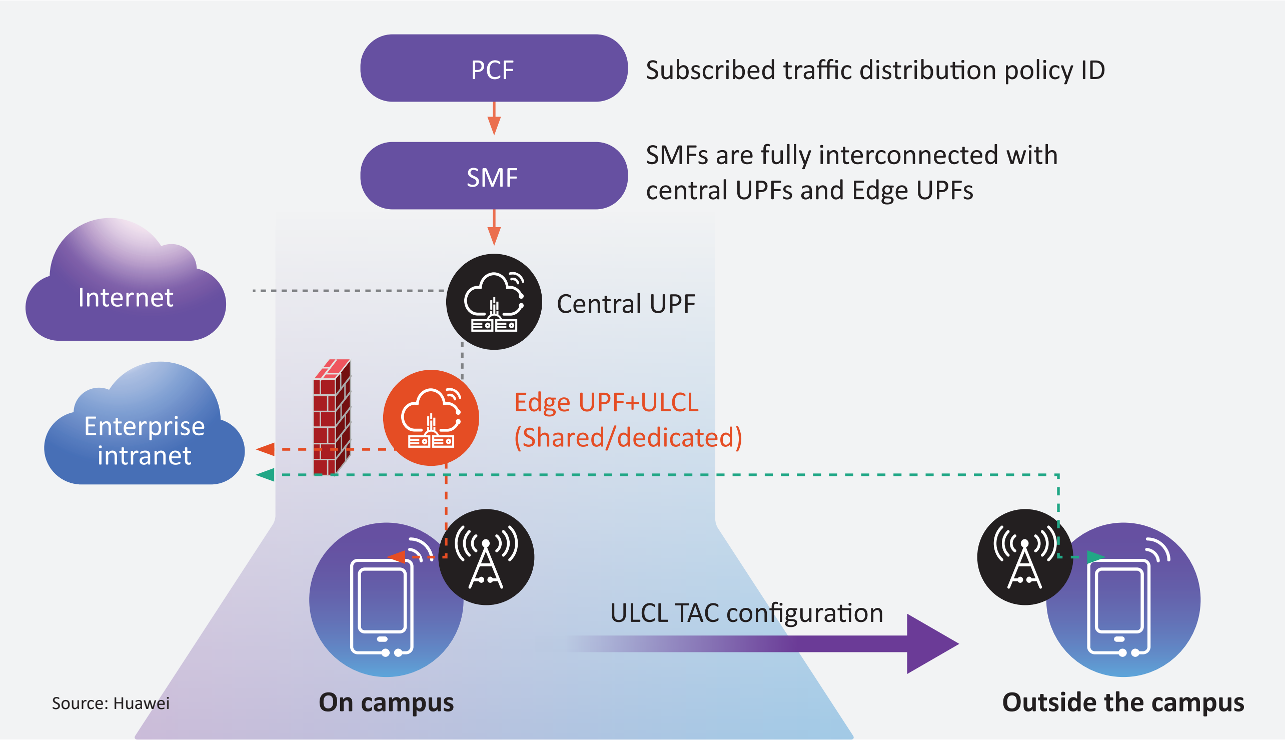
For instance, in this scenario, e-government extranet users leverage a dedicated UPF/MEC which is deployed in the government campus to connect to the e-government extranet. The e-government extranet users' traffic is distributed locally as the dedicated UPF/MEC implements traffic distribution between the campus and internet services. The dedicated UPF/MEC forwards the traffic for accessing e-government services to the e-government extranet while the traffic for accessing the internet, while within the campus, is instead forwarded to the 5G UPF/MEC deployed by the telecom operator for the city.

Since the e-government UPF/MEC can control service access based on user locations when e-government extranet users are outside the campus, they can only access the internet. When they enter the campus, the e-government UPF/MEC identifies service traffic through the ULCL. Therefore, internet services are distributed to the UPF/MEC in the telecom operator's city, and service traffic for accessing the e-government extranet is distributed to the local service server.

Contrarily, when e-government extranet users leave the campus area, the ULCL traffic distribution policy cannot be triggered. Data flows are directly forwarded to the internet through the municipal UPF/MEC, and the e-government extranet cannot be accessed.

Target customers: This is a solution that is ideal for customers such as government entities. For instance, within any government location and in the outside area of a city, it is essential for the worker to be able to freely move (therefore no cable connection can be used) while being securely connected with high bandwidth needed to support video applications. With multiple city workers using the same network while working on different tasks (e.g., transport and road works, e-government, etc.) it is paramount to have a solution that can support large numbers of workers without compromising on quality.

Figure 4: Schematic representation of the Mobile VPN solution


PCF
Subscribed traffic distribution policy ID
SMF
SMFs are fully interconnected with central UPFs and Edge UPFs
Internet
Central UPF
Enterprise intranet
Edge UPF+ULCL (Shared/dedicated)
ULCL TAC configuration
On campus
Outside the campus

Source: Huawei

2. **Roaming scenario**

Details: In this second option for the deployment of the mobile VPN solution the ULCL function is placed in the central UPF. This also allows for the support of international roaming as all the data passes to the central UPF first. Even outside the campus network the connection can pass through the central UPF and then through distributed edge UPF.

A roaming scenario includes for instance, government officials and public servants with office devices, such as mobile phones and tablets, which due to business trip or remote work, need to access both campus services and the internet.

In such a multi-service scenarios where common terminals, such as mobile phones and tablets, used by government users need to access both campus services and the internet, these enterprise requirements can be met by the terminal-side traffic distribution architecture or by the network-side traffic distribution solution. In the first case, the UE identifies service flows on the application side, differentiates services, etc. However, this requires application customization and is dependent on the terminal support.

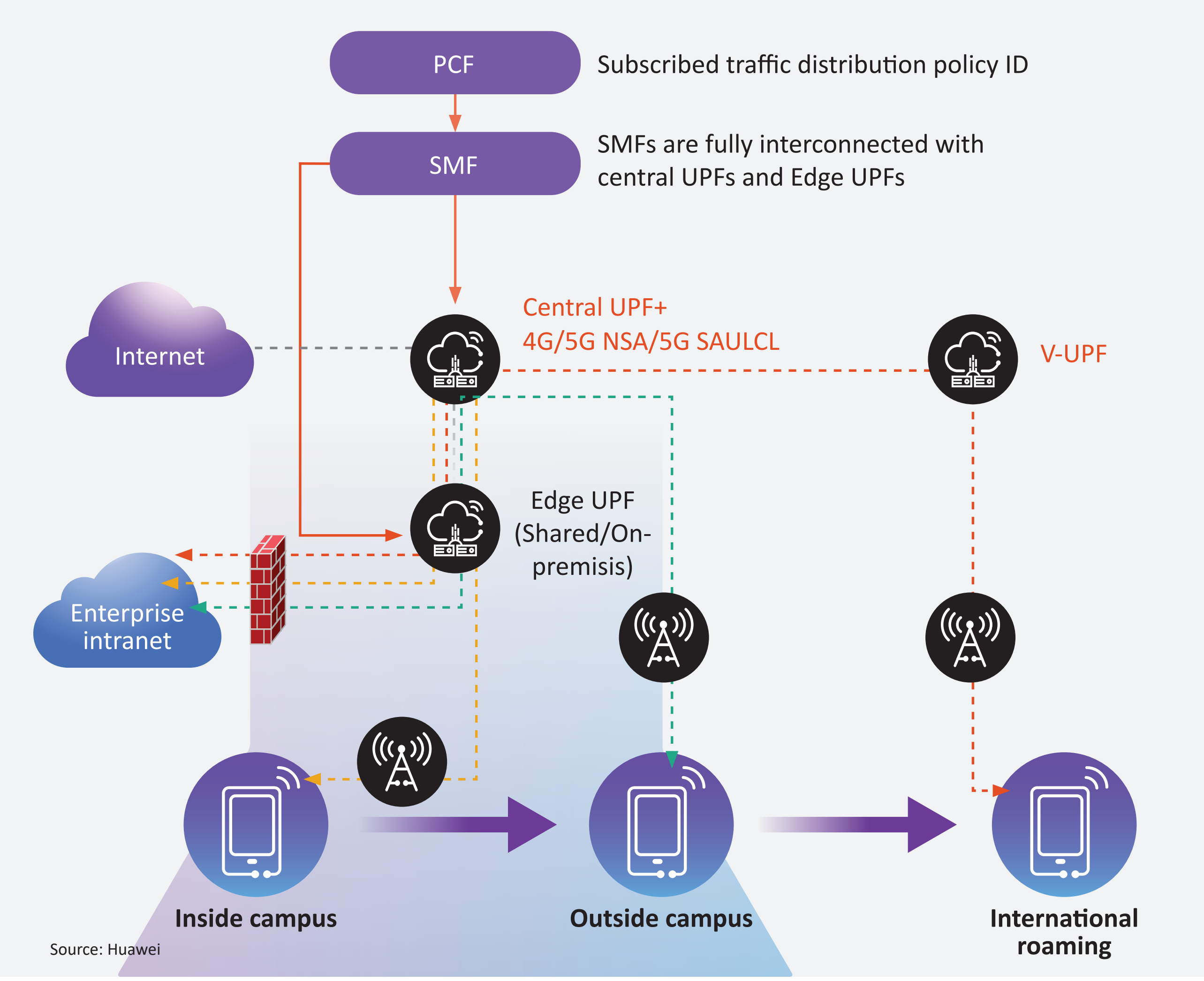
To eliminate the dependency on terminals in multi-service scenarios, the super roaming solution proposes a flexible offloading solution for roaming subscribers on the network side. This solution leaves the complexity to the network thus reduces the complexity in the terminals.

The roaming network side identifies service traffic of e-government subscribers accessing the internet and e-government extranets. The UPF/MEC deployed by the carrier in the roaming network functions as the ULCL anchor point to identify and distribute different service traffic. The traffic that accesses the internet directly accesses the internet in the roaming area. Traffic from accessing the e-government intranet is instead forwarded to the home UPF/MEC, and the home UPF/MEC backhauls the traffic to the UPF/MEC in the campus to implement e-government service access.

The network-side traffic distribution solution directly accesses the internet in the roaming area, implementing local offloading of internet traffic, reducing transmission paths of internet service traffic, and improving user experience when government users access the internet in the roaming area.

Target customer: An enterprise with multiple sites across different regions and potentially different countries is the target type for this solution. A manufacturer with plants across different countries needing to have experts travelling from one site to another for training or troubleshooting purposes is an example of a potential customer.

Figure 5: Mobile VPN schematic representation


PCF
Subscribed traffic distribution policy ID
SMF
SMFs are fully interconnected with central UPFs and Edge UPFs
Internet
Central UPF+
4G/5G NSA/5G SAULCL
V-UPF
Edge UPF (Shared/On-premisis)
Enterprise intranet
Inside campus
Outside campus
International roaming

Source: Huawei

Mobile VPN deployment scenarios

Once the private network has been established the mobile VPN solution can be directly deployed. At this point, the enterprise has two options to choose the preferred mobile VPN solution based on the service scenario that more closely meets its needs and budget.

Exclusive UPF

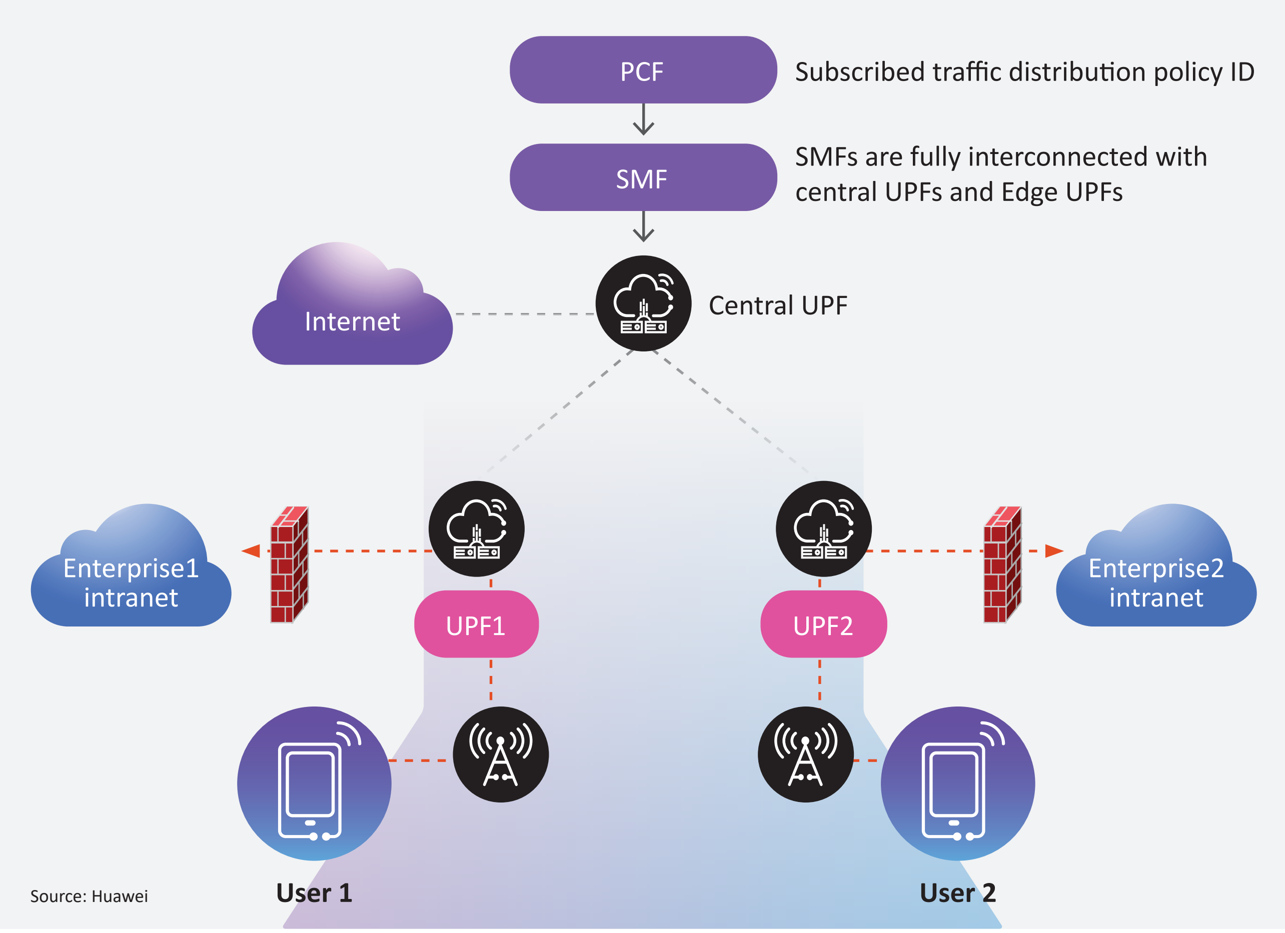
Details:

- Data is more secure and isolated from other enterprise networks.
- Higher reliability: The upgrade and maintenance time of independent UPF devices and software are determined by enterprises, which is not affected by other services, improving service continuity.

- Enterprises can deploy independent UPFs in their own campuses. If the campuses do not have sufficient space, they can also be deployed in carriers' equipment rooms.

Target customers: This deployment option is recommended for customers with large budgets such as large enterprises; it is also recommended for those customers who have higher security needs and therefore by choosing an independent UPF deployment they can obtain a more secure and reliable 5G private network experience.

Figure 6: Mobile VPN deployment with exclusive UPF


PCF
Subscribed traffic distribution policy ID
SMF
SMFs are fully interconnected with central UPFs and Edge UPFs
Internet
Central UPF
Enterprise1 intranet
UPF1
UPF2
Enterprise2 intranet
User 1
User 2

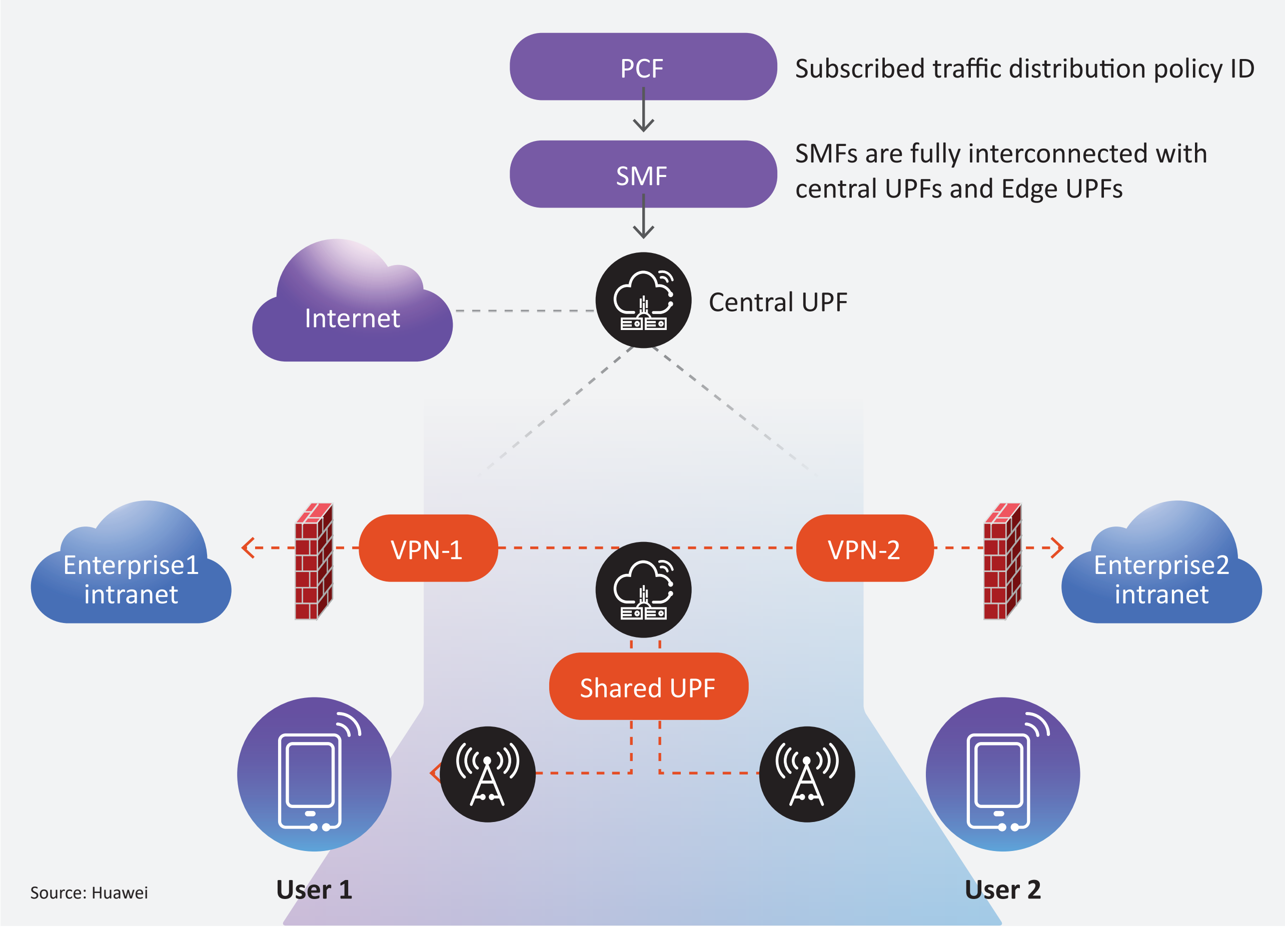
Source: Huawei

Shared UPF

Details: The shared UPF deployment option allows for a less costly private network option as the cost of the UPF is not incurred by the enterprise, since this will be a resource that will be shared with the telecom operator and therefore with other enterprises. The shared UPF architecture leverages the existing architecture of a telecom operator.

Target customers: This deployment option is particularly well suited for an enterprise which only wants to access the public and private networks, and which may have limited budget. Sharing the edge UPF with other enterprises to deploy the mobile VPN solution allows the enterprise to leverage the solution even having a smaller budget.

Figure 7: Mobile VPN deployment with shared UPF


PCF
Subscribed traffic distribution policy ID
SMF
SMFs are fully interconnected with central UPFs and Edge UPFs
Internet
Central UPF
Enterprise1 intranet
VPN-1
VPN-2
Enterprise2 intranet
Shared UPF
User 1
User 2

Source: Huawei

The benefits of mobile VPN

The benefits of the mobile VPN solution compared to the traditional VPN are multiple and can be divided into two main branches. On one side mobile VPN improves the user experience and on the other it optimizes cost and operation.

Mobile VPN provides many advantages over traditional VPN. Firstly, it provides a more secure experience since the connection does not travel through the internet as in the legacy VPN but rather travels through the telco's internal transport network. Secondly, it provides seamless connectivity with a single SIM and no need for a cumbersome log in authentication while also providing better experience by providing 5G high-speed connectivity.

Improved experience

Superior experience: the solution provides access to high-speed 5G. The downlink network rate can be ten times higher as packets are directly transmitted through the operators' intranets, rather than being detoured through the Internet.

Ease of experience: A single SIM card is used to access the company's intranet and public internet with no need for manual log in or the high cybersecurity risky use of passwords. The user connects without the need for a manual log in and can benefit from both the intranet and external public network connectivity inside and outside the campus area.

Ease of connection: The traffic destined for the private and public networks is authenticated and steered automatically in the operators' core networks with no need for manual tasks.

Optimization of cost and operation

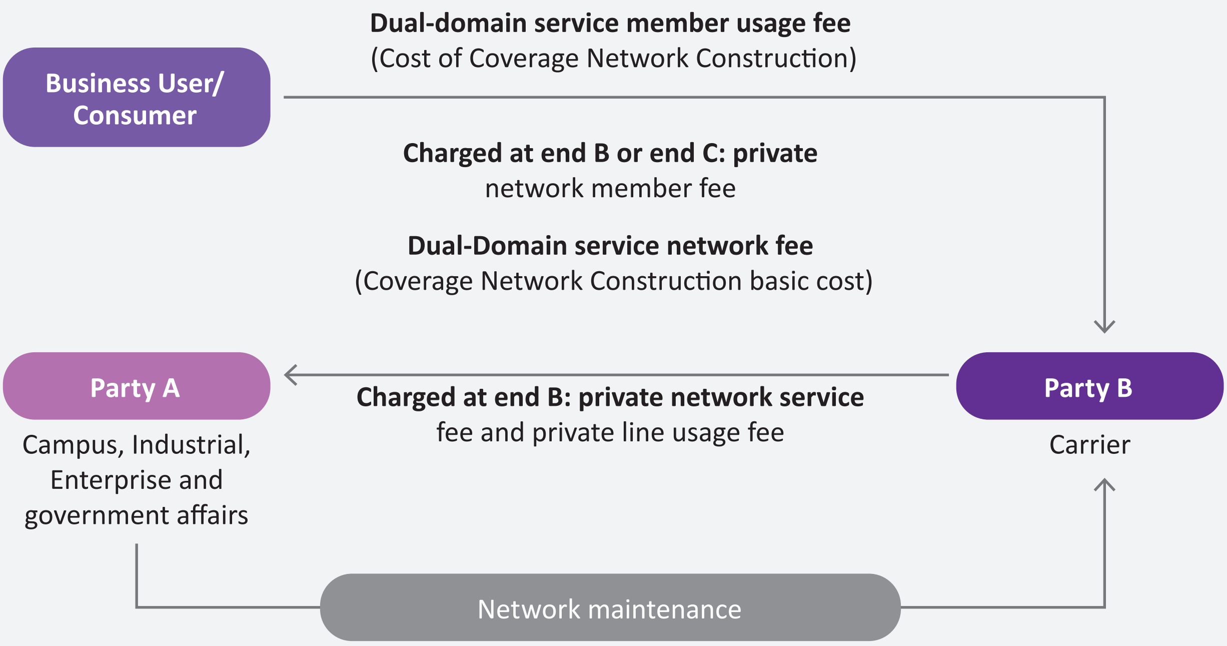
High reliability and security: Since the data does not need to go through the public internet but is transmitted on the operators' intranets, the solution reduces data exposure risks. Security is also improved thanks to carrier-class E2E authentication.

Cost savings via cheaper O&M: While with legacy VPN the enterprise is responsible for O&M for instance for the VPN gateway or for any other network component, with mobile VPN the enterprise can leverage the telco 4G and 5G networks. This brings a faster time of adoption and reduced O&M since the telco oversees the O&M of its network.

Mobile VPN presents an opportunity for telecom operators

Mobile VPN has formed its own business logic:

Figure 8: The business logic of Mobile VPN


Business User/ Consumer
Dual-domain service member usage fee
(Cost of Coverage Network Construction)
Charged at end B or end C: private network member fee
Dual-Domain service network fee
(Coverage Network Construction basic cost)
Party A
Campus, Industrial, Enterprise and government affairs
Charged at end B: private network service fee and private line usage fee
Party B
Carrier
Network maintenance

Source: Huawei

Mobile VPN is addressing various needs of the industries while at the same time bringing significant benefits for the telecom operators.

- Mobile VPN helps carrier to gain new customers, by providing a solution that addresses the security requirement of the enterprise while improve the user experience.
- Furthermore, as enterprises take the solution and as they see the benefits this further helps telecom operators to sell more 5G connections to the enterprise.
- Lastly, mobile VPN addresses industry problems and therefore carriers are gaining experience and momentum in selling solutions.

Case studies

Education – **Zhejiang University campus project**

The Zhejiang University is an education institution with eight campuses and more than 80,000 personnel between staff and students.

As COVID-19 affected online classes and remote access to labs and campus databases, the network became a very important asset to guarantee quality education.

The University leveraged the mobile VPN solution since August 2021. The University can count on a shared UPF and currently has 2,000 subscribers to the mobile VPN.

The benefits of the mobile VPN solution include a comparable cost versus the traditional VPN solution while delivering a better experience, free O&M as the network O&M is conducted by the telco, and country-wide coverage.

Table 1: Cost comparison between mobile VPN and legacy VPN

	Cost (CNY)	Bandwidth	Users
Mobile VPN (5G)	903,000	1G	2,000
Traditional VPN	~850,000	400M	2,000

Service:

Online class

Viewing of scientific research data

Case studies

Public sector – **Shenzhen smart city project**

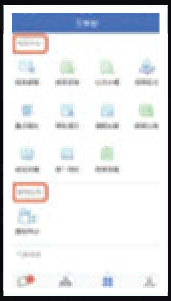
The Shenzhen smart city project encompasses 6,000 employees serving one million people in 23 communities. Governments need to support increasing data-heavy demands to their network. For instance, the city is adding more than 10 office applications in a year. The requirements of these applications are also evolving with increasingly large file size for download and transmission of multi-channel 4K videos.

The mobile VPN solution was launched in January 2021 and has an on-premises UPF serving 4,000 subscribers. Benefits include the secure access to the intranet, high-speed 5G access, and no need for manual VPN log in.

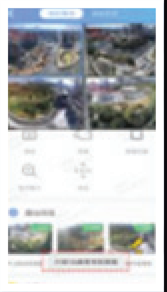
The network slice supporting the e-government application is isolated and independent from the public network traffic and the solution also uses 256-bit encryption algorithm for transmission security.

Scalability is another important benefit of the mobile VPN solution. In Shenzhen, the network covers the Pingshan district, including six subdistrict offices, 23 community, and 670 grids (areas of a few blocks). Having one network supporting all e-government applications, delivered savings as both network investment and time of deployment compared to a wired network were reduced on average by 50%.

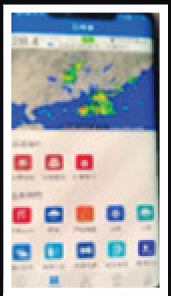
Service:



Outdoor mobile working



Mobile video surveillance



Emergency command

Case studies

Additional case studies overseas

The Mobile VPN solution has also been deployed across various verticals in different countries with PoC conducted in Saudi Arabia, UAE, Thailand, Oman, and Kuwait. Verticals that are adopting the solution for commercial use include education (university) and transport and logistics (Port).

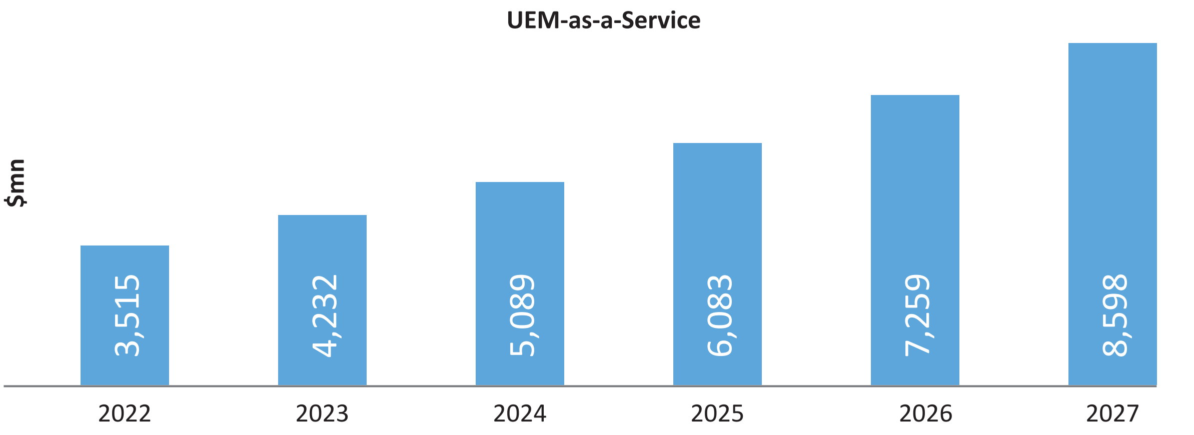
In the UAE, an enterprise in partnership with Huawei deployed a 5G Portable Private Network MEC solution supporting an enhanced remote work experience (reach workspace anywhere, anytime). The solution improved the user experience by eliminating the log in time and avoiding the time-consuming detour of traditional VPN through the Internet eliminating those latency delays and performance drawback. In this scenario the mobile VPN solution brings clear benefits to the enterprise office environment. For instance, it supports employees to roam outside the campus while being able to connect to the intranet without the need for a manual login. It also improves the worker experience and efficiency by solving the issues of conference calls interruptions and failure to share large files outside the campus due to slow network speed. All these benefits are delivered while providing enhanced security as the data does not need to detour on the internet before reaching the intranet.

Market opportunities for mobile VPN

In China there are more than 800 cases which have been commercially launched in verticals such as government, education, and transport. As seen above the demand for mobile VPN is also strong in other countries such as UAE, Oman, and Thailand.

Mobile VPN is a solution that will be able to address a wide variety of use cases from remote connection for troubleshooting, to lessons, and access to digital resources. Among many market opportunities, mobile VPN will play a catalyst role within the unified endpoint management market opportunity which is set to grow to reach US$8.6 billion by 2027 with a 2022 to 2027 CAGR of 19.6%.

Figure 9: Unified endpoint management market forecast: 2022-2027



Source: Enterprise Services Total Addressable Market Forecast: 2020–27

Mobile VPN is poised for growth as enterprises are embracing the use of enterprise 5G mobile broadband for their connectivity needs. In this framework, mobile VPN becomes an add-on that could be monetized by telcos in order to deliver an augmented security and improved user experience, which are the key elements that will be highly sought after by any enterprise. Enterprise 5G mobile broadband subscriptions are forecasted to reach 501 million by 2027 with a 2022-27 CAGR of 59.4%.

Appendix

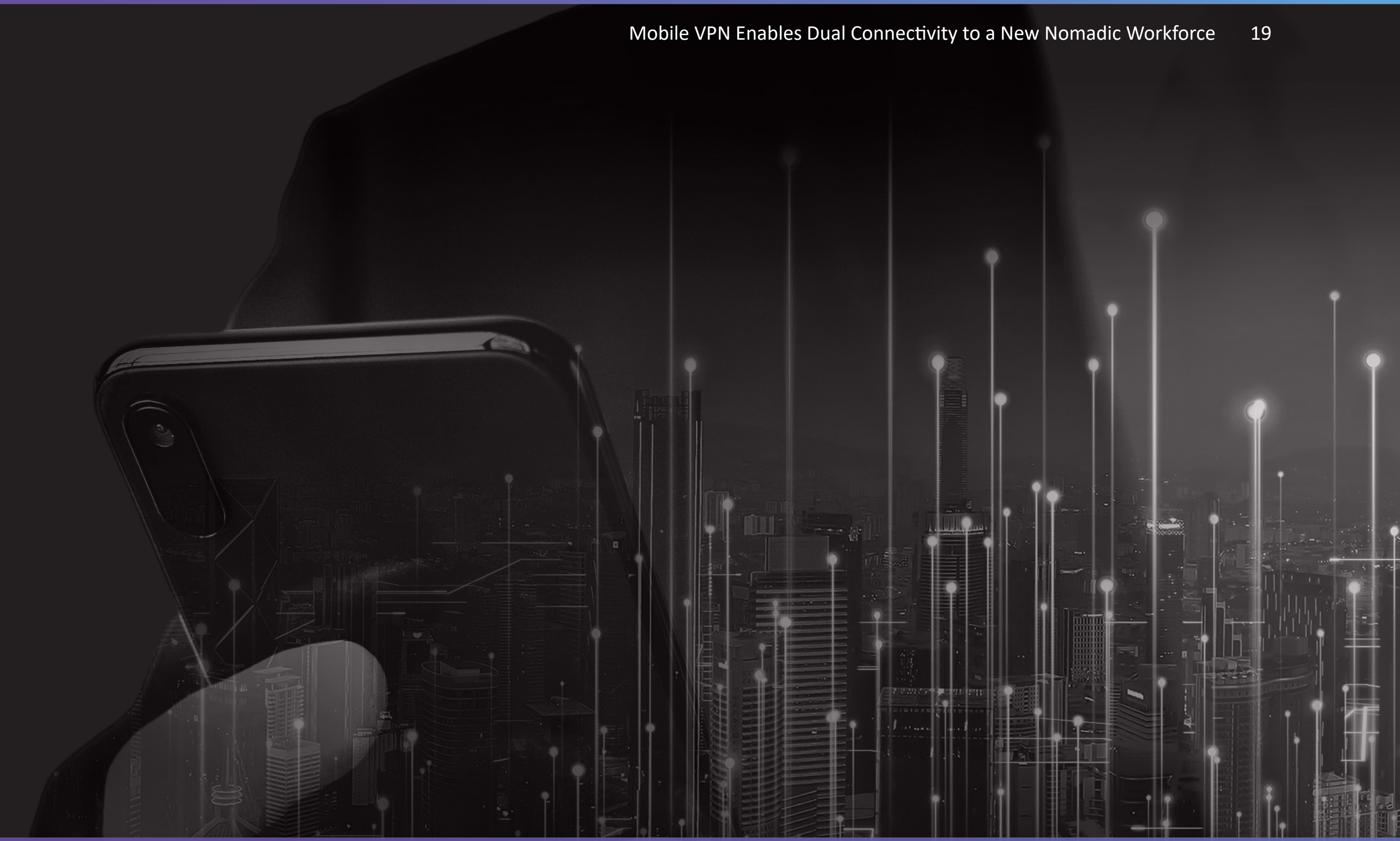
Methodology

This whitepaper was created using Omdia's own market knowledge and data resources as well as leveraging in-depth product briefings and case studies from Huawei.

Author

Pablo Tomasi
Principal Analyst Private Networks and Enterprise 5G

E Pablo.tomasi@omdia.com



Get in touch

www.omdia.com

askananalyst@omdia.com

Omdia consulting

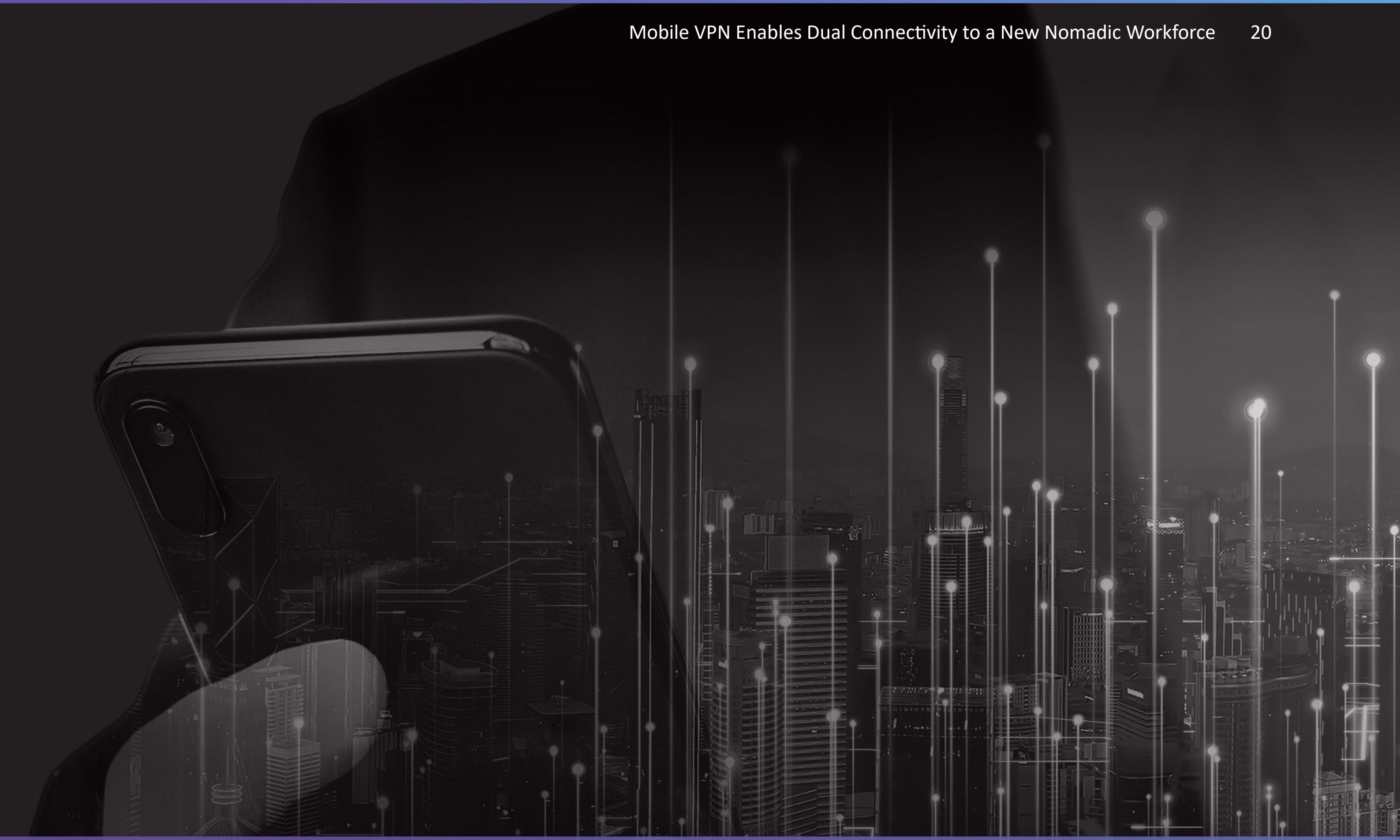
Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantages for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions.
If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.



Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.