Connecting a Remote Workforce

Why the network matters

With the continuing rise in organisations embracing a remote workforce, a lot of time gets spent talking about the apps they'll use to keep them productive and in touch with their co-workers and teams.

However, at the heart of any remote working capability is the networking technologies that keep them connected. Traditional networks weren't designed or optimised to cope with the diverse application location and content requirements of today's businesses.

While everyone is familiar with the concept of VPNs, is this still the best way to keep your remote workers connected or are there better alternatives and how has the cloud impacted this?

In this paper, we explore how the network has evolved to support a remote workforce, what the best connectivity options are now and how they rate against 4 key criteria:

1. Security
2. Speed: Latency & bandwidth
3. Convenience: Ease of setup/use
4. Value

MATRIXCNI
COMPLETENETWORKINNOVATION

7-layer model for network communication

The Open Systems Interconnection (OSI) model was developed by the International Organisation for Standardisation (ISO). Each of the seven layers in this conceptual model for network communication between two systems is responsible for performing assigned tasks and transferring completed tasks to the next layer for further processing. Many communication protocols are developed based on the seven layers within the OSI Model. While the model is not new, it provides a useful framework for understanding evolving technology and protocols as they continue to change over time.

	Layer	Function	Protocol data unit (PDU)	
1	Application	Network process to application (human interface)	Data eg. HTTP, FTP, IRC, SSH, DNS	1
2	Presentation	Data representation, encryption, compression	Data SSL, FTP, IMAP, SSH	2
3	Session	Interhost communication, authentication, permissions	Data eg. APIs, Sockets	3
4	Transport	End-to-end connections and error control	Segments eg. TCP, UDP, ECN, SCTP, DCCP	4
5	Network	Path determination, addressing (IP), routing/switching	Packets eg. IP, IPSec, GRE, ICMP, IGMP	5
6	Data Link	Physical addressing, error detection, flow control on physical link	Frames eg. Ethernet, SLIP, PPP, PPTP, FDDI	6
7	Physical	Media, signal & binary transmission	Bits eg. Coax, Fibre, Wireless	7

Beyond the virtual private network?

Initially the OSI model was applied primarily to direct communication over a cable connecting two systems inside a private network, and later over wide area networks (WAN). As organisations grew, and the need to connect to remote locations increased, building ever-expanding private networks became impractical.

Virtual private networks (VPN) provided a new way for mobile workers away from the office to access data back in the office. VPNs have of course gone on to become ubiquitous because of their ability to provide encrypted connection over a less secure network, using new protocols within the 7-layer OSI model. VPNs enable appropriate levels of security for connected systems even when the underlying network infrastructure alone cannot provide it. For example, a VPN can tunnel securely across the internet to remote locations without the need to build a proprietary physical cable network connection.

Are VPNs still the best network option though for remote access to corporate computing in a mobile age? In many cases the answer is yes, but with the maturing of private, public and hybrid cloud solutions, organisations now need to consider options including:

- **Virtual Private Networks (VPN)** –VPNs extend private networks across a public network or internet, enabling you to send and receive data as if your device were directly connected to the remote private network. You have to download files across the network and save them locally in order to work on them, using the software installed on your local computer. Legacy VPNs often require users to start additional software and complete complex login authentication processes.
- **Virtual Desktop Infrastructure (VDI)** – Virtual desktops enable you to access your entire remote desktop with a virtual representation. This gives you secure access to all of your files and software environment as if you were sitting at your desktop, regardless of the device or operating system you happen to be using. VDI is driven by virtualisation software sitting on central servers so there are obvious implications for demands on the corporate network.
- **Desktop as a Service (DaaS)** – Desktop as a Service is very similar to VDI but avoids the need for heavy server and administration loads to manage the central infrastructure supporting VDI. With DaaS you outsource the virtual desktop to commercial cloud providers and the loads and security management transfer to those commercial networks. This reduces demand on corporate networks and administrators and whilst it is good for generic desktop configurations, it is still new territory for highly customised desktop configurations. As this market continues to mature though it will present increasing challenge as an alternative to the traditional VPN model.
- **Software-defined wide area networks (SD-WAN)** – Traditional VPN networks rely on individual device configurations, so central administrators often use third-party tools for configuration management - this however becomes stretched with internet VPNs that continue to grow organically. SD-WAN solutions solve this with a hierarchical, template-driven structure for network administration. For example, you can start by defining what each site type should look like in advance, assign sites to that software defined network configuration, and from then on simply update the site template to instantly update associated sites. Think for example of a pathology provider with offices in health care centres nationwide, or a retailer with similar store requirements in all states. SD-WAN can be used to specify network characteristics such as single or dual WAN connections, VLAN settings for voice/data, SSID for internal and guest Wi-Fi, Quality of Service (QoS) schemes, firewall policies, IP subnet ranges for LANs, and more.

While much of the public dialog still tends to focus on the mobile devices that mobile workers use, the reality is that the underlying networks are the critical enabler. Four key criteria are central to a meaningful assessment of network options for your organisation:

Security **Speed** **Convenience** **Value**

Security

Security must be a consideration in every network decision. In times past, that led to a fortress concept of delineating between activity inside and outside the corporate firewall. With increasing mobility changing the network landscape, how should network security considerations influence decisions on VPN, VDI, DaaS and SD-WAN in a world of private, public & hybrid cloud? The answer is different depending on the specific needs of each organisation, but there are general factors to consider

Security considerations and network implications

VPN

Connecting from hotels, airports, coffee shops, 4G/LTE and 3G cellular networks, requires secure access to internal corporate resources. To achieve this, Virtual Private Networks (VPN) often require users to start additional software or open a web browser and complete a manual log in process. VPNs only assign an IP address within a LAN or WAN, so they can expose your corporate network to any issues on your home or remote network. The more open tunnels there are to the work environment, the more avenues of attack the corporate network is exposed to.

Different communication protocols offer different strengths depending on your needs:

- IP Security (IPSec) – One of the weaknesses of the original Internet Protocol (IP) is that it doesn't ensure authenticity and privacy of data as it is passed over the internet. IP Security (IPSec) provides a secure communications protocol (OSI Model Network Layer 3) to channel through an existing IP network.
- Generic Routing Encapsulation (GRE) – GRE can be used as a tunnelling protocol, encapsulating a wide variety of OSI Model Network Layer 3 protocols inside virtual point-to-point links over an Internet Protocol (IP) network (examples: IPv4, IPv6, AppleTalk)
- Point-to-Point Tunnelling Protocol (PPTP) – PPTP is an OSI Model Data Link Layer 2 protocol (set of communication rules) that enables corporations to tunnel securely across the internet. Initially implemented heavily in Microsoft Windows products, PPTP builds on other protocols including Point-to-Point Protocol (PPP) and an enhanced version of GRE.
- Secure Sockets Layer (SSL) VPN – Modern SSL VPN offers both client-based options (installing software on the client) and clientless options (avoiding the need to permanently install anything on the client). While still not giving the remote user their full office desktop, SSL VPN can for example, enable remote users to login through a web browser to access a portal of internal web applications and file shares.
- Mobile VPN (mVPN) – mVPNs are used in environments where workers need to keep application sessions open throughout the working day while travelling and connecting and re-connecting via various wireless, 4G/LTE and 3G networks, encountering gaps in coverage, or suspending-and-resuming their devices to preserve battery life. A conventional VPN cannot cope with these network tunnel disruptions, causing applications to disconnect, time out or fail. An mVPN overcomes this by maintaining a virtual connection to the application even while the endpoint changes, with the mVPN handling the multiple network logins transparently behind the scenes.

VDI / DaaS

- With VDI you have all the control at your location because it is an on-premises solution. However, that also means you are responsible for managing it in the event of something going wrong.
- DaaS is a service-based approach to virtualisation, granting admins/IT managers control over end-user desktops via an administration gateway. With DaaS, VDI from vendors such as Citrix, Amazon and Google provides security and hardware managed by the provider, with no need for you to manage rack space or maintenance. This subscription-based model is great for agile computing, but regulated industries are still better served by VDI, and latency, data hosting and regulations can present issues.

SD-WAN

While security is not the primary motivator for moving to SD-WAN, the ability to apply template driven networking policies to entire sites provides significant benefits for security management across your network. The ability to apply context-sensitive security configurations across a complex hybrid network provides significant comfort for time-poor central network administrators. It means you can provide smart software-defined network administration and enforce enterprise-wide password, data protection and security policies.

NGFW

Next Generation Firewalls (NGFW) provide more granular and context-aware understanding of application traffic, with identity-based rules so you can manage inbound traffic securely when enabling partner access to small portions of your internal network and services. NGFW are not ideal though for mobile users connecting to the internet from outside the network. So for secure mobility, NGFW should be augmented with cloud-based and mobile security solutions to maintain policy, application and data protection across the organisation.

Speed: Latency & bandwidth

The most comprehensive solution in the world may look good on paper but if it results in unacceptable latency and bandwidth impacts for users, it may be untenable. There is no one right solution in terms of speed, but each of the network options presents particular considerations to factor into your evaluation decision-making.

Latency & bandwidth considerations and network implications

VPN

VPN tend to be bandwidth friendly because they do not rely on processing heavy server infrastructure like VDI. Some mobile VPNs offer additional mobile management to enforce access policies based on the network in use, bandwidth of the connection, on OSI layer-3 and layer-4 attributes (IP address, TCP, UDP port), time of day, and in some VPNs, the ability to control access by individual application software. Quality of Service functionality can provide the ability to specify the priority that different applications or services should receive when contending for available wireless bandwidth which makes it possible to prioritise mission critical applications when bandwidth is constrained. Some organisations choose to use a secure VPN service. Factors to consider in relation to VPN transfer speeds include, distance to VPN server, which protocol is being used to connect (different protocols have different connection overheads), and what hardware is being used to connect (example: a new mobile device will be far more efficient at connecting than an old laptop).

VDI / DaaS

- VDI relies on interaction with a server or servers in the data centre running virtualisation software. All hardware, software, licensing and deployment is handled in house. Latency is minimal and IT has complete control. However, hardware failure and software issues can still occur, and when they do it can end up more expensive in the end. VDI can also create LAN and storage bottlenecks as multiple PC sessions travel over the local network to the hosting servers in the data centre.
- DaaS subscription-based models are great for agile computing, but regulated industries are still better served by VDI. Latency and data hosting regulations can present issues to be managed. You also need to consider what end users will do when they do not have access to a reliable or fast-enough internet connection (ie many public locations). Equally, if working on-site with clients, your mobile users may find themselves using wireless internet connection subject to perimeter security or a VPN that prevents them from accessing your DaaS provider. Your network design needs consider all of these factors.

SD-WAN

Moving to a software-defined solution can deliver a familiar network topology while solving some of the performance and management challenges of traditional VPN. SD-WAN solutions make it possible to separate underlying infrastructure from the overarching network. In practice, this means that your SD-WAN can include a mix of multiple types of connectivity (for example a mix of business-grade ADSL2+, plus a cable modem link plus a 4G/LTE service). Your SD-WAN can manage across that pool of connectivity and automate traffic decisions on a per-packet basis to use the most effective available route at the time and even duplicate critical packets across circuits if needed. This makes your network a viable option for more applications and different links and drop in and out over time without bringing down the entire network. It is also a sophisticated solution for mobile users moving in and out and across different connectivity options during the course of a day

Next generation firewalls

Next-Generation Firewalls (NGFW) are faster than their predecessors, but they do involve heavy processing and network traffic (the more inspection rules the perimeter firewall is expected to process or enforce, the more horsepower and network resources required). So you should stress test systems you are evaluating to make sure they can handle the throughput needs of your network to avoid impacting network latency and bandwidth. In a mobility context, it is also important for mobile devices connect to the Internet from outside of the NGFW. So while you can backhaul remote and mobile traffic to pass it through an onsite NGFW, that is bandwidth intensive and expensive.

Convenience:
Ease of setup and use

You also need to consider the administration practicalities of your organisation's network infrastructure decisions. How complex will it be to set up? How challenging will your network choice be to administer on an ongoing basis? Do you have those skills in-house or will you need to engage support or enhance your admin team? Different network choices raise different convenience considerations.

Convenience considerations and network implications

VPN

Establishing a traditional VPN requires:

- VPN software on the client to enable the user to initiate a secure remote connection
- VPN-aware routers and firewalls to allow legitimate VPN traffic through
- VPN server to manage incoming VPN traffic and access to network resources.

One of the advantages of this approach is that IT administrator skills are readily available as a result of the longevity and pervasiveness of VPN approaches. However this has to be balanced with the challenges of managing mobile access for remote users and increasing pervasiveness of cloud solutions which are radically changing the IT landscape.

VDI / DaaS

While VDI is improving all the time, there is still a relatively heavy administration requirement for initial set-up and configuration of virtual desktop templates. The advantage of course is that once set-up, the same desktop model can be rolled out easily to multiple devices. DaaS has similar ease of use characteristics, with the added benefit that contracting this out to a service provider means you hand them the responsibility for configuring adaptations to present the virtual desktop on multiple different types of devices and operating systems. That said, DaaS tends to come into its own on generic desktop configurations with a base suite productivity software. Once you start moving into increasingly tailored sets of software with desktop configurations requiring specialist software applications, the administration simplicity fades with the increasing complexity.

SD-WAN

- Site-by-site introduction of SD-Wan for problematic VPN sites can provide a low risk transition to test the new technology and then assess if it is logical to roll it out more widely in your organisation. The software defined template nature of the solution makes applying templates to new sites relatively simple which is highly attractive for organisations with a large number and/or rapidly changing number of sites under management.

Value

What though of cost considerations? Where do value considerations factor in on network option evaluation? As in many things, the answer depends on the specific characteristics of your user base, the data and applications they interact with, and where they need to access those systems from.

Cost/value considerations and network implications

VPN

Traditional VPN are good for scalability and cost-effectiveness because you can add an almost infinite amount of capacity through your Internet Service Provider (ISP). Also, if one VPN client gets interrupted, it won't necessarily take down everyone on the network.

VDI / DaaS

DaaS provides many of the same advantages of local-network VDI including centralised desktop /data control and security, centralised backup and disaster recovery for virtual PCs, but at far less initial capital expense than on-premises VDI deployment. You rent it from the cloud provider as part of a subscription cost. It can seem cheap, but only in its most bare-bones configuration. When you add up all the service components for DaaS in a fully managed configuration, the per user per month cost can get pretty high.

SD-WAN

SD-WAN feature sets are beginning to present a compelling alternative as a VPN replacement. Some solutions are priced comparably to the maintenance of traditional VPN – which again makes considering SD-WAN to replace problematic VPN sites an attractive option for some organisation.

Making the right network decisions for your organisation

Increasing mobility and cloud-based solutions provide a brave new frontier for truly mobile organisations but the fact remains you need a robust underlying network designed and optimised for the needs and characteristics of your users. Security, speed, convenience and value considerations are all critical factors when you evaluate network optimisation options. If you need help, specialist network advisors can be a sound investment to guide your decisions and assist with implementation.

About Matrix CNI

Matrix CNI is an Australian owned specialist network integrator with expertise in the fields of Campus LANs, Converged Data Centre Infrastructure, Unified Communications, Wireless Mobility, Application Availability and Security. We maintain strategic relationships with a select group of key industry vendors to provide competitive, reliable and secure network solutions with best of breed performance to support a fixed and mobile workforce. MatrixCNI clients include a wide range of education, health, government and enterprise organisations.

MATRIXCNI

MatrixCNI Pty Ltd

13-15 Lyon Park Road
Macquarie Park NSW 2113

1300 850 400 | info@matrixcni.com.au