celestix

PSN compliant remote access

Whitepaper

March 2015

DirectAccess and IPsec connectivity in the public sector

Mobile working in the public sector is nothing new but in recent years the nexus of forces that impact on mobile working initiatives has increased. PSN guidelines and the data protection act are key considerations that impact remote working. Cost saving initiatives through the reduction in real estate and the streamlining of IT services also has a significant bearing on mobile working. These factors combined with the rise of mobile friendly technologies have mixed together to create the perfect storm for public sector organisations.

In this document we will explore the key considerations faced by public organisations when reviewing their mobile working strategy. We will also look at how DirectAccess addresses the considerations for delivering secure, compliant and seamless mobile working.

The Nexus of Forces

There are many considerations that must be addressed by public sector organisations when reviewing their mobile working strategy but they can be grouped into three primary areas

- Ensuring compliance with regulatory guidelines
- Improving the remote working experience for users
- Reducing operational costs

Ensuring compliance

PSN guidelines provide clear and sensible guidelines for the use of remote working solutions. The simple nature of the guidelines pertaining to remote working is due in part to the long standing availability of mobile working technologies. There are four key tenets that must be considered

1. Remote/mobile devices shall employ encryption to protect data at rest and in transit. The cryptography used shall have a suitable level of assurance.
   This is a common sense and widely understood requirement. The use of encryption at the endpoint and also to protect remote access sessions has been in use for years and so compliance with this requirement should be simple for any organisation.

2. Where possible any mobile/remote device that has access to PSN services/networks should use two factor authentication

   Two factor authentication is another familiar technology to IT staff and it is commonly used to validate the identity of users when requesting access to the corporate network. But this PSN guideline refers to devices and not users which causes ambiguity when determining how best to identify users when they work remotely.

3. Any mobile/remote device that has access to PSN services/networks shall be considered by the organisational lockdown and configuration management policies

   This requirement can be complicated to deploy, difficult to enforce, and require cross vendor solutions to achieve.

4. The organisation must be able to show appropriate control and management of the technical environment of any device that has access to PSN services/networks

   Considering the standard nature of the previous three guidelines this requires much greater consideration. Appropriate control and management of the environment is subjective, and it doesn't only apply to the remote environment but the whole environment.

In addition to these guidelines is the requirement for public organisations to ensure they are using fully supported technologies. Due to the rapid technological advancements in mobile working technologies many remote access solutions have become End of Life (EoL). The use of EoL technologies is a risk that must be avoided.

Complying with these guidelines is an excellent starting point for architecting a mobile working strategy but as is often the case compliance does not guarantee security. Compliance may also adversely impact the mobile working experience through the need to apply so much technology as to make the user experience difficult.

Improving the remote working experience

The desire to improve the remote working experience is the number one priority to all public organisations. Advancements in mobile hardware technologies such as tablets, smart phones and software technologies like Windows 8 have enabled organisations to embrace mobile working on a far greater scale than previously possible.

The modern workforce now expects to be able to work remotely and in a flexible manner. Availability of the latest devices is seen as a benefit of most modern jobs.

The combination of a workforce that is hungry for flexibility and the availability of technology that supports it has provided organisations the ability to meet modern working requirements.

In public organisations the mobile working experience may also require the use of devices with 3G/4G connectivity which further extends the capabilities of remote working, when signal reception allows.

But with greater flexibility comes a higher level of risk which, if not managed carefully, can affect an organisation's ability to comply with data handling regulations.

Reducing operational costs

Public organisations are under sustained pressure to demonstrate cost savings. In many cases real estate is being sold off and workforces consolidated into fewer buildings. Pressure is also on to ensure all expenditure delivers best value for money.

Organisations that have scaled down their real estate have been presented with an ideal opportunity to enable a more mobile workforce. The aforementioned advancements in mobile technologies support this. And because mobile working is not new, all organisations have technologies in place that can deliver mobile remote working already.

The challenge is not in enabling a mobile workforce but rather how to do it on a much larger scale.

If flexible working, the use of new and diverse endpoints, and a mobile workforce presents security risks then consider the true scale of those risks when as much as 50% of a previously office based staff are now to work remotely.

The other, often overlooked, issue with reduction in real estate is that while it may allow an organisation to demonstrate a tangible cost saving, and in many cases it puts money back in the coffers, it can actually be responsible for moving cost rather than eliminating it.

When a greater number of staff is empowered to work remotely this will require investment in portable devices. It will also require a greater level of IT infrastructure to support mobile connectivity and security.

Then there is the issue of IT literacy and impact on helpdesk. Most workers are not experienced with the systems they use to consume content and this causes helpdesk calls. Now amplify this when allowing staff, whose primary remit is not IT, to work remotely. Now they must interact with a VON client, use a one-time password to log in, and if anything goes wrong they have to call IT because they cannot work until the issue is resolved.

So even through there is a focus on reducing operational costs, the provision of mobile working can increase IT costs considerably.

Summary of the Problem

Addressing the need for mobile working in the public sector is about building a robust strategy. This is required because of the increased scale of mobile working and the requirement to juggle the needs of the organisation, the aim to reduce costs, and the need to handle and share data in a compliant manner.

Through all of this there is a potential solution that also allows the organisation to do more with less.

The Solution

With such a complex combination of compliance, security and flexibility, any mobile working technology to meet the need would need to be extremely complex and potentially expensive.

Yet since its launch, Celestix E Series has provided a very simple answer to the mobile working challenge.

Celestix delivers PSN compliant mobile working solutions to the public sector on their E Series range of appliance and virtual appliances. The platform includes a hardened and secure instance of Windows Server 2012 R2 which has been optimised to run the Unified Remote Access role.

Revolutionary remote access

One of the core remote access capabilities is DirectAccess, the most revolutionary advancement in the field of remote access since the launch of SSL VPN.
DirectAccess provides a secure and encrypted always on network connection for compatible domain joined Windows 7 and 8 devices.

Furthermore, DirectAccess is CPA certified by CESG to deliver a compliant and secure remote access platform for the public sector.

Since its inception, Celestix E series has become the reference architecture for deploying PSN compliant remote working in the UK. So how has it been able to address the diverse and complex nexus of forces?

Improving the user experience

DirectAccess offers the remote worker the same experience as if they were sitting in their organisation's office. The connectivity from the endpoint device to the network is automated and requires no user interaction.

Not only does this enable the user to be more productive, it also removes the need for the user to interact with any complex technologies such as initiating a VPN session. This in turn reduces the volume of helpdesk calls from remote workers.

celestix

In addition, DirectAccess connectivity initiates rapidly, even over 3G networks, resulting in more remote devices connecting more regularly to the corporate domain. This drives even greater productivity gains particularly for truly mobile workers such as community workers.

Ensuring compliance AND security

DirectAccess is only available to domain joined devices running Windows 7 ultimate or enterprise edition, or Windows 8 and 8.1 enterprise edition. Connectivity between the endpoint device and the E series gateway appliance is encrypted and uses IPv6 for the transport to the gateway.

This has one powerful outcome when considering PSN compliance. It means that only employees using corporate issued devices that are a member of an AD group that is authorised to connect via DirectAccess, and that have a corporate issued certificate can gain access to the network.

Organisations that wish to show appropriate control and management of devices accessing their network can demonstrate this clearly by using DirectAccess because quite simply the gateway is not available to anyone other than people and devices that meet the strict criteria.

In addition, the solution provides encryption profiles that are aligned to the PSN standards, meaning that all remote sessions are fully encrypted in transit. In many instances, the session can be double encrypted.

This is already a powerful tool, but DirectAccess delivers even greater security and control by virtue of its bi-directional connectivity.

DirectAccess empowers organisations to demonstrate far greater control and management of their IT environment in three principle ways;

1. DirectAccess enabled devices are always on the network and so can receive all group policy updates
2. DirectAccess enabled devices are always visible to the administrator and so user technical issues can be addressed without the need to use a third party tool to connect to the remote device.
3. DirectAccess enabled devices are accessible and so the organisation can initiate proactive vulnerability scans on all devices, regardless of their physical location.

The security capabilities don't end there. It is commonplace for organisations to enforce the use of endpoint encryption technologies such as bitlocker, which not only encrypt the device but can also be used to identify the user. The combination of machine based certificate, user credentials and encryption PIN being sufficient to achieve PSN approval.

Reducing costs

Unlike most traditional VPN solutions DirectAccess does not require the purchase of client access licenses. The only requirement to run DirectAccess is the use of a Windows Server 2012 R2 gateway device and a compatible version of Windows at the endpoint. Being able to reduce the need for licensing employees for remote access can deliver tangible cost reductions.

In addition the provisioning of the DirectAccess capability is delivered through issuance of group policy. There is no need to install any agent software on the devices.

Because of the high levels of security that inherent in DirectAccess, most organisations are able to comply with PSN regulations while terminating the need for traditional user two-factor authentication, saving more money and further reducing IT administration overheads.

celestix

Meeting the Need – PSN compliant, user friendly, low cost mobile working

Transformational working initiatives aligned with developments in mobile working technologies and made it easier than ever to enable modern and flexible remote working.

Traditional VPN solutions may not be compatible with modern devices and operating systems and in many cases they are End of Life or End of Support and require significant investment to upgrade.

DirectAccess addresses the core PSN guidelines for mobile working and the bi-directional capability also enables organisations to comply with other aspects of the guidelines.

Compliance is easier to demonstrate by virtue of the CPA certification of DirectAccess.

But it is the improvement in remote working experience that really sets DirectAccess apart from other remote access solutions.

With DirectAccess it is possible to deliver a robust and consistent mobile working strategy.

Final Thoughts

This white paper concentrates solely on the use of DirectAccess for employee based access to the corporate network.

The E series solution also incorporates the other features of the Unified Remote Access role with Windows Server 2012 R2. These include IPsec VPN, web application proxy, AD FS proxy, Remote Desktop Gateway and Workplace Join.

About Celestix Networks: Celestix Networks is the world's largest Microsoft security OEM partner. The business has been supplying ISA server, TMG and UAG appliances to the public sector since 2004. Our solutions ensure a secure, reliable and performant platform and provide a range of enhancements to the DirectAccess solution.

Celestix E series is the reference architecture for deployment of Microsoft's DirectAccess solution within the public sector.

Corporate Headquarters
Celestix Networks, Inc.
3125 Skyway Court
Fremont, California 94539
+1 510 668 0700

EMEA Headquarters
95 London Street
Reading RG1 4QA
United Kingdom
+44 (0) 118 959 6198

Asia Pacific Headquarters
62 Ubi Road 1
#04-07 Oxely Bizhub 2
Singapore 408734
+65 6781 0700

Celestix Networks, Japan
2-12-4 Hirakawa-Cho
Chiyoda-ku
Tokyo, Japan
+81 3 5210 2991