

Freedom for Remote Workers by David Beesley

Clientless VPNs are opening the remote working floodgates for more companies, by cutting the costs of deploying and managing secure remote access. David Beesley, director of Network Defence shows how to tell if the technology could work for you

True remote working used to be the preserve of the privileged few – the senior managers and directors of big PLCs that could afford the technology, and manage its inherent complexities. These included slow data connections, the need to deploy and manage special software on remote PCs, and handling encryption and user authentication to maintain security.

However, the last two years have seen a surge in remote working, as a new technique has made it viable for a far greater number of companies without compromising security. Called clientless virtual private networks (VPNs), this new technique offers a number of key benefits both to companies and users.

Users get secure access to corporate resources over the Internet from any Webenabled PC anywhere – boosting overall productivity. This is achieved with no need to install or manage special software on the remote PC. What's more, it's easier for IT staff to manage, and it's friendlier for users because access is done through a familiar web browser interface.

When these benefits are combined with external factors such as wider staff mobility and widespread broadband Internet, you have all the ingredients for a quiet revolution in the way your staff use your office systems when they're out of the office – whether visiting customer sites, at overseas meetings or simply on a long weekend away.

Making the links

So how does a clientless VPN work? Put simply, VPN server software is deployed on your corporate network, enabling remote users to set up a clientless VPN link

from any web-enabled machine with a browser that supports secure shell (SSH), the well-established encryption and authentication technology.

As mentioned earlier, there's no need to install and manage special software on the remote PC. So, for example, if a user is at a customer site within another company's network, he or she could borrow a web-enabled PC and create a secure, encrypted link back to the home network simply by connecting to the VPN server via the browser and authenticating themselves.

You also decide the access rights that each remote user can have – helping you to manage the usage of company systems and resources.

So far, so good. But how do you scale a VPN to the right size for your company? What upgrades – if any – do you need to make to your network infrastructure? And how do you ensure that this level of 'anytime, anywhere' access doesn't make a company's network more vulnerable to attacks, from nuisance hacking to unauthorised access to sensitive data?

Here's how you can answer these key questions, and reap the benefits of the technology cost-effectively.

How much VPN capability do I need to buy?

The key points to consider here are the numbers of remote users and their predicted usage patterns. When you've established this, you can then look more closely at the costs of VPN software and licensing issues (e.g. per-user licensing or concurrent user licensing). By building a usage model, you can be sure that you're only buying what you need now, with the capability to expand in the future as your users' needs evolve.

Do I need to upgrade my comms infrastructure?

The short answer is no. Moving to a clientless VPN means that you can simply use your existing Internet pipe (whether ISDN, broadband or leased line). There's no need for additional comms equipment or dial-up connections to be deployed at the corporate network end.

Some clientless VPNs support data compression, which can be used to good effect if some remote users have to use a slow Internet connection to set up their VPN link. Compression also keeps call and data charges low when staff have to use pay-asyou-go connections.

What about my existing security policies?

Clientless VPNs typically do not affect your existing security policies. VPN traffic is encrypted using SSH, and other types of strong encryption (with 128-bit keys, or longer) can be deployed according to need. If you have existing token-based authentication, clientless VPNs can support this too. Also, because the VPN server software uses SSH and can include firewall functionality, it's easy to filter data traffic to exclude unauthorised traffic or users trying to enter the network.

What about ongoing support?

Once you have set up the identities, permissions and access rights for your remote users, there's very little support needed because there's no widely distributed client software to manage. Also, there's virtually no support overhead from remote users because of the simplified user experience – a simple pop-up login dialogue or a bookmarked web page in a browser.

What about support for mobile connections and devices? As the cost of mobile computing falls, it's worth establishing that the clientless VPN solution you choose can support the technology. New solutions, such as those from AppGate, support 2.5G and 3G mobile connections by enabling roaming, which overcomes the common problem of unstable connections and poor network coverage.

If the connection to the VPN server is lost, the software will automatically reconnect the user when the network becomes available again, and the application will remain available to the authenticated user without logging them out due to lack of activity.

In summary, a clientless VPN solution could help set your company on the path to greater productivity and more flexible working. Using these guidelines, you can be confident of putting the technology to work for the benefit of you and your staff.