Secure Remote Access. What does it mean today?

Diggers, 2014-08-05

I've been working with remote access solutions for nearly 15 years now and looking back the use of these solutions has changed dramatically over that time. We've moved from a time where remote access was available only to a vital few - IT or the Chief Exec for example, to an era where there are use cases for most if not all users.

There are many factors that have driven this shift; improved connectivity with broadband capability being generally available; the advent of mobile compute platforms giving users capable devices that can be used in any location; better security with device analysis, management and policy control ever improving; increased capability for delivering applications centrally, using web, SaaS, cloud and virtualisation technologies. All of these have driven demand for organisations to provide coherent capabilities to allow users, partners and 3rd parties access to our previously ring fenced networks.

The challenge today then is, not "How do I give remote access to my users?" But "How do I give remote access whilst meeting the plethora of different requirements that covers?"

Clearly, a solution that focuses purely on VPN, or on mobile access management for example, whilst probably doing that well, will only deal with part of the requirement. With that approach you could easily end up with multiple point solutions to manage and even then still have gaps in what you can do.

At F5 we've always approached these challenges from the application perspective. In fact our mission as a company is: "To help organisations to deliver the the most secure, fast and reliable applications to anyone, on any device, anywhere, anytime". How then does that translate into a solution that will meet the needs of today's enterprises? Well, let's look at the challenges in a bit more detail.

We need to support the wide range of access methods users have available today and let's not forget we're not just talking about tablets and smart phones, we still need to support PC's, Macs and Linux.

We need to be able to differentiate between the various device types and provide the right type of access. To do this we also needs to be able to understand the applications, so traffic can be directed to the right content delivery servers.

We need to have a solution that's in the right place physically to provide secure access and perimeter protection. Remote access by its very definition involves opening the perimeter and letting access in, so that needs to be controlled preferably at an application level.

We need to be able to understand the posture of the end point devices and provide policy controlled access based upon the user's access scenario - Who is the user? Is the device a corporate device? Is the user an employee, partner, customer or other? Where is the user? What state is the device in? What rights should the user have?

These, I would class as the minimum requirements for any solution. What else should we be considering then? We'll lets go back to the applications first:

We need to be able to deliver not only enterprise applications, and desktops (VDI) but also SaaS and cloud based applications – these in particular are seeing massive enterprise take up now and for good reason, because they’re easy to deliver! Then we need to make it easy for the end user to consume whichever type of application they need, so a single point of access, single sign on and federated access (I.e SAML) are all important.

Next we also need to consider performance. We no longer have the luxury of LAN conditions. We're talking WAN now and unknown conditions at the users end, so we need to do what we can to optimise the connectivity and the applications. This may be through optimisations at the network layer, such as adjusting TCP to give best throughput, or at the application layer such as dynamically refactoring web based applications to give better loading experience or maybe through adding dynamic caching and compression. It's a simple and unfortunate fact that if you don't get your application performance right, your users will quickly become disenfranchised with the solution.

What then are the final two considerations? The last pieces of the jigsaw? Manageability and cost. As I mentioned earlier, if you try to meet all these requirements using point solutions you're going to have a bad time. At a minimum you're going to have network firewalls and VPN, add in wan optimisation, federated access, cloud bridging, traffic management, application firewalls and more and your problems increase. You'll have multiple appliances, multiple support costs, multiple management methods, multiple training requirements and that's before you try and get them all working together.

Back to F5 then. One of the key benefits of our range is that we offer a module based solution. We have modules for firewall (ICSA certified of course), for VPN (ICSA certified of course), for Web application firewall (yep you guessed it – ICSA certified), traffic management and also optimisation and acceleration. These modules sit on our traffic management operating system TMOS and can be deployed together, with centralised management, to give a solution that meets all of the needs described earlier. Couple that with the ability to deliver these functions on a virtual, appliance or chassis based high performance fabric that will easily grow with you as you develop your environment, means that moving to cloud, SDN or hybrid architectures will not have to adversely affect your remote access solution.

At this point I'd encourage you to take a look at the Application Services reference architecture that's available at: https://f5.com/solutions/architectures/application-services

I'm sure you'll find plenty of useful information in there to help you design the remote access solution that your company deserves.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com