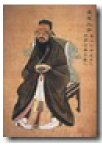
CloudFucius Dials Up the Cloud

Peter Silva, 2010-07-07



According to IDC, the worldwide mobile worker population is set to increase from 919.4 million in 2008, accounting for 29% of the worldwide workforce, to 1.19 billion in 2013, accounting for 34.9% of the workforce. The United States has the highest percentage of mobile workers in its workforce, with 72.2% of the workforce mobile in 2008. This will grow to 75.5% by the end of the forecast period to 119.7 million mobile workers. The U.S. will remain the most highly concentrated market for mobile workers with three-quarters of the workforce being mobile by 2013 and Asia/Pacific (excluding Japan) represents the largest total number of mobile workers throughout the forecast, with 546.4 million mobile workers in 2008 and 734.5 million in 2013. This means more workers will be using mobile devices, not being tied to an office cube and will need to have access back to the corporate network or applications hosted in the Cloud.

Enterprises and management are faced with a potential contradictory business situation. The level of employee collaboration is on the rise; yet at the same time, the locations and work hours are changing and growing. Additionally, companies understand the importance of providing access to their critical systems, even during a disaster; and that doesn’t necessarily mean a major tornado, flood, hurricane, earthquake or other natural phenomenon. What does an enterprise do when it’s so cold and snowy that employees can’t get to the office? Declare a “snow day” and close their doors? Certainly not. What does an employee do when they are sick, injured or their child is home from school? Depending on the severity, they might be able to work from home. As for the users, it's not just a bunch of office employees and road warriors accessing shared files; but it’s also consultants, contractors, telecommuters, partners and customers using home computers and mobile devices to get our job done. Squeezed in the middle are the IT guys facing the demands of both management and users, along with the ever expanding and evolving security requirements.

SSL VPN has become the mainstream technology of choice for remote access and Infonetics reports that the Worldwide SSL VPN gateway revenue increased 13.9% to $116.8M in 4Q09 and will grow 19% to $138.7M by 4Q10. Traditionally, corporate VPN controllers have been deployed in-house or in the corporate data center since the needed resources were also located there. Management and control over that VPN has been critical since it’s the gateway to the corporate network along with much of the sensitive info that resides ‘on-the-inside.’ Plus, *most* VPN controllers are full appliances – dedicated/branded hardware with the vendor’s code baked in. Finally, the advancement of cloud computing has become an enticing choice for IT departments looking to deploy corporate systems and sensitive resources for user and customer access.

Enter FirePass SSL VPN Virtual Edition.

A couple weeks ago F5 released FirePass v7, improving SSL VPN functionality, scalability, third-party integration, and offering new flexible deployment options including a virtual appliance. Virtualization as a technology, has reached a point of widespread adoption and many customers have requested the option of running FirePass as a virtual appliance. Providing a virtual edition of FirePass allows customers to potentially save money by allowing them add SSL VPN functionality to their existing virtual infrastructure. With FirePass VE, you get better scalability & flexibility due to the ability of being able to spin up and spin down virtual FirePass instances across the globe, in much the same way we talk about the BIG-IP appliances managing virtualized environments around the world.

FirePass Virtual Edition is the full fledged, full featured FirePass code and currently runs on VMware ESX* and ESXi 4.0*. It’s vMotion enabled and you can cluster for config-sync, load balance VMs and service providers can have multiple VMs running on one system for a hosted VPN service. FirePass VE provides flexibility, scalability**,** context, and control particularly for Small & Medium Enterprises whose budgets might still be tight but need a remote access solution. It’s also a perfect solution for Enterprises who need a remote access business continuity solution.

Asterisk alert*: If you are like me, and see a little * after something, I immediately drop to the bottom fine print to find the catch. FirePass VE is sold & supported just like FirePass hardware and is fully supported on the VMware products listed above. VMware also has a link off their website about the FirePass VE/VMware interoperability. As with any piece of software, there are minimum hardware and configuration requirements along with recommended VM provisioning but actual performance may vary depending on the target system. The FirePass v7 VE release notes *(logon may be required)*** does provide the VMware system minimum characteristics. Just want to properly set expectations, especially with that pesky asterisk. :-)

And one from Confucius: *A man who has committed a mistake and doesn't correct it, is committing another mistake*.

ps

The CloudFucius Series: Intro, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Digg This