VOLUME 8 | ISSUE 6 | November - December 2014

VITAL

INSPIRATION FOR THE MODERN BUSINESS

Smart glasses help the blind "see"

INSIDE

Easing network woes in a cloudy world of change and complexity

The piecemeal transition to a wholly virtual environment is causing IT departments endless security and compliance headaches, but a new breed of software known as security policy orchestration can quell the pain, argues Tufin's ***Reuven Harrison****...*

As organisations seek to gain greater agility and efficiency by virtualising their IT infrastructure and making ever more use of cloud services, they're encountering a big problem: how on earth do they ensure their increasingly complex web of systems and networks remain secure and compliant amid an accelerating onslaught of change?

IT operations staff are constantly having to tweak network and security settings as the business requests swathes of changes to applications and services, as well as to the way these can be accessed (and by whom). In larger firms, this can amount to hundreds of changes every day, which often puts a huge strain on IT resources and hampers businesses' ability to achieve the agility and efficiency gains that virtualisation and the cloud can bring.

Even more worrying, the sheer volume of change, coupled with the growing complexity of their network set-up, means it's extremely hard for firms to ensure that systems remain secure and compliant. A tweak to one part of their architecture can all too easily result in unforeseen changes occurring elsewhere that introduce new security holes, break compliance in some way or otherwise cause things to malfunction.

What about hybrid IT?

Many providers of cloud and virtualisation technologies point out that network management is actually far simpler when you use their systems. Because they are built "virtually" (i.e. in software), management can be fully centralised and automated. Indeed, many organisations are moving towards this world of "software-defined" datacentres and networks precisely because of the increased agility, flexibility and ease of management that it promises to deliver.

VMware, for instance, proclaims that its NSX network virtualisation and security platform can protect software-defined datacentres without having to set up multiple firewalls and internal security checkpoints. The product includes a hypervisor-level firewall that examines all the traffic flowing through dispersed, virtualised networks and gives users a single, software-based control panel to make any changes needed.

While that's all well and good if your IT is fully virtualised, this just isn't the case for most organisations today. Companies typically use a mixture of virtualised systems, cloud services and legacy physical kit in a so-called "hybrid IT" environment. Their move towards the software-defined datacentre and software-defined networks is a gradual transition, so this hybrid environment is likely to remain the dominant model for some time yet. And, even when the transition to virtual is complete, a software-defined datacentre will always be running on top of a physical environment that will still need to be effectively secured.

Security Policy Orchestration

Clearly, if organisations want to achieve the full agility and efficiency benefits of virtualisation during this transitional period and beyond, they urgently require a way to automate and centralise network and policy management across their entire, and increasingly disparate, IT estate – both the virtual and physical parts. Fortunately, there is a solution: Security Policy Orchestration.

Security Policy Orchestration can hook into multiple network management and security systems, mapping out how they all interact and giving users a holistic view and a single point of control over both virtualised platforms like VMWare and over physical networks and traditional security systems. These tools understand the organisation's security and compliance policies, and can ensure every part of the architecture adheres to them, fully automating the task of configuring everything correctly.

This lifts the burden of constantly having to make manual changes to a multitude of different devices, giving IT departments the opportunity to re-deploy newly freed-up human resources into activities that add more value to the business. It also eliminates the constant worry that a misconfigured firewall, system, application or network could open up an organisation to security breaches, compliance failures or system downtime – any of which could result in serious reputational damage and/or financial loss.

"While that's all well and good if your IT is fully virtualised, this just isn't the case for most organisations today. Companies typically use a mixture of virtualised systems, cloud services and legacy physical kit in a so-called "hybrid IT" environment"

But how easy is it for a typical organisation to implement Security Policy Orchestration? Generally, it's best to take a phased approach. First you need to define the policies you need to enforce, as distinct from the technologies doing the enforcement. It is then relatively simple to connect your software to your infrastructure (both the physical and virtual parts), at which point the system will start passively analysing your set-up, giving you valuable insights and alerting you to potential issues – such as any parts of the system that have been misconfigured, or when a change to one part of the system causes a policy breach somewhere else.

Even bigger benefits flow though when you move into the second phase of Security Policy Orchestration deployment – full automation. Once you let the system proactively take control, when you action a change it will automatically make all the necessary configuration tweaks to connected physical and virtual equipment that are required to ensure the organisation still adheres to all of its security, risk and compliance policies.

Automation accelerates the process

As with all process changes or additions, a small investment of time and patience is required as the system matures and settles, but this is very quickly recouped once Security Policy Orchestration is fully up-and-running. Automation massively accelerates the speed at which an organisation is able to make network changes, as well as dramatically reducing its exposure to risk and freeing up even more IT resources. The additional agility and efficiency this enables gives an organisation a clear competitive edge over rivals that haven't embraced Security Policy Orchestration, allowing it to innovate more quickly at lower cost, serve partners, staff and customers more effectively and thus capture more business in the markets it is targeting.

Ultimately, though, all organisations will have to embrace automation. When the legacy systems are finally decommissioned and "software-defined everything" becomes the norm – which won't be that far into the future – all network and policy management (and much more besides) will be automated. The market is heading inexorably in that direction. This immutable fact only makes the case for deploying Security Policy Orchestration now even more compelling. After all, the organisations that get a head start today on what everyone will be doing tomorrow are far more likely to stay in the lead.