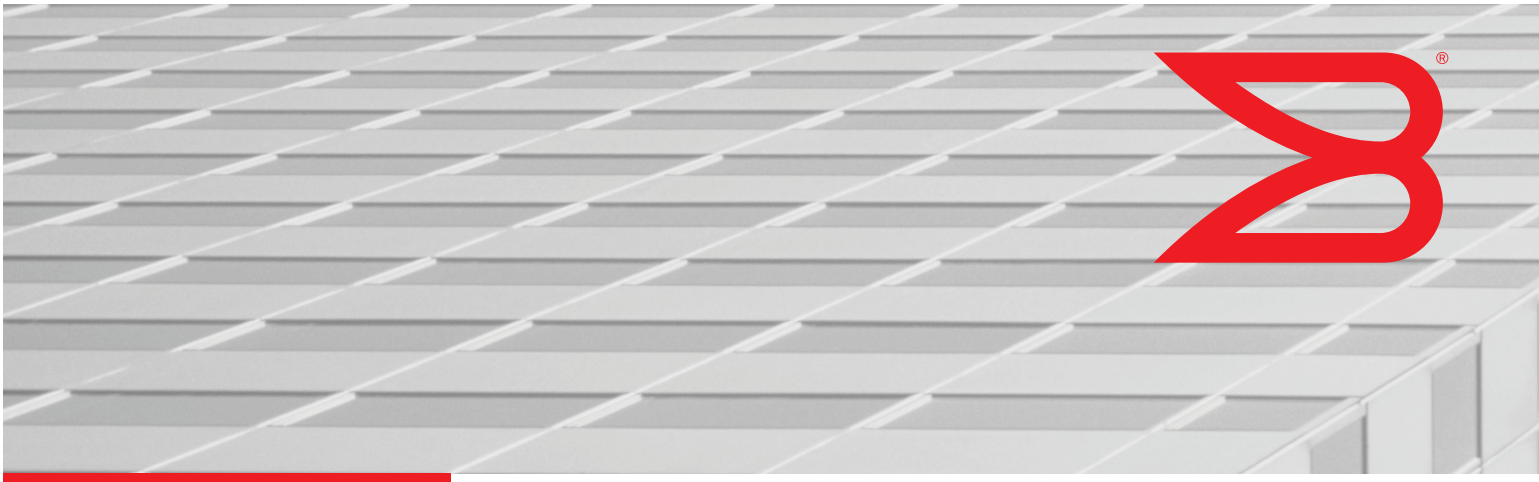

NETWORK FUNCTIONS VIRTUALIZATION

The Top Five Virtualization Mistakes

BROCADE

Virtualization is taking the IT world by storm. After years of IT build-out, virtualization suddenly fixes everything from data center crowding to high cholesterol. But many IT managers are just getting started with virtualization and are employing it in only the most straightforward ways. If you're in this camp, you could be leaving your network vulnerable to attack, needlessly complicating your disaster recovery plan and double-spending on your network infrastructure.

This paper describes five mistakes common to many implementations of enterprise virtualization. Most of these mistakes relate to virtualization and networking infrastructure. Ideally, after reading this paper, you'll be sensitized to these issues so that you can plan for them and make your virtualization projects more successful.

THE TOP FIVE VIRTUALIZATION MISTAKES

Mistake #1: Leaving the network unsegmented

Virtualization represents both an opportunity and a threat. It can generate a huge cost savings in capital equipment and an increase in manageability. However, virtualization introduces a new piece of software to the IT infrastructure, the hypervisor or virtual machine manager. Like any new software, it carries potential risk.

In the same way that an operating system flaw can compromise every application running on that operating system, a flaw in the hypervisor can potentially compromise every virtual machine running in a hardware system. Because of this, it's important for companies to develop a security strategy that addresses the risks associated with the hypervisor itself, particularly as it interacts with the network.

In a recent survey of *Network World* readers[1] who felt that virtualization technology had added a security threat, more than half the respondents said they were dealing with the threat by further segmenting the network.

[1] *Virtual System, Real Risk*, Network World, August 20, 2007, p 30.

Where most networking solutions would require you to deploy additional equipment to solve this problem, the Brocade software-based networking solution implements advanced routing and security functions to segment an existing network within a virtualized environment. Vyatta easily filters traffic running between different subnets and routes between individual VLANs. Using these features, you can allocate separate network segments for each of the applications running in a virtualized environment and help prevent a security breach from spreading beyond the initial intrusion. Figure 1 shows a segmented data center.

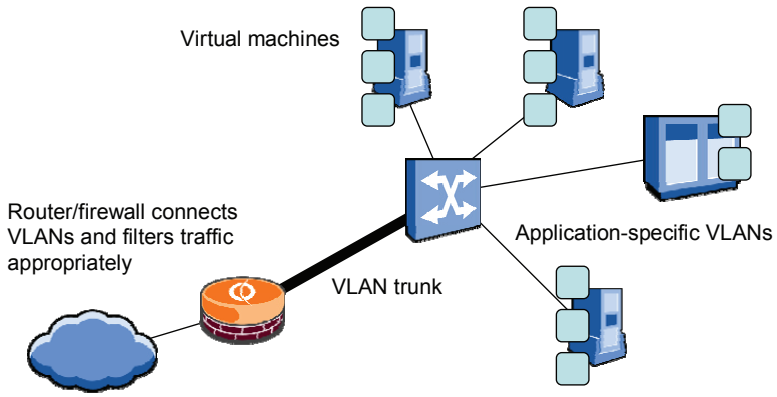

Figure 1.
Brocade Vyatta can be used to enhance data center security by segmenting the LAN into separate application-specific VLANs and providing firewalling between them.

While many routers and firewalls can help you segment your network, Brocade does so at a far lower cost than other solutions. Because Brocade uses x86 hardware, it offers multiple deployment options, saving you money in multiple ways:

- You leverage the commodity pricing of the x86 ecosystem, saving on the initial purchase of a chassis, network interfaces, memory, and other components
- Because you're using commodity hardware, you can typically share components between your firewall/router and the other servers in your data center, reducing sparing costs and increasing availability
- You can easily deploy Brocade Vyatta on blade servers as well as rack-mount or tower systems, allowing you to integrate Brocade into your overall physical infrastructure plan. With blades, you'll be sharing power supplies and fans with all the other infrastructure, improving overall efficiency

Mistake #2: Virtualizing only the servers

Today, most people think of virtualization as a server technology, and indeed it started that way. If you stop at the server, though, you're not getting all the benefits you could from virtualization. Think about virtualizing network functions as well. In fact, some of the greatest capital expense savings will come from network virtualization.

Because Brocade Vyatta runs on standard x86 hardware, unlike proprietary networking products, it can be virtualized with the same hypervisors (VMware, XenSource, Hyper-V, Red Hat KVM, etc.) as server operating systems such as Windows and Linux. Consequently, Brocade Vyatta makes it possible to virtualize the entire infrastructure associated with a given application, including network components.

You can virtualize Brocade Vyatta by putting multiple instances on a single piece of hardware, each serving a different application, as shown in Figure 2. This works well for large data centers and applications implemented with multiple tiers of servers, whether virtualized or not.

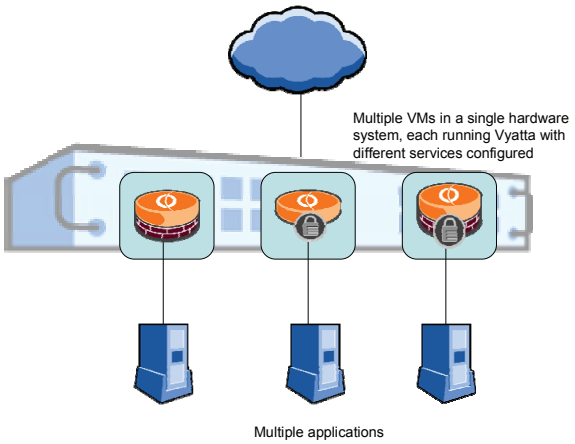

Figure 2.
Using virtualization, you can run multiple copies of Brocade Vyatta on the same piece of hardware, each servicing a different application.

In cases where the whole application is deployed on a single server, the configuration shown in Figure 3 may be more appropriate. In this configuration the virtualized network infrastructure shares the hardware with the application virtual machine. Deploying Brocade Vyatta this way can provide an effective security solution, implementing firewall and VPN services. This technique is particularly useful when adding security services to Internet-facing applications such as Microsoft Exchange mail servers. It can also secure communications to a particular application by placing a VPN in between the application and the clients.

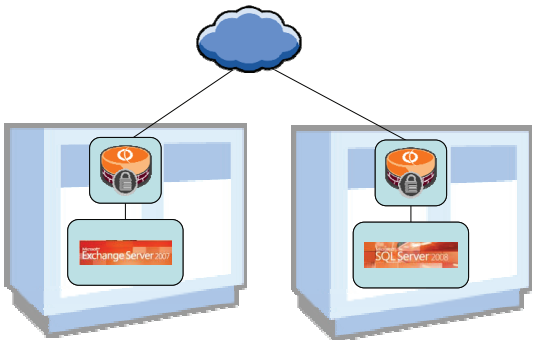

Figure 3.
You can virtualize Brocade Vyatta and co-locate it with an application on the same hardware to provide network and security services.

Mistake #3: Forgetting to virtualize the branch office

In an October, 2006 report titled *The Evolving Branch Office: Intelligently Reducing Your Network Infrastructure Footprint*, Forrester Research addressed the huge push toward branch consolidation. In describing some best practices for branch office consolidation, Forrester listed the challenges associated with trying to implement the holy grail of branch consolidation—the "branch-in-a-box." While there are solutions that deliver substantial

functional integration, Forrester admitted "…realistically we don't see an all-in-one branch solution." In spite of Forrester's pragmatic assessment, you can come close to a "branch-in-a-box" and virtualization can help.

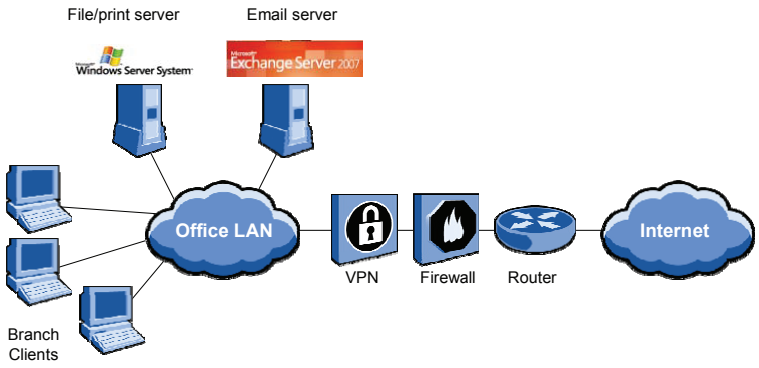

Figure 4.
A typical branch office containing multiple servers and network appliances.

IT managers often think about virtualization in a data center context. However, as shown in Figure 5, virtualization can also help consolidate multiple disparate applications and systems onto the same hardware in a branch office. For example, with virtualization, local mail and file servers can be consolidated onto a single server, even if they are running different operating systems.

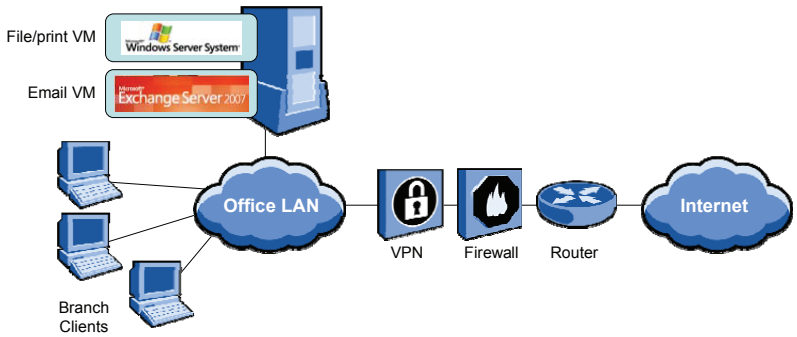

Figure 5.
You can use virtualization in the branch office to consolidate servers onto a single hardware system.

You can take this one step farther, however. Rather than waiting for a single vendor to deliver an "all-in-one branch-in-a-box" solution, you can build your own "best-of-breed branch-in-a-box" from individual parts. Using Brocade Vyatta and virtualization, you can virtualize the router, firewall, and VPN that connect the branch office to headquarters, along with the file/print and email servers. Figure 6 shows this configuration.

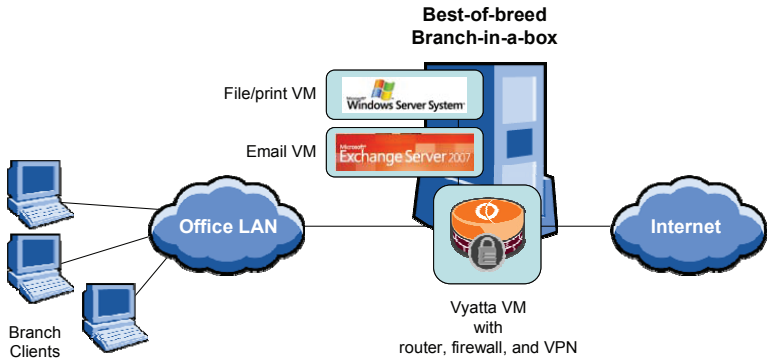

Figure 6.
Using Brocade Vyatta and virtualization, you can create a best-of-breed branch-in-a-box containing multiple servers and networking functions.

Mistake #4: Forgetting to virtualize the network as part of the disaster recovery plan

Companies plan very carefully for all kinds of disasters—from earthquakes to malicious code. Crucial applications are backed up; data centers have redundant equipment and power, all to make sure that companies can get back to business as quickly as possible. Virtualization adds a great technology to help deal with disaster recovery. Some hypervisors support snapshots and automatic migration of virtual machines from one physical system to another, making it far easier to move a data center's-worth of infrastructure from one location to another, nearly instantaneously, in the event of a disaster. This rapid-migration capability makes it much easier to come up with a disaster plan. As an added benefit, such features also speed routine data migration projects.

Unfortunately, many IT managers concentrate their disaster planning efforts on the servers and applications and assume that the network will provide the set of services they need to keep users connected. When it comes to basic L2/L3 infrastructure such as switching and routing, you'll want to provision connectivity to both your primary and backup locations. But are network services such as firewalls and VPNs part of the network itself, or should they really be considered part of the applications running on the servers? To put this question into sharper focus, if you have a firewall at your primary site, are you diligent about replicating all firewall rule changes over to your disaster recovery site? Do you keep your firewall firmware patched and updated to the latest revisions at the backup site?

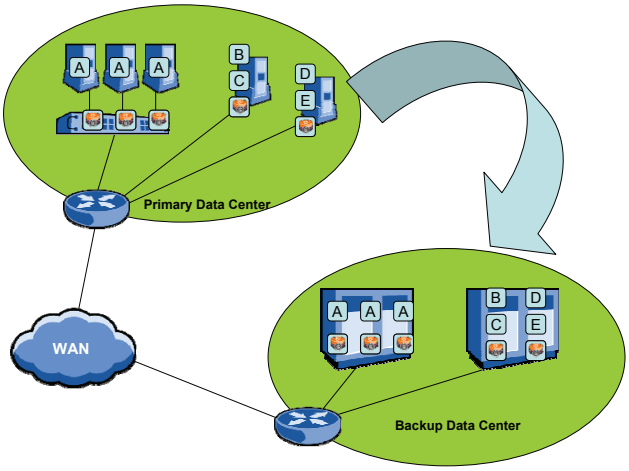

Figure 7.
Using Brocade Vyatta with virtualization makes it easy to replicate firewall and VPN configuration to a disaster recovery site along with other application state.

Virtualization can help us with this problem, once again. As Figure 7 shows, rather than provisioning identical proprietary firewall equipment in both locations and worrying about keeping firmware and configurations synchronized every time something changes, simply replicate a firewall virtual machine from one location to another, just as you would an application server. Depending on how you have built your network, the configuration should be relatively compatible with the new site (possibly needing some IP address adjustment). Develop a short set of step-by-step instructions to make the required changes as part of your disaster plan. Using this technique, you can be assured that your backup site is fully updated with the firmware revision and configuration of the primary site—because it's running the same virtual machine as the primary site.

Mistake #5: Forgetting to sell your old hardware on Ebay

Once you have implemented your virtualization plan, don't forget to sell all that old proprietary networking hardware on eBay. You can recoup at least some of your original investment and use that to fund an expansion of your virtualization strategy.

FINAL CHECKLIST

To get the most out of your virtualization project and to avoid common mistakes, here's a checklist to use in planning.

1. Look for unsegmented networks that might be at risk from virtualization and use virtualization tools to segment them.
2. Look at the networking functions associated with servers you plan to virtualize and virtualize them together.
3. Consider networking functions such as routing, firewalls, and VPN as part of branch virtualization projects. Putting them on the same hardware as other applications will get you a long way toward "branch in a box."
4. Use virtualize to include network functions in disaster recovery plans, so that when there's a disaster, your routing, firewall, and VPN will come back online along with the rest of your compute resources.
5. Sell off specialized network hardware on eBay. By using x86 hardware and virtualization, you'll save money on purchase, operation, and maintenance.

More more information, visit www.brocade.com

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.co

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE