Global Knowledge®

Expert Reference Series of White Papers

Using VMware NSX for the Microsegmentation of Security

Using VMware NSX for the Microsegmentation of Security

Bill Ferguson, VCI3,4.5,6, CCSI, LVCI, and MCT Alumni

Introduction

In the past, before we had virtual machines (VMs), each of our servers existed in a specific physical location and rarely if ever moved from that location. Therefore, we configured our security policies to either allow or deny traffic to and from that physical location. I can remember setting up powerful (at that time) firewalls called "bastion hosts" that stood between one part of my network and another to protect my servers. The rules that we applied to those firewalls were customized to take into account the specific physical location of each resource. After all, how else could one secure anything?

Well, times have changed and the explosive growth in software-defined data centers (SDDCs) and SDNs makes it mandatory that we find a new and better solution than we've used in the past. Most businesses have hundreds or even thousands of applications that they need to protect. Each of these applications may require a different type of protection with different security parameters needed to protect the data and connectivity of the application. In addition, these applications are not necessarily "sitting still" in the same physical location anymore. In fact, services such as VMware's vMotion can move a running VM server from one physical location to another, and services such as Distributed Resource Scheduler (DRS) can automate those moves to balance compute loads across hosts in a cluster. Because of these new capabilities to "play musical chairs" with our servers, we need to be able to control their security without regard to their physical location. That way, we can keep our data and networked applications safe; regardless of where their servers are located. VMware NSX provides not only a virtualized network but also the possibility for microsegmentation of security. *The microsegmentation of security is the ability to individually configure and continue to apply security for each connection on every VM on your network regardless of its physical location; and regardless if the VM is moved to another physical location.*

Therefore, since each of your VMs are running a specific application on a specific connection, you can configure that application with its own specific security parameters. This flexibility of security gives you the power to secure your data and your network assets in exactly the way you need for every application. While this may sound complicated at first, it's actually easier than the security methods of the past, once you get your head around it. In addition, VMware NSX provides tools and software to make it simple to incorporate many third-party tools for guest and network introspection. In this paper, I will examine all three of these important concepts regarding the microsegmentation of security using VMware NSX.

Using NSX provides for the microsegmentation of security in a virtualized network

The use of SDN transforms your network into logical switches that span an entire transport zone, which could be your whole data center. Once your VMs are connected to the logical switches, they are on a virtual wire that connects them to the other logical switches through a Distributed Logical Router (DLR). The main point is that they will then connect to other networks in exactly the same way regardless of which physical host is currently providing the VM with its compute resources.

Therefore traditional concepts, such as the location of the VM and one side of the firewall or the other, completely go away and are replaced by concepts such as the business purpose of the VM, regardless of where it is located in the physical network. This in turn transforms the options that you have as a network administrator in regard to security and traffic control. Figure 1 illustrates this concept. Note that each of the logical switches (Web, App, and DB) span the entire transport zone.

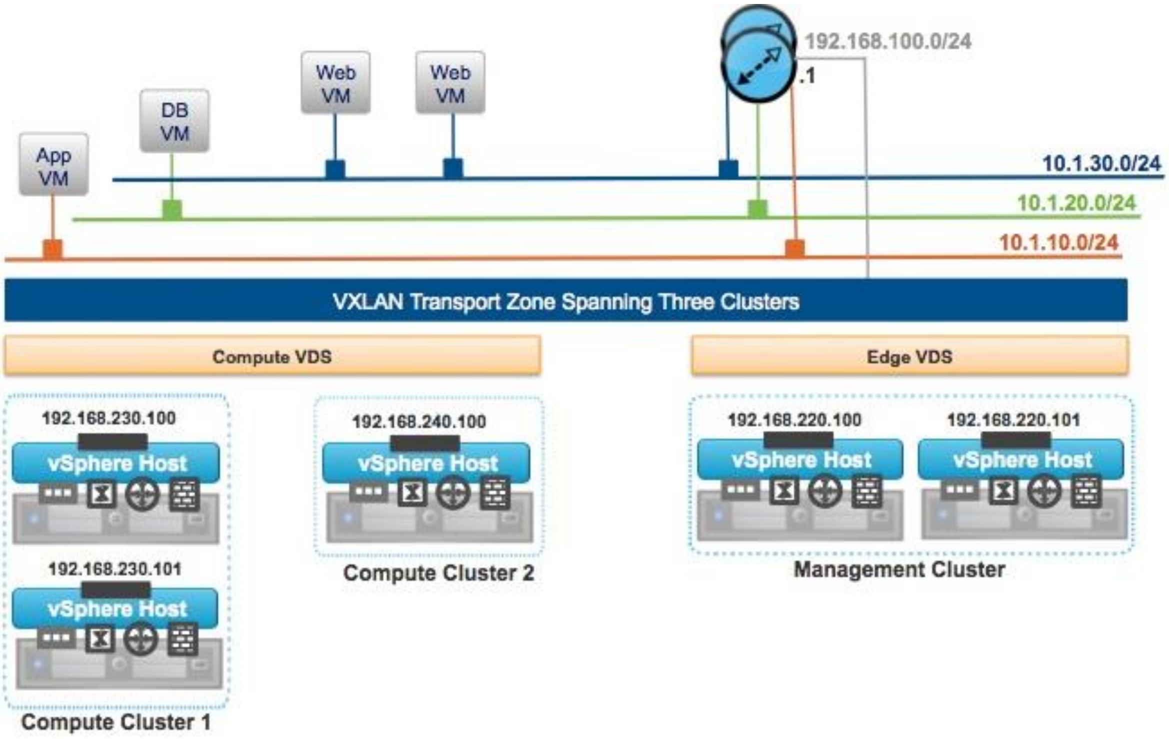


Figure 1. NSX Logical Switches Span the Transport Zone

In addition, the concept of what side of the firewall a VM is on can also completely go away because NSX uses a distributed logical firewall that is based in the VMkernel. Without getting too deep here, basically what that means is that the firewall configuration for each VM's virtual network interface card (vNIC) is in the same exact software that created the VM in the first place. That means the rules that you use to configure the distributed logical firewall will become part of the DNA of the virtual machine itself, and will thereby control the behavior of each vNIC on every VM in regard to what traffic it wants to send and what traffic it wants to receive.

In other words, rather than have a separate firewall component with which the VMs compete, or which must be configured properly to traverse, this software works as one cohesive system to control the data traffic in a very logical fashion (please pardon the pun). Furthermore, since you can control traffic on every vNIC of every VM, you can therefore control traffic within a logical switch just as easily as between two logical switches. In other words, you don't have to send the traffic through a router to apply the rules to it. This means you can easily configure rules that govern how VMs can communicate to each other, regardless of whether their vNICs are on the same logical switch or not.

This in turn means that you can create rules that are based on business context without limitation in regard to the physical location of the VM, its logical location or where it's taking its compute resources. Figure 2 illustrates the concept of the distributed logical firewall in NSX. Note that the distributed logical firewall is actually enforced on each of the vNICs on each VM.

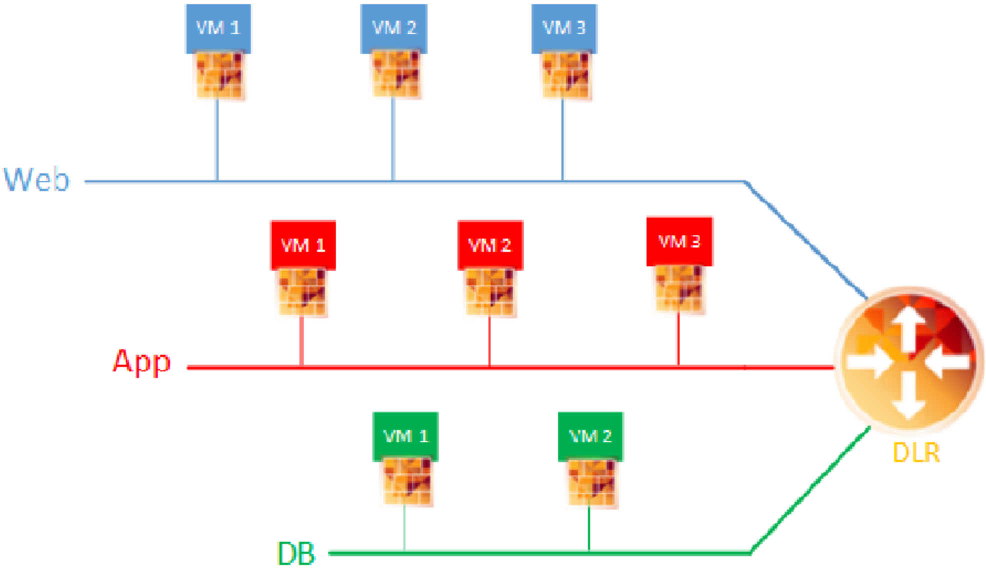


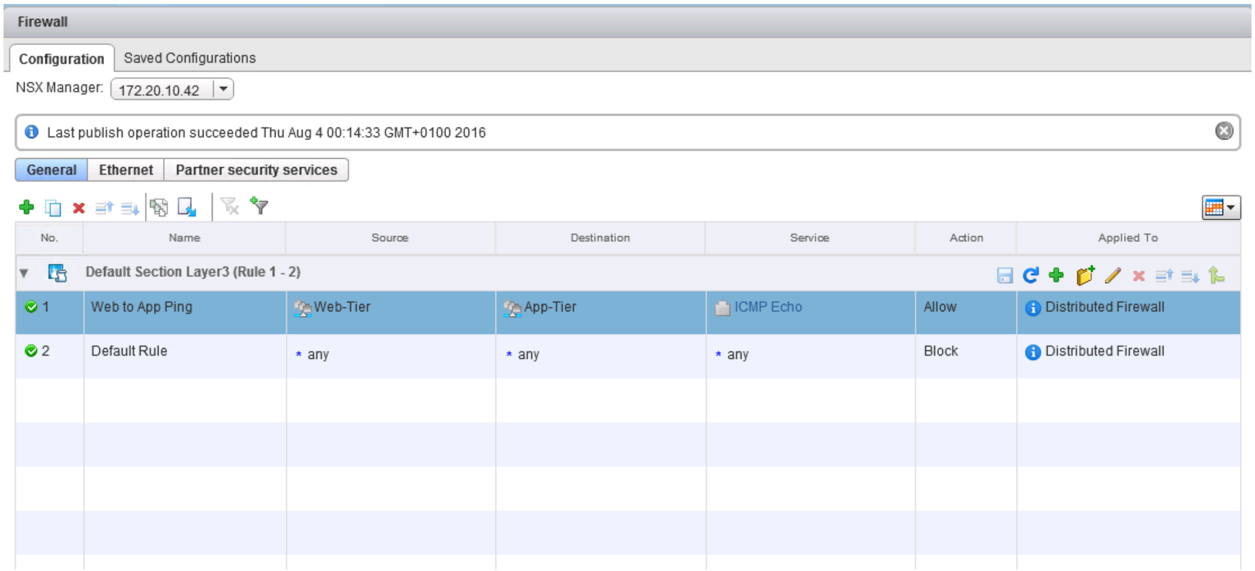
Figure 2. The Distributed Logical Firewall Is Enforced on Each vNIC

Controlling security with a virtualization context is actually easier than with traditional methods

Now you might be thinking that something this complex must be very difficult to configure, but actually just the opposite is true. After you strip away all of the physical aspects such as the actual physical location, IP address, and so on, you can then focus directly on the business context of the VM or the logical switch to which it's connected. In addition, firewall rules based on virtualization context do not require a change every time you add another VM to that broadcast domain. For example, when you add a new Web VM to the Web virtual wire, the new VM will be governed under the same set of rules as all of its predecessors—automatically!

The main reason this is possible is that the firewall rules that protect your data and assets are based on the virtualization context, without regard to the physical location of the VM. Figure 3 shows a distributed logical firewall rule that will allow any VM in the Web Tier logical switch to ping Internet Control Message Protocol (ICMP) echo for any VM connected to the App Tier logical switch. Note that the default rule will prevent any other traffic. This is just a very small example of a virtualization context rule, to help you see how the microsegmentation of security can be a powerful tool for your data center.

For example, you could allow only specific VM servers to communicate to a remote data center, based on the logical switches that the VMs are on. That way, if you want another VM to also be able to communicate to that data center, you have only to connect it to the appropriate logical switch. In addition, you could allow communication that originates on one of your logical switches to connect to another while at the same time not allow the communication to be originated from the receiver; and you can do this in plain English without regard to IP addresses or the physical locations of the servers.



NSX Manager: 172.20.10.42

Last publish operation succeeded Thu Aug 4 00:14:33 GMT+0100 2016

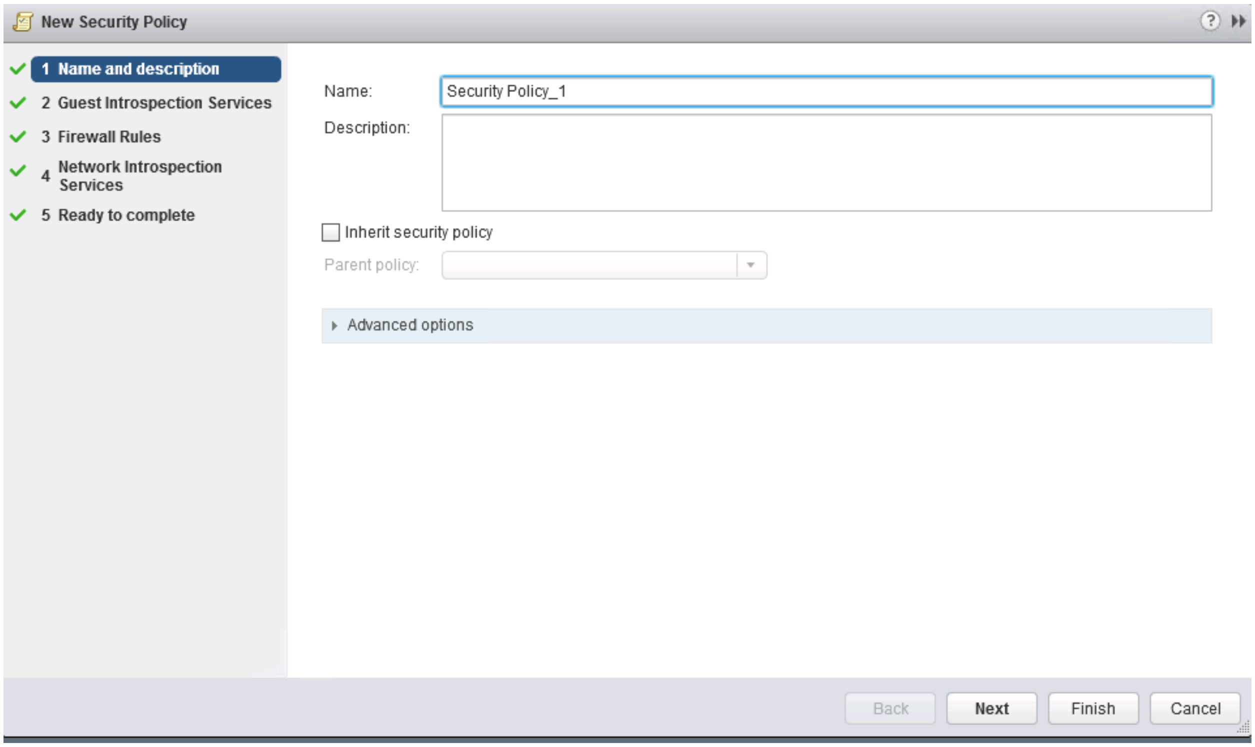
No.	Name	Source	Destination	Service	Action	Applied To
Default Section Layer3 (Rule 1 - 2)						
1	Web to App Ping	Web-Tier	App-Tier	ICMP Echo	Allow	Distributed Firewall
2	Default Rule	* any	* any	* any	Block	Distributed Firewall

Figure 3. A Distributed Firewall Rule with Virtualization Context

NSX also provides a simple way to incorporate many third-party security applications

NSX includes a feature called Service Composer that enables you to easily incorporate third-party security tools into your security design. For example, you can redirect traffic to a Palo Alto Networks (PAN) firewall or network introspection device by identifying the source and destination addresses of the traffic that is to be redirected. In addition, you can force specific types of communication to undergo additional guest introspection, such as with Trend Micro or McAfee anti-virus software.

Figure 4 shows the wizard with which you build your Service Composer policy rules. Note that you can easily integrate guest introspection, firewall, and network introspection rules and services into the same security policy.


New Security Policy

- ✓ 1 Name and description
- ✓ 2 Guest Introspection Services
- ✓ 3 Firewall Rules
- ✓ 4 Network Introspection Services
- ✓ 5 Ready to complete

Name: Security Policy_1

Description:

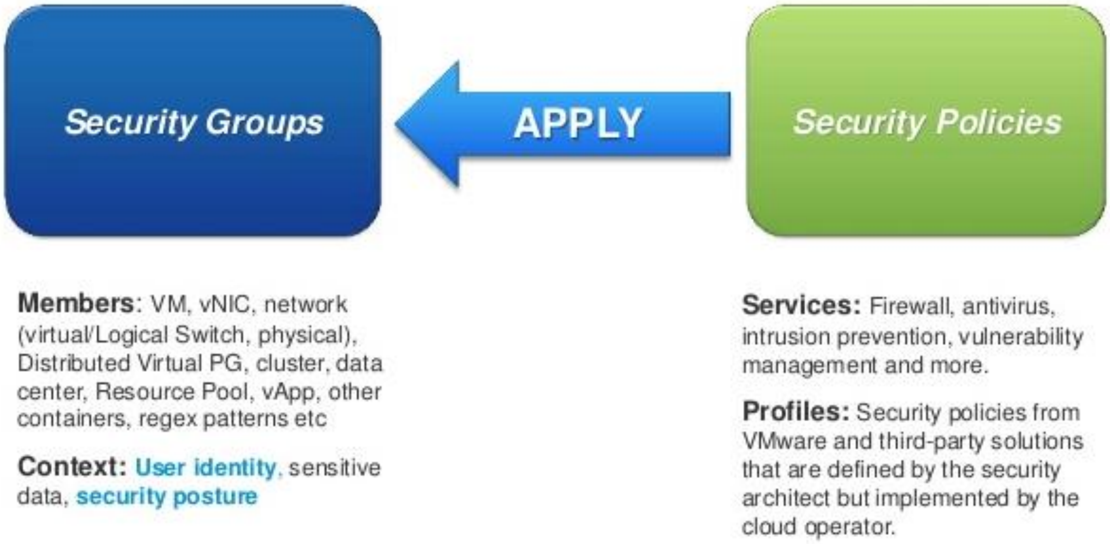
□ Inherit security policy

Parent policy:

Advanced options

Figure 4. The New Security Policy Wizard

Here again, something that seems like it might be difficult is made much simpler because the physical location of the resource creating the traffic is often not even in consideration. Because of this, you simply identify what you want to protect with a security group, then identify how you want to protect it with a security policy, and finally apply the security policy to the security group as shown in Figure 5.



Members: VM, vNIC, network (virtual/Logical Switch, physical), Distributed Virtual PG, cluster, data center, Resource Pool, vApp, other containers, regex patterns etc

Context: User identity, sensitive data, security posture

Services: Firewall, antivirus, intrusion prevention, vulnerability management and more.

Profiles: Security policies from VMware and third-party solutions that are defined by the security architect but implemented by the cloud operator.

Figure 5. Applying a Security Policy to a Security Group

Now, you may wonder how to attach all of these new third-party security features to your existing NSX. Basically you do whatever the third party says to do. You will be adding a new Service Definition to your system by registering it with the third party involved. Some companies will install a virtual appliance as part of their service, while others will not need that component. You will, of course, need your administrative credentials and the fully qualified domain name of the system to which you are adding the Service Definition.

Speaking of administration, you might also wonder how you are supposed to determine the end result and make sure that it's what you intended. Service Composer uses an ingenious software tool called a Canvas for each security group that you create. By viewing the Canvas of your security group, you can not only see what policies are applied to the group, but also the members that resulted from your selection process. Figure 6 shows Canvases for multiple security policies. At first it might seem like it can't be that easy and that there must be something missing from the information. Upon closer inspection, what you'll find is that the piece of information that is missing is the physical location of the resource, and the reason that it's missing is that it doesn't matter. Security policies based on components of your SDN will operate exactly the same regardless of the physical location of the VM.

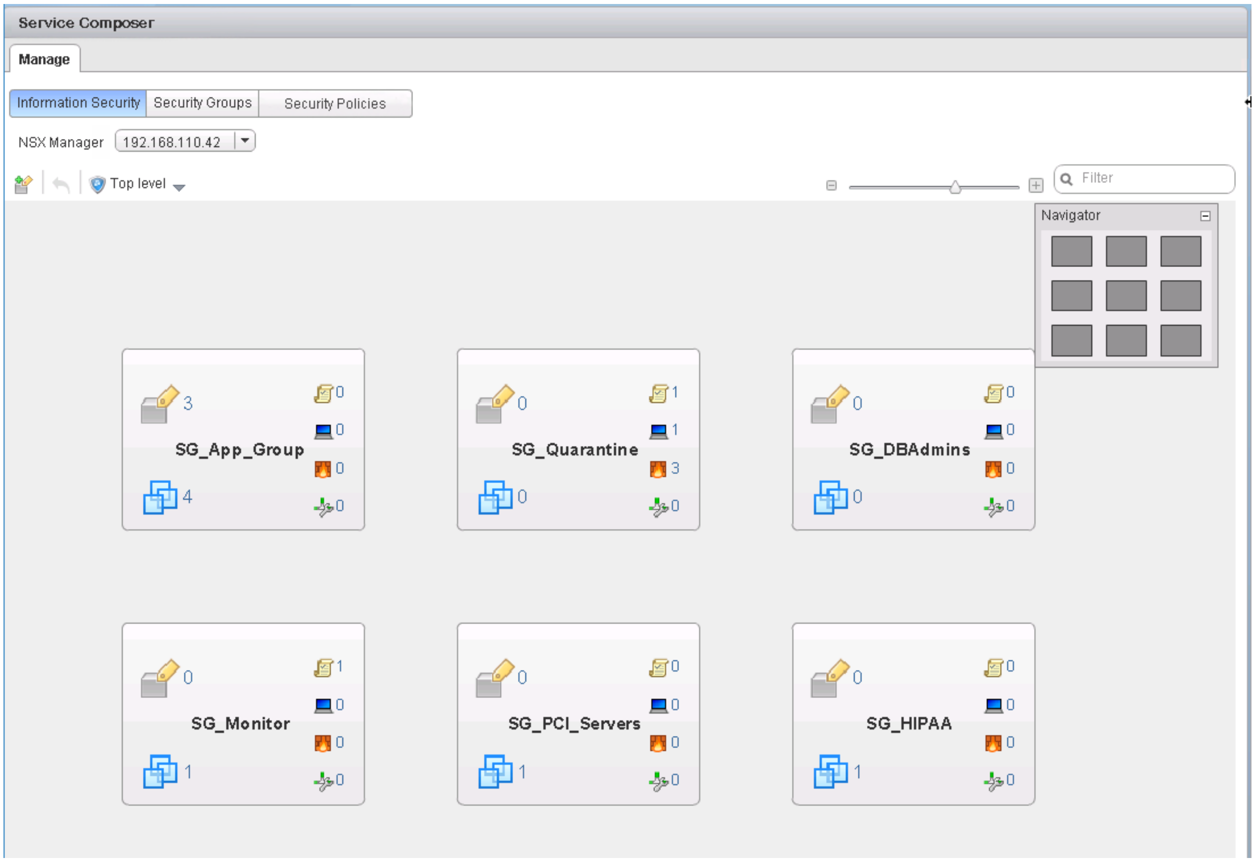


Figure 6. Canvases for Multiple Security Policies

Conclusion

The methods of security that we have used in the past are not scalable into the future. Using NSX provides not only for a virtualized network, but also delivers a platform for the microsegmentation of security. The microsegmentation of security makes it possible to configure specific security settings on each of your applications and to continue to apply the settings regardless of the location of the server providing the application. Using a virtualization context to manage security allows for an easier way to keep your data and networked applications safe. You can manage your network connections using business terms instead of, or in addition to, IP addresses and subnets. Your NSX network will also integrate easily with the third party's for network introspection and guest introspection services. All of these features can help organizations manage security with microsegmentation down to the individual application, VM, or vNIC, enabling even large organizations with multiple tenant environments to keep their data and networked applications safe, now and into the future.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

VMware NSX: Install, Configure, Manage [V6.2]

VMware NSX for Internetworking Experts Fast Track [V6.1]

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Bill Ferguson, VCI3,4.5,6, CCSI, LVCI, and MCT Alumni has been in the computer industry for over 25 years. Ferguson runs his own company as an independent contractor in Birmingham, Alabama, teaching classes online and in person for many national training companies, including Global Knowledge. Additionally, Ferguson has written and produced many technical training videos including various Exam Cram, Sybex/Wiley Press, and Pearson/VMware Press titles. His latest publications include "vSphere 6 Foundations Exam Official Cert Guide" (Pearson/VMware Press 2016) and video courses including "Up and Running with NSX" and "Learn VMware NSX Security" (Lynda/Linked-In 2016).

Ferguson's aspiration is to know the technical material so well that he make it easier for you to learn than it was for him to learn!