Realtime publishers

The Essentials Series:
Virtual Security Concerns & Solutions

Understanding & Improving Virtual Network Security

sponsored by

eEye Digital Security®

by Greg Shields

Understanding & Improving Virtual Network Security 1

The Effect of Machine Migrations on Networking...3

Implications of Cross-Virtual Machine Traffic 4

External Agent-Based Approaches Overcome Virtual Transience 4

Copyright Statement

Understanding & Improving Virtual Network Security

A virtual network is not the same thing as a physical network. You've seen virtual networks before. These are the networks created inside most enterprise-class virtualization solutions for connecting virtual machines to each other and the outside world. They create linkable virtual switches that leverage a virtual host's internal bus rather than its network card to connect virtual machines to each other. Virtual switches can also be attached to physical interfaces in the server in complex ways to route virtual machine traffic over multiple external networks. A graphical representation of this is seen in Figure 1.

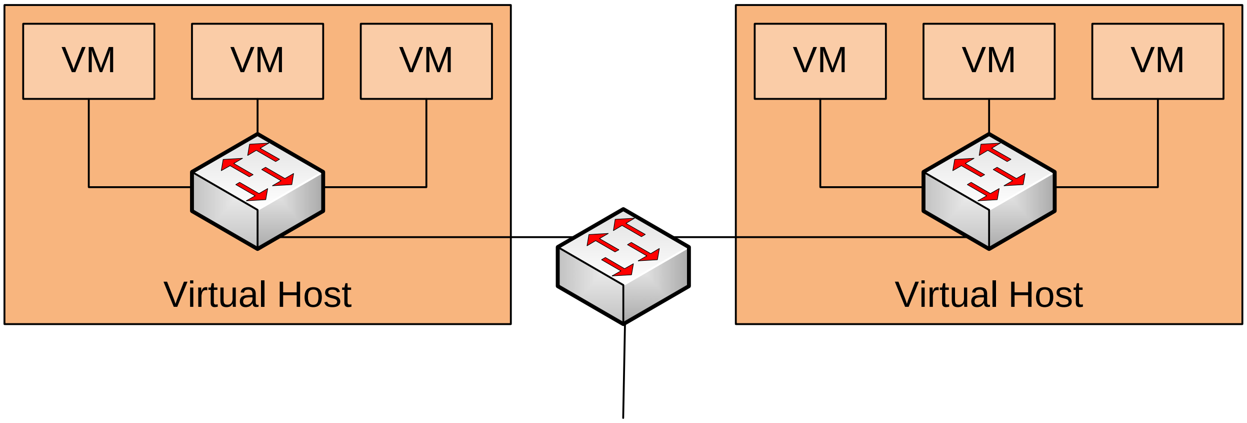

Figure 1: Virtual switches connect virtual machines to each other and the outside world.

Yet these virtual networks are indeed not the same as their physical equivalents. Though they appear at first blush to provide much of the same functionality as seen with traditional networks, these networks are special. The level of functionality they provide is quite different than you're used to seeing with your Cisco or Juniper devices. For example:

- *Hubs vs. switches.* Many virtual switches actually function as network hubs rather than network switches. This support varies by vendor but can be a critical difference in how you want to set up your virtual networking infrastructure within a virtual host. Switches by nature have the ability to segregate traffic across ports, isolating traffic to only its destination host. This process reduces the effect of improperly configured network cards while eliminating the ability to promiscuously sniff for traffic intended for other hosts. If your virtual network environment is not fully trusted, a hub-based virtual switch may not provide the level of security you require.
- *Layer 2 vs. layer 3.* The virtual switch itself in most virtualization platforms today operates at the OSI model's layer 2 rather than layer 3. Most physical infrastructures today have elevated their network configuration beyond the limitations of layer-2 switching due to the need for layer 3's configurable virtual routing. With virtual switches operating at layer 2 instead of layer 3, it can be difficult for virtual routing to be correctly applied. Many virtual platforms leverage external mechanisms for the support of VLANs, yet these tend to be proprietary in nature.

- *Access control.* Virtual switches are often wide open in terms of access control, with no capabilities for the assignment of per-port access control lists (ACL). This lack of effective access control means that external traffic destined for virtual machines within a virtual host can often only be controlled to the point of the virtual host itself—though again some proprietary VLAN support is often available. This lack of internal ACLs also means that virtual machine-to-virtual machine traffic within a virtual host is similarly uncontrollable. When virtual machines need to interconnect with other virtual machines via a controlled interface, often the only mechanism to support this need is through the creation of a third firewall-type appliance that controls that traffic between each. This firewall-type appliance can impact available resources needed for its processing and its positioning must be carefully controlled as the migration of virtual machines occurs over their operational life cycle.
- *Switches vs. routers.* Virtual switches are simply that: switches. Thus, if routing support is necessary, an external device or virtual appliance that supports routing is necessary. As discussed earlier, the same elements associated with router appliances can used for virtual firewalling. As virtual switches, their native functionality often lacks the advanced protocol support used by routers for the routing of network traffic.
- *Layer-4 protection.* Lastly, as layer-2 devices, virtual hardware today cannot protect individual virtual machines from traffic arriving over specific ports. Layer-4 ACLs allow traffic to route to a network endpoint but restrict that traffic to network ports that are appropriate for the services being hosted atop that endpoint. Without built-in layer-4 protection, it is challenging to lock down the traffic routed to virtual machines to only appropriate ports.

Care must be taken when incorporating the use of virtual machines in the environment when security configurations require advanced network configurations. Those network configurations may not be possible using virtual networking due to these inherent limitations.

The Effect of Machine Migrations on Networking

Another facet of virtual networking that must be considered is how virtual networking is impacted by the effects of virtual machine migration. All enterprise-class virtualization platforms include the ability to hot migrate virtual machines from one host to another. This hot migration may occur for resource load-balancing purposes or as an automated action that occurs with the loss of a virtual host. In either case, that migration has the potential to impact networking in a number of different ways:

- *Source and target host virtual networking mismatch.* When a virtual machine is migrated from one host to another, there is the possibility that elements of its networking configuration at the virtual switch layer may not follow. Testing must be done to ensure that the virtualization platform successfully transfers the virtual switch configuration with the virtual machine during a migration event.
- *External networking configurations.* When external networking configurations are targeted on a per-virtual host basis, there is the potential that migrated virtual machines will begin service after a migration at their target virtual host without the correct networking as seen by external network equipment. External networking equipment must be configured with the flexibility to quickly "find" the relocated virtual machine and reconfigure to support its new location.
- *Speed of convergence and name resolution update.* A situation that is arguably more problematic in migrations that occur across subnets—such as in a disaster recovery situation—the timing of network convergence and name resolution must occur at a rate that is acceptable to connecting clients. Convergence embodies the amount of time required for the network as a whole to recognize the changes to routing associated with a change to the topology. Name resolution refers to the need for resolution mechanisms such as DNS to properly update across the organization with the virtual machine's new location.
- *Inappropriate cross-virtual machine communication.* Lastly are the concerns of virtual machines that should not have the ability to directly communicate with each other. A more detailed example of this type of communication is provided in the next section. These may be one business unit's application that must not communicate with another's due to line-of-business regulatory or legal considerations. Organizations that leverage virtualization and who operate under these restrictions must be aware of and compensate for the potential for inappropriate cross-virtual machine communication.

Implications of Cross-Virtual Machine Traffic

The best way to explain the final bullet in the previous section is through the use of an example. Consider a financial institution that runs an internal payroll application in addition to its front-end finance tools. Although these may leverage the same technology for their operation, legal and compliance regulations may require the isolation of these two applications from each other. The internal finance application must never have direct—for example, non-firewalled or uncontrolled—communication with the front-facing application.

When these two applications are hosted in a physical environment, it is relatively easy to ensure that their communication remains controlled at the network layer. Setting ACLs within the network infrastructure to prevent cross-communication is a trivial matter. Neither physical instance has the need or the ability to relocate its position on the network.

Yet when those applications are virtualized, the situation changes significantly. Their initial positioning within the virtual infrastructure may keep them segregated from each other. However, over time, the virtual infrastructure's load-balancing or high-availability features may later result in both virtual machines landing on the same virtual host. Assuming that external networking protections are put in place to appropriately isolate traffic as the machines migrate, once both virtual machines are collocated on the same host, they may begin cross-communicating via the internal virtual switch. Considering the limitations discussed earlier, this situation could violate the required segregation of these two virtual machines. To resolve this situation, techniques can be implemented such as advanced TCP/IP security on the host or the use of a third-party agent-based solution. These solutions enable administrators to ensure that cross-communication does not occur even as virtual machines migrate from host to host.

External Agent-Based Approaches Overcome Virtual Transience

Necessary in these instances are external tools that enable advanced networking functions similar to those discussed earlier. When native tools are not enough to provide the level of network agility required by the complex business, external tools may be necessary to manage network connectivity between virtual machines. Segregated solutions that incorporate vision outside the confines of the virtual infrastructure ensure that no matter where virtual machines go they are always under management. Agent-based solutions within the virtual host ensure that actions can be implemented based on the monitoring data gathered through the segregated tool.