Securing Flat Networks

Network administrators who adopt flat networks to improve performance and support virtualization don’t have to give up on security controls. We explore Layer 2 security options for physical and virtual networks that can keep traffic properly segmented.

By Richard Dreger
<table>
<thead>
<tr>
<th>3</th>
<th>Author’s Bio</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Executive Summary</td>
</tr>
<tr>
<td>5</td>
<td>The World Is Getting Flat</td>
</tr>
<tr>
<td>5</td>
<td>Figure 1: Use of Virtualization Technologies</td>
</tr>
<tr>
<td>6</td>
<td>Old Faithful: Layer 3 Filtering</td>
</tr>
<tr>
<td>6</td>
<td>Figure 2: Three Segmentation Scenarios</td>
</tr>
<tr>
<td>7</td>
<td>Figure 3: Importance of LAN Equipment Features</td>
</tr>
<tr>
<td>8</td>
<td>Moving to Layer 2</td>
</tr>
<tr>
<td>8</td>
<td>Three Controls</td>
</tr>
<tr>
<td>8</td>
<td>Figure 4: Private VLAN Choices</td>
</tr>
<tr>
<td>9</td>
<td>Figure 5: Supported Networking Technology</td>
</tr>
<tr>
<td>11</td>
<td>Virtual Security</td>
</tr>
<tr>
<td>12</td>
<td>Figure 6: Unified Stacks Incorporating Virtualized Networking and Storage</td>
</tr>
<tr>
<td>13</td>
<td>Four Reasons to Get Flat</td>
</tr>
<tr>
<td>15</td>
<td>Related Reports</td>
</tr>
</tbody>
</table>

---

**ABOUT US**

*InformationWeek Reports*’ analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at awittmann@techweb.com, content director **Lorna Garey** at lgarey@techweb.com, editor-at-large **Andrew Conry-Murray** at acmurray@techweb.com, and research managing editor **Heather Vallis** at hvallis@techweb.com. Find all of our reports at reports.informationweek.com.

---

**S e c u r i n g  F l a t  N e t w o r k s**
Richard Dreger is president of WaveGard, a vendor-neutral security consulting firm. Rick has significant, broad-based technology experience with extensive skills in the information assurance, security and wireless networking fields. He has consulted for a wide breadth of clients in both the public and private sectors, and his professional background includes more than 15 years of experience in Fortune 100 companies as well as smaller technology consulting firms. Rick has complemented his hands-on consulting experience by leading courses such as the CWNP wireless curriculum and the (ISC)2 CISSP review.

In addition to being one of the 11 founding members of the Certified Wireless Network Experts (CWNE) roundtable, he is also coauthor of the Certified Wireless Security Professional (CWSP) v2 study guide and numerous InformationWeek articles. Rick obtained his BSE from Duke University and his Masters from Villanova University.
There’s a debate emerging in the IT community about the use of flat networks vs. traditional tiered networks. In a flat network, hosts on the same subnet don’t require the use of a Layer 3 switch or router to communicate. This reduction in L3 activity can make flat networks more efficient and increase network performance. Flat networks can also support highly virtualized environments and key virtualization features such as virtual machine migration.

However, by moving to a flat network, common L3 filtering controls such as firewalls and access control lists won’t necessarily be available because more devices will sit on the same subnet. But this doesn’t mean giving up on security controls. A variety of Layer 2 technologies are available for physical networks and virtualized environments that let IT restrict communications among devices.

We’ll look at control options such as VLAN access control lists (VACLs) and private VLANs (PVLANs). VACLs can be set up to block specific traffic types, and can provide fine-grained control around which devices are allowed to communicate with other devices on the same subnet. PVLANs provide broad segmentation of Layer 2 traffic, and can be used to restrict intra-device communication.

We’ll also look at the use of port profiles and security profiles for use in virtualized environments. These mechanisms apply a predefined set of policies and configurations that determine access controls and other security rules. These profiles remain with the VM regardless of its location. Given the highly automated nature of VM creation, and the ability of VMs to move among physical servers, having predefined security settings that are included when a VM is created helps IT maintain its security controls.
The World Is Getting Flat

Flat networks are a hot topic in IT. Calling a network flat simply means that the networked hosts have IP addresses on the same subnet and do not require the use of a router or Layer 3 (L3) switch to communicate. As long as we know the destination IP and MAC addresses, we can send the frame via physical or virtual switches that are optimized to transmit packets very quickly without the need to route between different networks. If we do need to talk between subnets, then we must employ routing, which takes us further up the OSI model (from Layer 2 to Layer 3) and thus makes the communication more tiered and less flat.

Flat networks have the potential of being faster than a tiered network because the reduction in L3 routing enables more direct the communication flow between devices. Flat networks also can facilitate features such as VM mobility, which allows virtual machines to move from one physical server to another.

However, a shift to flatter networks introduces a familiar security conundrum: How do we properly balance performance against risk? In particular, the removal of L3 boundaries starts to erode the network defense-in-depth model. Here’s why. Basic firewalls and access control lists (ACLs), two of the most common network filtering controls, usually operate on L3 network parameters (for example, IP addresses). Data flows originate from and are delivered to particular IP addresses or groups of addresses. Security policies and sys-

**Use of Virtualization Technologies**

<table>
<thead>
<tr>
<th>Virtualization Type</th>
<th>Extensive Use</th>
<th>Limited Use</th>
<th>Evaluating</th>
<th>No Use/No Plans for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server virtualization</td>
<td>79%</td>
<td>18%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Storage virtualization</td>
<td>27%</td>
<td>30%</td>
<td>24%</td>
<td>19%</td>
</tr>
<tr>
<td>Application virtualization (e.g., ThinApp/XenApp)</td>
<td>15%</td>
<td>27%</td>
<td>33%</td>
<td>25%</td>
</tr>
<tr>
<td>Desktop virtualization</td>
<td>11%</td>
<td>33%</td>
<td>42%</td>
<td>14%</td>
</tr>
<tr>
<td>Network virtualization (e.g., OpenFlow, Cisco Nexus, NextIO, HP)</td>
<td>10%</td>
<td>20%</td>
<td>26%</td>
<td>44%</td>
</tr>
<tr>
<td>I/O virtualization</td>
<td>10%</td>
<td>27%</td>
<td>29%</td>
<td>34%</td>
</tr>
</tbody>
</table>

Data: InformationWeek 2011 Virtualization Management Survey of 396 business technology professionals, August 2011
tem requirements dictate the filtering rules that manage which IP-to-IP flows should be permitted or denied. By removing this familiar inter-subnet role and putting more devices on the same subnet, we lose a security tier—our ability to filter certain data flows at L3.

However, there are controls that can be implemented at Layer 2 (L2). This report discusses the concept of maintaining or enhancing robust network traffic segmentation via L2 controls, both for physical networks and in highly virtualized environments that rely on virtual network interfaces. These controls include VLAN access control lists (VACLs), private VLANs (PVLAN) and L2 firewalls. We’ll also look at the use of port profiles and security profiles that can be applied to virtual machines.

**Old Faithful: Layer 3 Filtering**

Before we delve into the new, let’s make sure that we are on the same page with regard to the common and omnipresent L3 network segmentation architecture. Traditionally, L3 networks have been carved up into myriad virtual LANs, with each VLAN representing a subnet. VLANs are created to break up broadcast domains, logically group devices and provide a point for implementing access controls between subnets. There are various methodologies and requirements that go into exactly which devices will be placed in a given VLAN, and placement relies strongly on organizational preferences, but common reasons include:

- To separate relative security levels, such as placing guests on one network and secure device management on its own separate subnet
- To separate devices by type, such as putting all servers into one or more VLANs
- To separate by physical location, such as floors or buildings
- To segment densely populated networks
- To ease monitoring or troubleshooting by putting certain systems on visually recognizable networks (for example, 10.222.222.x/24)

Once devices have been assigned to a VLAN, they can then be tied back together with L3...
routing devices, firewalls or other mechanisms to allow them to communicate with approved systems on other subnets. Some networks, such as DMZs are commonly created on physically isolated equipment that plugs directly into a firewall interface and is controlled by an appropriately tight perimeter control suite (for example, application firewalling, IPS, DLP, network AV) that directs the traffic flows. Guest networks can be a bit trickier, but these subnets will often use a mixture of access control lists, physical isolation and routing tricks to prevent an untrusted VLAN from interacting with corporate systems.

Another benefit of separating devices into various subnets/VLANs is that it provides network administrators with context clues as to the nature of the device(s) residing on that network. For example, if you know that a certain guest VLAN should never interact with any other corporate networks, it’s easy to create a rule that blocks all traffic from this one subnet to any other RFC 1918 private network.

Subnet context can also be valuable for inventory and monitoring. For instance, the operations team might know that all devices on a given VLAN, say VLAN 100, are router management interfaces, and that all devices on VLAN 110 are wireless corporate users. This information can help administrators with troubleshooting, network optimization and other common activities.

A further advantage of network segmenta-
tion, and one not to be overlooked, is that systems exposed to the Internet are physically isolated, and must pass through a firewall before they can interact with any sensitive systems or data. If a given system is compromised, then IT has a better chance of localizing the damage to a given subnet and catching the exposure more quickly through firewalls or other host- or network-based controls. Finally, network segmentation is a core tenet of defense in depth, and is used in conjunction with other defense mechanisms, including host-based controls, application filtering, traffic inspection and so on.

Moving to Layer 2

Moving to a flatter network architecture also moves us away from the L3 multi-VLAN segmentation model and into a different design strategy. VLANs will not go away, nor be fully removed from the multi-tiered hierarchy, but their use will be more limited as more diverse devices operate in the same subnet. For example, in a L3 model, you might put Web servers and database systems in two different subnets, and run the network traffic between those subnets through a firewall. In a flat L2 model, you might now put those hosts into a single subnet, but implement L2 controls so that only approved traffic flows through each system.

As with anything new, we must understand the pros and cons of this approach. I propose the following items as key security requirements in a flatter L2 design:

• Strong segmentation and filtering options between L2 entities
• Intuitive labeling and management of devices, because VLANs won’t necessarily provide context clues
• Consistent application of L2 access controls via usable tools
• Security controls designed for the unique requirements of virtual environments (for example, quick system builds and virtual machine migration)
• An ability to clearly show how traffic is being controlled to meet audit requirements

These concepts are essential to understand as we move into the next sections. First we’ll discuss L2 segmentation options that exist on our physical switches, routers, and firewalls and then look at options in the virtualized environment.

Three Controls

When we think about devices residing in the same L2 subnet we may often conceptualize these systems as having similar roles

<table>
<thead>
<tr>
<th>PRIVATE VLAN TYPE</th>
<th>CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous port</td>
<td>Device can communicate with other interface types on the PVLAN</td>
</tr>
<tr>
<td>Community port</td>
<td>Device can communicate with promiscuous ports and other community members on the PVLAN</td>
</tr>
<tr>
<td>Isolated port</td>
<td>Device can only communicate with promiscuous ports on the PVLAN</td>
</tr>
</tbody>
</table>

Source: Richard Dreger
(servers/workstations), access requirements (Internet accessible) and/or security levels (guest/trusted/DMZ). Typically, for systems and traffic residing on the same subnet and traversing non-virtualized network equipment, we have few options for providing segmentation and limiting how these intra-subnet devices communicate. Since we already discussed L3 segmentation and are interested in understanding our L2 control options, we will examine VLAN access control lists (VACL), private VLANs (PVLAN) and the deployment of appliances that support L2 firewalling. Note that multiple vendors (such as Cisco, Juniper, Palo Alto Networks) support some or all of these features on various products that they sell.

The first control in our toolkit is the VLAN access control list. VACLs are intended to be used in much the same way as traditional L3/L4 access control lists, with the added benefit that they are also applied at L2 on a physical switching/routing device. This means that a VACL can filter traffic bridged between devices on the same VLAN and does not just need to apply to routed traffic going into or out of a VLAN.

VACLs can be defined to block specific traffic types (udp, tcp, ports) and be applied directionally to and from various hosts. More specifically, VACLs can be tied to specific interfaces or be more generally applied to a whole VLAN, depending on your implementation and granularity needs. This means that we can enforce least-privilege concepts; for instance, allowing traffic from one Web server to talk with its requisite database system on specific...
ports, while blocking traffic going to a second, unrelated server on the same subnet. This is nice functionality to have. However, implementing VA CLs correctly requires a solid understanding of your hosts’ data flows based on your network communication requirements. If your VA CLs are not locked down properly or are overly limiting, improper device communication may occur, or devices may be prevented from communicating correctly.

Private VLANs, again implemented at the physical switch/router, can be used to group a system into one of three category types, each with its own traffic control properties: promiscuous port, community port and isolated port.

A promiscuous port PVLAN designation, typically used for the gateway of a given subnet, has unfettered access to other interfaces on the PVLAN. A community port PVLAN designation allows communication with other members of the community and promiscuous ports on the PVLAN, making this a good choice for a group of servers that need to talk on a given segment, such as a Web server and database server. The isolated port PVLAN applies the most draconian controls. This designation limits the device to only talking with promiscuous ports on the PVLAN (for example, the gateway type device) and prevents communication with other systems. Private VLANs provide broad segmentation of L2 traffic rather than granular control. Still, they are useful to support defense in depth and break up subnet broadcast domains, plus they work in tandem with VA CLs if more specific access profiles are needed.

L2 firewalling is similar to the functionality provided by VA CLs, but can further be wrapped up in a nice user interface. System like the Palo Alto Network (PAN) firewall (and others from competing vendors) support the ability to actually switch between two or more interfaces on the same VLAN and inspect traffic traversing this path. The upside to this L2 approach is that it leverages the abilities of an enterprise-class firewall and provides a clean way to integrate controls into a consistent firewall policy.

The downside is that it would be expensive to implement per-device L2 firewalling, due to port density requirements and the cost of each physical interface. True Layer 2 firewalling (not transparent-mode firewalling), while fairly uncommon, can make sense to implement as a filter between communicating devices on the same subnet that reside on different physical switches. Simply put, L2 firewalling is an option, but one that is uncommon at best due to its port usage and unusual blend of bridging and firewalling. The use of L3 or fully transparent (i.e., bump in the wire) implementation models are far more common.

Keep in mind that the addition of any L2 controls introduces another layer of filtering and potential breakage. If a host becomes inaccessible, we have to look at all the usual suspects, such as the firewall, host adapter, application processes or network. In addition, we have to determine if L2 filtering might be causing a problem.

This operational impact is essential to consider when you apply new controls. Make sure
that whatever you chose to implement has excellent management controls and audit capabilities to streamline configuration tasks and ease potential troubleshooting. Typically, this means using a management tool or element manager that can monitor filtering rules; provide centralized, actionable audit logs; and help enforce consistency throughout your implementation. These concepts of manageability and consistency are essential as we move away from the physical appliance and transition into our next topic of virtual L2 controls.

**Virtual Security**

As mentioned earlier, flat network architectures are well suited to environments like private clouds or highly virtualized data centers with migrating VMs. But you still need L2 networking controls in these environments, and that means working with virtual interfaces and virtual switches. Fortunately, when you understand VACLs, PVLANs and L2 firewall control options in the physical realm, these VM-centric controls will not appear radically different.

Network administrators need a system to enable granular, L2 segmentation for virtual systems with strong auditing, scalability and visibility into how traffic is being controlled. Ideally the system will allow us to expand the breadth of our L2 networks, which in turn would require less L3 routing instances and ultimately enhance performance. Strong, low-level segmentation options between systems are still required and become more important as the quantity of virtualized devices occupying a given subnet expand. Further, centralized and intuitive management becomes even more necessary as the complexity of the design increases.

For this discussion, we are using VMware ESX for virtualization, a Cisco Virtual Security Gateway (VSG), Cisco Nexus 1000v, and other back-end SAN storage, blade systems and supporting equipment with appropriate interconnects. Other product suites from competing vendors provide compelling functionality, such as VMware’s vShield product suite, but these tools do not fall within the scope of this article.

To begin, let’s define the different components that make up the environment. At the lowest level of our discussion is the virtual network interface card (vNIC). As the name indicates, this is the component that a virtual machine uses to communicate with the network. It appears to the operating system just like a physical NIC would on a non-virtualized server. This is the lowest common denominator that we will be dealing with. The vNIC will have a MAC and IP address.

The next component is the Nexus 1000v, which includes a Virtual Ethernet Module (VEM) as well as a Virtual Supervisor Module (VSM) that controls/manages the VEMs. The VEM is the networking software that integrates with ESX and replaces VMware’s integrated virtual switch technology. The VEM, just as you might expect for a virtual switch, can perform an array of functions, including L2 security options such as VACLs and PVLANs.

The last major component is the Virtual Security Gateway (VSG), which provide virtual firewalls features including security zones, and an ability to group systems based on attributes such as names or system functions.

All of these items work together to create...
tightly crafted network controls that filter traffic with varying degrees of granularity. They also allow for the easy addition of new systems into the subnet and automatic application of policy controls.

A key concept in implementing VM security is the port profile. A port profile is a collection of settings and configurations that dictate how members of the profile function. One key facet of port profiles is the security profile, which includes access control settings. Once port profiles have been created they are very easy to implement, an administrator only needs to assign the port profile to the appropriate vNIC, and then the settings are automatically applied. The configurations in a port profile stick with the VM even as it migrates to different physical hardware or changes state.

For groups creating new VMs regularly, these profiles can be applied at creation time. For example, a security profile might be created to lock down administrative GUI access only to a particular management subnet. Or a profile might explicitly deny network access from a less trusted group of systems to a more sensitive set of VMs. Group profiles simplify administrative tasks and help to enforce a consistent security baseline for similar systems. Beyond port profiles, the VSG lets administrators create multiple security zones that can be used for network segmentation. A security zone is simply a grouping of devices that share some common characteristic such as operational role, relative security value, access requirements or the like. These grouping will

**FAST FACT**

24%

Respondents who have purchased or are seriously considering unified stacks incorporating virtualized networking and storage.
provide simplicity and time savings later on when security rules are written that reference the zones as traffic sources and destinations. Application servers can be put in an app-zone, Web servers in a Web zone and so on. Systems can be put into zones based on network information, as well as VM names, OS guest name, ESX host and numerous other attributes. This means that if you have a standard naming convention, once you build a new virtual machine it will get mapped directly into the correct zone. This can be very helpful in ensuring that rules are consistently applied throughout a deployment.

Once the zones are created, rules are then written to control traffic to and from the zones. For example, we may wish to allow traffic from the Web zone to the database zone for 1433/tcp to facilitate SQL traffic, because we know that our Web servers need to query our DB systems. This rule is created as part of what ultimately becomes the security profile, which in turn will be mapped back to the port profile. Simply put, each vNIC gets a port profile that dictates, among other things, network security settings. These security settings then control ingress/egress traffic from the zone level down to interface-to-interface traffic flows. Thus the solution is essentially creating firewall profiles for each vNIC and allowing centrally managed filtering of network traffic traversing L2 neighbors.

**Four Reasons to Get Flat**

So really what does all of this discussion of filtering and L2 segmentation really mean, particularly for the virtual machine environment? What it shows is that many of the same concepts we’ve used for years (firewalls, VACLs, PVLAN) still apply to VMs. More importantly, it shows that these tools can simplify tasks in complex environments through the implementation of smart naming conventions, data flow definitions and profile creations. All of this can then be wrapped up with intuitive tools that help to facilitate organization and standardization—both of which help to promote security and smart risk management.

Flatter networks, particularly in virtualized environments, can reduce network complexity (fewer VLANs and simpler subnets), save cost and improve performance. But do we trust this model? It can be difficult to break down a security wall and move away from a traditional tiered, subnet-based segmentation model, regardless of how well constructed it may be. Here are four reasons why it’s worth considering taking this step.

1.) When protecting systems data flows, what we really care about from a network perspective is that we properly control traffic to and from our networked devices. However, the way in which we identify network entities is becoming more flexible. We can use host names, object names, IP addresses, Active Directory user information, group membership or other identifiers to build our access rules and view our audit logs. If we architect the solution correctly, we should care more about whether the communication flows between Host-A and Host-B are appropriate, and less about their IP addresses or relative subnets. Should we really care that a device is talking...
to our Web server on port 80 from the same subnet versus a different VLAN? Not if our access rules are correctly implemented, the source devices being permitted are acceptable, and we trust the software that is analyzing and applying our security policy.

2.) Implementing access controls at the vNIC/NIC level provides more comprehensive network flow control than simply filtering at L3 transition points. This is because L2 filtering in a virtualized environment captures all traffic entering or leaving a given interface, regardless where it is sourced. A L3 filter design wouldn’t capture traffic flows that originated from other devices on the same subnet.

3.) Operational ease, consistency and intuitiveness for security management are essential for long-term efficacy of our controls. Being able to automatically apply security policies based purely on a logical naming convention, for example, greatly increases the usability of the system and minimizes the possibility of errors. Overly segmenting networks or introducing myriad new VLANs adds complexity to the environment and reduces that intuitive mapping of device type to subnet that we discussed earlier. Note as well that routable VLANs do not by themselves enhance security unless there is some type of filtering between the subnets.

4.) The approach described in this report allows for VACLs, PVLANs and stateful firewalling between devices on the same subnet. While these controls are not quite as robust as a full-blown perimeter firewall, we must also consider the point at which “good enough” can suffice for a given security control. We all struggle with balancing performance versus security; if segmentation in our flatter architecture has acceptable risk levels using just stateful firewalling, then we have a compelling option that is worth consideration.

Keep in mind that even with L2/L3 filtering occurring within virtual systems, the need for sophisticated application-aware firewalls, IPS, DLP and all of the other perimeter controls still exists. The overall approach should still be a layered solution whereby we filter as much traffic at the lowest possible level before we work our way up to the dedicated firewall or application-layer filtering device. This technique helps conserve resources throughout the architecture, because a frame dropped at the initiating network interface has much less of an impact on the overall environment than one that must traverse multiple systems to be dropped by the firewall.

At the end of the day, there is no absolute best solution. What we know is that we are endeavoring to implement a control model of integrated, layered security controls that complement one another and help reinforce the overall security of the network. Breaking down network boundaries is not the right answer in all cases, particularly when the risks exceed the benefits, but it’s an intriguing option for virtualized architectures. Fortunately, with the crop of new tools, better management software and good security control options for physical and virtual deployments, we no longer need to be afraid of implementing and managing complex segmentation policies between devices communicating on the same Layer 2 subnets. It’s time to consider the benefits of getting flat.
Want More Like This?

*InformationWeek* creates more than 150 reports like this each year, and they’re all free to registered users. We’ll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you’ll find:

**Strategy: Networking in a Virtualized World:** We explore the technical issues exposed by virtualized infrastructure and looks at standards, technologies and best practices that can make your network ready to support virtualization.

**Research: IT Pro Ranking: LAN Equipment Vendors:** Cisco leads on the LAN, with an overall score of 77% based on product reliability, product performance and other key criteria, but HP, Dell and others are finding ways to compete.

**Fundamentals: Understanding Private Cloud Stacks:** For IT organizations willing to dispense with traditional application hosting models, a plethora of pure cloud software options beckons.

**PLUS:** Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.