Realtime
publishers

Security Management Tactics for the Network Administrator

The Essentials Series

Using Network Maps and Inventories for Security Compliance

Mike Danseglio

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Using Network Maps and Inventories for Security Compliance

Our modern workplace is dynamic. The workforce shrinks and grows as acquisitions are made and spun off, groups are merged and split, and employees are hired, laid off, renewed as contractors, and so on. Remaining dynamic and changing in response to market and industry demands are crucial to almost any business today.

This level of dynamic change leaves the IT staff in a difficult position. What's the best way to forecast the number of email servers for the next fiscal year if the company might double its staff or lay off 20% of employees? The flexibility of most modern industries is a boon for productivity and market response, and in a global economy, that is obviously crucial. But for the IT staff, not having enough information to plan can be disastrous.

Frequently, the IT department deploys hardware, such as desktop computers for new employees, on a very short timeline. IT is rarely considered when hiring employees. For example, at one large software development house, IT is not informed about new employees until their first day of work. All their assets—from building access credentials to smart cards to domain accounts to desktop and laptop computers—must be implemented and configured before they can be fully productive. None of that work starts until the employee shows up on their first day. And as many readers know, setting up a software development workstation environment is neither simple nor fast.

One unexpected ramification of this behavior is on the company's security and compliance position. Most companies today must adhere to various rules about how their IT assets are managed, how data is governed, and s on. But these just-in-time deployments often don't allow for full integration with the company's security and compliance processes. That's not to say that the computers aren't deployed without the proper virus scanner or hard disk encryption. At a higher level, most compliance processes require documentation of what assets exist, where they exist, and what they are authorized to do. This documentation is frequently skipped during rapid deployments, resulting in an incomplete asset inventory for the next audit to reveal.

This scenario is even more common with physical and virtual servers. At the same company, when an email server is near capacity, an automatic process creates a new virtual machine within a set of existing physical machines. This new virtual machine is configured with the proper operating system (OS) and email server software, then added to the resource pool for use. Is the virtual machine an auditable asset? Yes. Is it inventoried? Possibly. But in many organizations, virtual machine instances are not inventoried as they are removed, replaced, or reconfigured on the fly at any time. That results in an auditable asset that may or may not be known by the IT staff, residing on a physical asset that will certainly be audited through the regular process.

Is there a way to find out what computers exist, analyze them, and use this information for security and compliance purposes? There are dozens of ways, actually, providing solutions for virtually every reporting need, price point, OS, environment, and security posture. The more interesting question is: Can existing data be used to satisfy the same need with little to no additional investment? In some cases, the answer is a compelling yes. This article focuses on that answer.

Identifying Your Assets

Most administrators, and in fact most folks in the IT field, are familiar with an asset inventory. They are used for a variety of IT-centric and non-IT tasks. The uses for a generic asset inventory in many companies include budgeting, tax evaluation, company value evaluation, scanning for recyclable assets, and more. IT extends this list with uses such as identifying computers for replacement, forecasting power and cooling requirements, confining sensitive computers to appropriate boundaries, ensuring laptops haven't been stolen or misplaced, and so on.

Most companies perform some level of periodic inventory; compared with these generic processes, IT inventories have very special differences. IT inventories must enumerate multiple items that a common physical inventory doesn't account for:

- Multiple virtual machines running within one physical computer
- Software packages installed or running on each computer
- Portable computers including laptops and netbooks
- Internal configuration of each computer including memory, CPU, and so on

An IT staff can walk up to a 19-inch server rack, look up and down, and determine how many physical computers and other devices exist. But how many logical systems exist, and how well they're doing (for example, suspended indefinitely, running at 100% utilization, etc.) is not really visible from the front.

Take a look at Figure 1 if there's any doubt that appearances can be deceiving. This basic rackmount server can run dozens of virtual computers or none at all. Clearly an asset inventory needs to cover more than the physical unit but without breaking the bank and preferably with existing infrastructure. There are two great ways to achieve this: logical network maps and logical inventories.

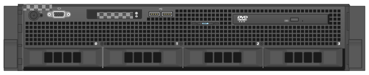

Figure 1: There's no telling what's happening in there.

Logical network maps are representations of the systems attached to the network. Most computer systems, and virtually all technologies, are network-attached, so logical maps are highly effective at finding all kinds of technology assets. Beyond physical computers, a network map shows the logical systems, how they connect, their relationship to other systems, and often what they're doing.

There are as many ways to create a logical network map as there are software and hardware solutions that will perform the task. Every solution has strengths and weaknesses, and they all pretty much get better as they mature. The most advanced network mapping technologies don't just look at network traffic—they grab enough data to perform an intelligent system analysis to determine more than just what's out there.

To elaborate further, consider the different levels of depth a network map can provide. At a basic level, nearly all tools identify the various computers and devices on the network. Going deeper, the more advanced tools use techniques to enhance the data and provide richer information. Some of these techniques, which vary based on software vendor, include:

- Identifying and classifying discovered hosts automatically using protocol analysis (for example, determining a packet that should only be created by a 3COM switch identifies that host)
- Classifying devices using MAC lookup
- Linking the TCP/IP and MAC addresses logically to facilitate asset identification
- Monitoring network traffic flow to distinguish different components, how they interact, and determine the relative bandwidth consumption of each, leading to richer business intelligence reporting and decision making
- Distinguishing between virtual and physical machines to provide more accurate and detailed analysis
- Performing granular analysis of each host to enable the indexing and lookup of detailed host information such as NetBIOS name, system vendor, and model number
- Configuration analysis of complex devices. For example, a basic network mapping tool will list a Cisco switch as existing, where an advanced tool will query the Cisco switch for VLAN data, routing tables, layer 2 forwarding information, and ARP cache tables.

Advanced network inventory and analysis tools can provide a rich set of data for reporting and tracking. Combined with a physical inventory, a logical network map built by an advanced tool is incredibly useful and gives a fairly complete picture of what's out there.

Note

More detailed network maps take longer to build but are always more useful than basic maps. Most advanced tools take days to thoroughly analyze and map a complex network. But the resulting product is worth the wait.

Similar to physical inventories, *logical inventories* are sets of data that represent systems. But going a step further, a logical inventory identifies all data of interest from a system. A logical network map or physical inventory will tell you, for example, that there's a 4U server in the rack running one host OS and three guest servers. But a logical inventory can reveal what's happening within each of those—what software is loaded or running, how it is performing, and so on.

Logical inventories are much more difficult to obtain due to their intrusive nature. Each system must be actively probed, prodded, queried, and questioned before a complete picture can be drawn. But there's a secret way to get this information that you probably already have access to.

Creating Maps and Inventories with Performance Data

You can use your performance monitoring infrastructure to easily obtain and analyze information about your network assets. It might sound a bit strange to use performance data to enumerate systems and determine their security and compliance state. So let me explain how this can work for you.

You may already have a network performance analysis infrastructure in place. Many organizations are concerned with performance analysis far earlier than inventory management or logical mapping. Thus, these systems tend to be in place frequently. Current performance analysis tools do a good job of determining what's happening within each system—physical, virtual, network-attached devices such as SAN and NAS, &c.

If you already have a performance monitoring solution in place that's reliably gathering data from the systems on your network, why should you implement a separate solution that might gather the exact same data? It's twice the maintenance, twice the overhead, and twice the complexity.

However, using performance monitoring data may not be the most efficient or effective manner to gather the data. Read the sidebar to understand a bit more about advanced discovery.

Advanced Network Discovery Technologies

Some technologies are simply better at performing a given task than others. Repurposing and getting more use of existing assets is great, as long as it is effective and reasonably efficient. But for truly enumerating the layout and components of an IT infrastructure, including virtually all networked devices, discovery and network mapping tools cannot be beat.

Most medium and large networks are a complex array of interconnected devices. Tools that enumerate them on different levels with different techniques are highly effective at determining what's on the network and how the pieces are connected. These tools often leverage standard network protocols such as SNMP, LLDP, ICMP, and ARP, which were in part designed to support network discovery. The most advanced tools combine these with multi-layer network analysis and secret analysis techniques that can build amazingly detailed and accurate network maps. If you use Microsoft Visio, many of the tools will even drop the data directly into a VSD (see Figure 2).

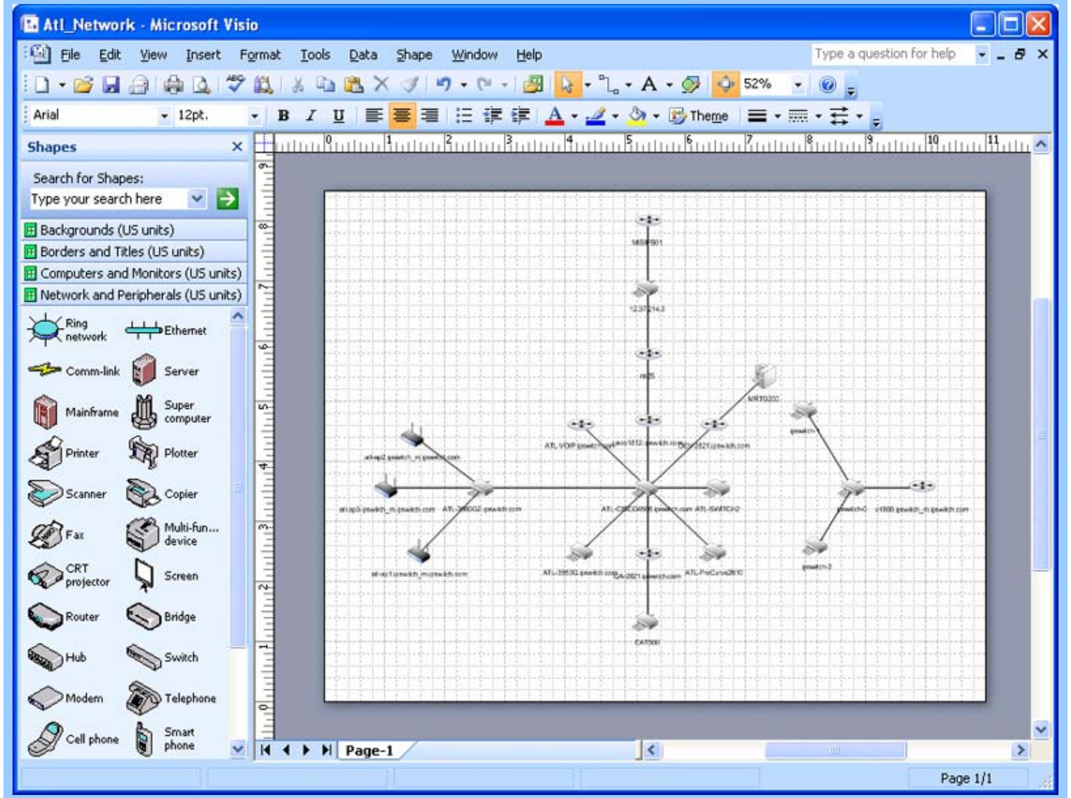

Figure 2: An effortless and accurate network map developed with automated tools.

Consider using a dedicated network discovery and mapping toolset if your network is at all complex or if you simply don't have the existing data to leverage. Continuing to manage a network without this level of detail is unnecessary and, likely, a waste of your time.

Repurposing the Performance Data

Now you know that, in all likelihood, your performance monitoring solution is already gathering (or can be told to gather) enough information to satisfy your security and compliance management requirements. You have two choices: use your current performance analysis tools to generate security reports or export the data to a dedicated security analysis and reporting tool.

Perception vs. Reality

Security and network administrators are often astounded by the fact that, for the most part, the data they gather to perform their tasks is very similar. Some security specialists may insist that only security-centric software is appropriate for gathering data used in audits and compliance work. Likewise, some network specialists will argue the fact that network performance tools have only one use: analyzing network performance.

These are very short-sighted views of the IT space. They are also uneconomical views. Each software implementation costs the company money in the form of software license and upkeep, personnel to manage it, time to use it, and so on. Although having multiple systems that do the same thing might be a great job security benefit, it simply doesn't fit into an efficient spending model. That money could be far better used elsewhere.

Your choice at this stage depends entirely on the tools at your disposal. Many IT departments use performance solutions that are flexible enough to create any report imaginable. So it is quite likely that, given a bit of time, you can create a compliance report within your performance analysis tools that satisfies security and compliance requirements. You should also check with your software vendor to find out if they have preconfigured reports of this nature available for download or purchase. Many such report templates exist and can very easily be customized to your needs.

Potentially, the most difficult task in using performance data for network and security management is taking the data gathered by the performance monitoring system and importing it into security and network mapping tools. There may be an easy way to do this depending on your specific tools and the data formats they support. Frequently, the task requires mapping data fields manually. The only nice part of this process is that it usually only has to be done once. Data exports and imports should be relatively painless after the initial discovery and research is complete.

Summary

Today's IT budget is tight. Determining how to meet growing demands for IT services and features while controlling spending is a challenge. Interestingly, many organizations have widely deployed tools that can be used for more than one purpose. Administrators and technologists often have the tools at their fingertips to deliver on demands while keeping budgets flat and minimizing their own efforts.

A great technology to leverage in this area is performance monitoring data. It can often be used to create logical network maps, inventories, security analysis, and compliance reports. With little additional work, you can probably take your existing performance monitoring solution and get much more value out of it by using it to meet a critical security need.