Network Misuse Revisited

Jim Metzler
Ashton, Metzler & Associates
jim@ashtonmetzler.com

Introduction

The May 2005 IT Impact Brief looked at the issue of network misuse. In that brief I defined network misuse as those instances in which a portion of the company's network is being consumed by supporting traffic that is unauthorized and inappropriate. The point that I made in that brief was that IT organizations should think of controlling network misuse as a bandwidth optimization technique similar to compression and caching. My reasoning for that statement was that if companies can control network misuse it typically frees up significant additional bandwidth that can be used to support legitimate traffic.

I am going to return to network misuse in this IT Impact Brief. In particular, I am going to use the results of a survey that we recently gave to the NetScout community to provide some insight into the extent of network misuse as well as how IT organizations are dealing with the issue.

In an upcoming brief I plan to discuss the topic of WAN vicious applications, which I consider a form of network abuse. WAN vicious applications are applications that run well over the LAN but run poorly over the WAN. While it may appear to be a bit of a stretch to say that WAN vicious applications constitute network misuse because in most cases they are authorized, it's also fair to say that they use the WAN in ways that are inappropriate.

Survey Results

In August we surveyed the NetScout community on a variety of topics, including network misuse. One of the questions that we asked the survey respondents was whether or not their company has a written policy regarding network use and misuse; i.e., using the corporate Internet for personal use such as reading email, gaming, downloading videos or music, etc. I was pleased to see that roughly 90% of the respondents indicated that their company had such a policy.

We also asked the survey respondents to identify the types of network misuse that they had found on their network. Their answers are contained in Figure 1.

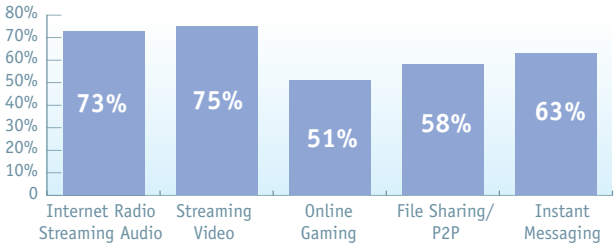

Figure 1 shows the types of network misuse seen by the survey's 223 respondents. For example, 51% of the respondents have seen unauthorized use of their network for gaming applications such as Doom or online poker.

In order to get insight in addition to statistics, we asked the survey respondents to identify the most unusual or outrageous network misuse discovered on their network. Below are some of the examples that they provided:

- A regional manager shared photos from the regional sales meeting with her immediate employees. Since most of the WAN was running at 128 Kbps and the attachments were 100 MB, this brought down the entire region for half a day.
- An employee was running a side business and using work resources to maintain and store daily transactions which he would then download to his home at night.
- Users were downloading content from a movie site in Vietnam. These users had also setup a Real Network Server to re-broadcast this streaming media to other users inside the network.
- Senior managers at a company were playing Doom during lunch.
- A contract IT worker had agreed to work full time for a given company. However, this worker was managing and working on projects for other customers using the network of the company for whom he was supposedly working full time.
- An employee at a branch office watched a 500K video stream on QVC all day long.

Since network misuse is widespread and can have a significant impact on network performance, we asked the survey respondents to indicate how they monitor for abuse. Just under forty percent of the survey respondents indicated that they do not actively monitor for network abuse.

Fifty-three percent of the survey respondents use a variety of somewhat informal techniques to monitor for network misuse. One example of this is having end users or managers report abuse. Another example is to identify misuse by exception; i.e., when troubleshooting a network problem. The respondents tended to use these techniques roughly equally at the headquarters and data center, as well as at remote sites.

In addition, over seventy percent of the survey respondents use multiple active measures to identify network misuse, including the use of content filtering (72%), network monitoring systems (64%), and firewalls or other security programs (81%). However, the use of these measures varies widely based on the type of site. For example, over three quarters of the survey respondents use these techniques in a data center and roughly two thirds of the survey respondents use these techniques in a headquarters site. However, under half of the survey respondents use these techniques in remote locations.

The fact that a relatively small percentage of IT organizations use active measures to identify network misuse at remote locations is somewhat disturbing in part because over the last few years the role of the branch office has changed dramatically. For example, up until a few years ago it was common to have the majority of a company's employees reside in a headquarters site and access applications locally. In addition, if an employee at a headquarters site wants to access the Internet, they typically do so over a high speed WAN link. Today most of the employees at the typical company do not reside in a headquarters site and they use the WAN to access a growing number of applications - both ones that are approved and appropriate and ones that are not. Given the number of employees that reside at remote locations and the ability of just one or two of these employees to congest a relatively low-speed WAN link by streaming internet radio, it is time for more IT organizations to actively monitor remote locations for network misuse.

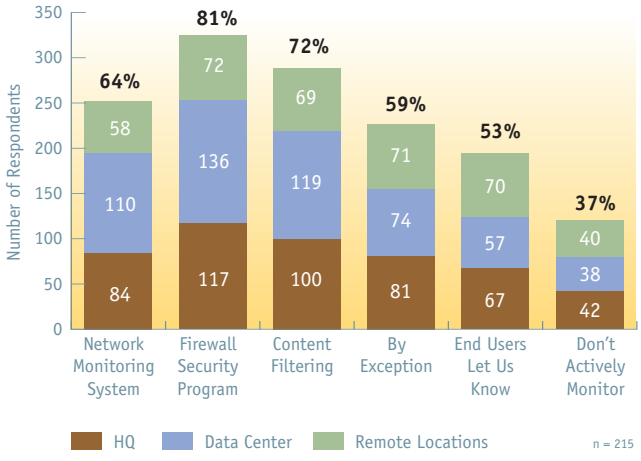

Figure 2 depicts the specific techniques that companies use to monitor for abuse as well as where they apply these techniques. To explain Figure 2, it is helpful to realize that 215 members of the NetScout community responded to the survey question that asked how they monitored for network abuse and that they could select multiple monitoring techniques and implement those techniques at multiple locations. For example, one hundred and seventy four (81%) of the survey respondents indicated that they use firewalls and security programs to monitor for network abuse in one or more components of the network - 117 in headquarters, 136 in data centers and 72 in remote locations.

Conclusion

Up until a few years ago, few networking professionals had any responsibility for application performance. Now, it is becoming increasingly common for the network organization to be held responsible for application performance.

Ensuring acceptable application performance is not easy. The first step is to understand what applications are running on the network. The second is to make sure that network misuse is minimized and that few if any WAN vicious applications are deployed, and the third and final step is to be able to do proactive alarming to identify, and hopefully resolve, issues prior to their impacting the users.