Global Information Assurance Certification Paper

Christian Boniforti
Version 1.4b Option B
March 2003

Securing a University's Bandwidth with PacketShaper

Introduction:

This paper is not limited to universities and could be applied to any network architecture. It is meant to bring attention to the importance of securing any network's bandwidth. This paper will assist the reader in the implementation, installation and configuration of the PacketShaper and the processes that are necessary to apply bandwidth utilization policies. It is important to remember that there is no "one size fits all" solution. I suggest using what is pertinent to your scenario and learn from my mistakes. I am not providing a guaranteed solution or an instructional paper; I am merely providing you with tools, strategies and the technology that I used in securing and providing reliable bandwidth to our institution.

One must also understand that this paper is written with an emphasis on a university network which differs greatly from traditional corporate enterprises. According to Ted Udelson, academic institutions are presented with special and complex challenges which are not faced by commercial or government entities. He further lists the most common threats:

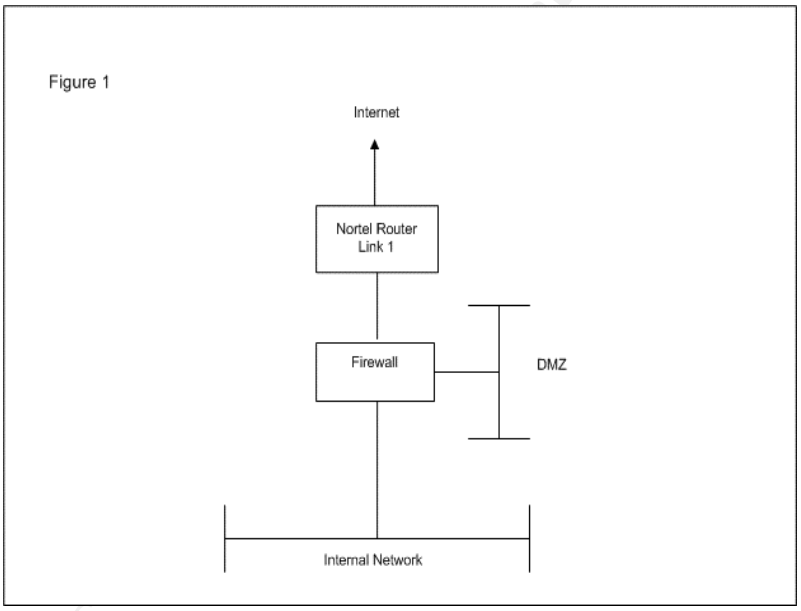
> They have difficulty in controlling end users.
>
> The culture cultivates free thinking and "open" access to information.
>
> The university serves as a research body, corporation, and Internet service provider. Colleges and universities must analyze each of these functions to determine the proper stance to take with regard to security (Udelson, p. 10).

These points brought up by Mr. Udelson, present a network administrator with many challenging and unique tasks. It is important to first, understand the threats that are specific to your network environment and then develop a solution that will fit best for your specific scenario.

Scenario: Before PacketShaper

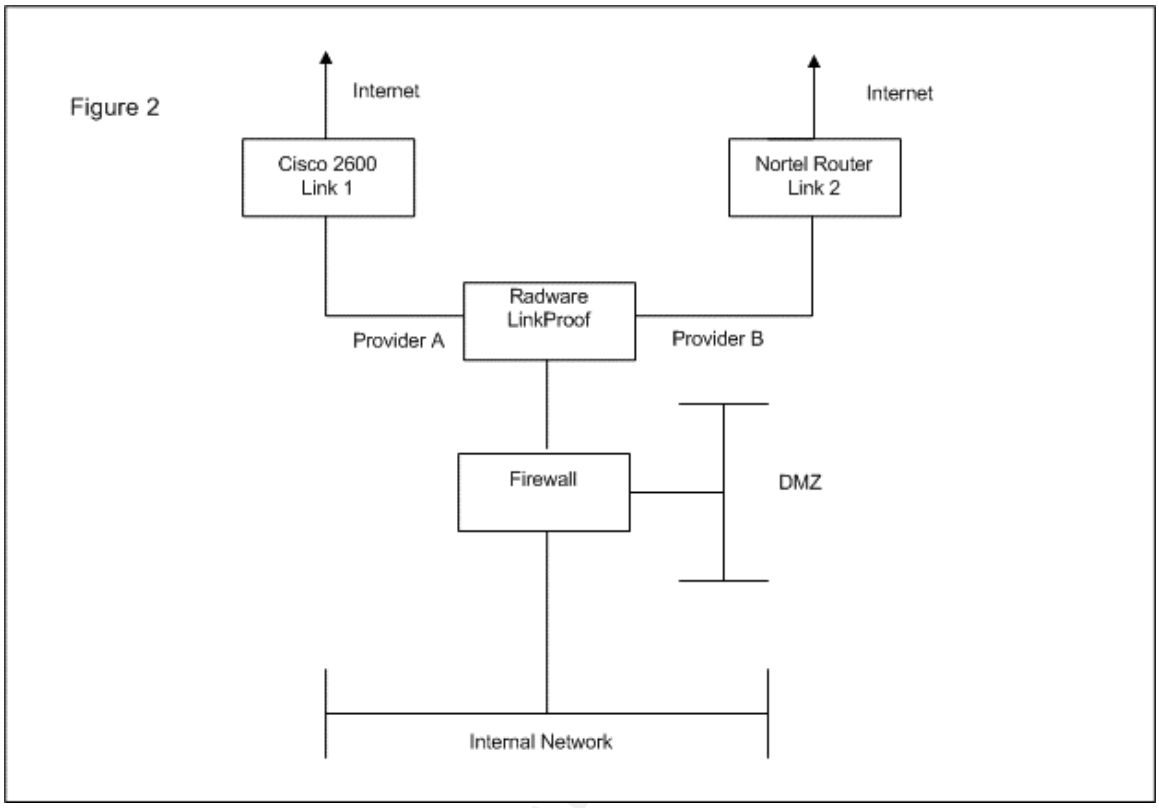
In late 2001, administration had received complaints from several students that the bandwidth that was provided to them was not adequate at times to conduct research. Specifically, students complained that at certain times of the day (a stretch between 10:00pm and 2:00am) internet access would come to a complete halt.

This was brought up to the CIO and the concern was later passed off to me. I conducted some research and monitoring using MRTG tool on our single T1. My report of the utilization of bandwidth showed that the T1 line idled between 80% and 90% utilization on working hours (9-5), and reached 100% during the 10:00pm – 2:00am stretch. **Figure 1** shows the basic public network setup.



My observation was passed along to my CIO and then onto administration. The problem needed to be resolved quickly and thus a very reactive decision was reached. Administration decided that the university should purchase an additional T1. This additional T1 was purchased in early 2002.

The university decided that it would purchase a device called Linkproof by Radware for the integration of both T1 lines. These T1 lines would be setup to provide load balancing, redundancy, and a larger bandwidth capacity. **Figure 2** shows the new design that was created for the integration of the dual T1.



The implementation of an additional T1 and the Radware Linkproof device were to provide the additional bandwidth needed and supply the university with some redundancy. The Linkproof device was able to eliminate

> . . . link congestions and bottlenecks from multi-homed networks, for fault tolerant connectivity and continuous availability of web services. By intelligently routing traffic and controlling bandwidth service levels across all Internet links, Linkproof enables effective link utilization, accelerating responsiveness, controlling bandwidth consumption and economically scaling operations. (LinkProof, p. 1)

The additional T1 and Radware Linkproof solution provided the university with larger amount of capacity and offered the university the needed tolerance, but it was not able to monitor internal usage.

Two weeks into the winter semester of 2002, the administration continued to receive complaints of slow internet access. Bandwidth monitoring was conducted once again and during the peak hours for the university (10:00pm to 2:00am) bandwidth readings would burst to the 100% capacity.

My first approach to this situation was to use portions of the “Defense in Depth” strategy and identify the business goals by the administration, faculty, students and the IT Department. Administration wanted a controllable, cost effective and quick solution. Faculty wanted guaranteed bandwidth and the Communications Department wanted designated bandwidth to conduct their streaming video

projects and presentations. Students wanted everything, from peer to peer networks to online gaming and Xbox live gaming. The IT Department wanted a better solution, one that would provide filtering, control and designate bandwidth on a policy based system. The IT Department also needed to be able to implement a VOIP (Voice Over IP) solution with adequate QoS (Quality of Service) in the near future.

It became apparent to the IT department that we could not continue to add T1's, and that we needed to come up with a solution that would be able to measure, monitor, filter and shape the bandwidth traffic. A solution also needed to be backed up by an "Issue-specific Policy". Currently the university had no specific internet utilization policy neither developed nor implemented.

A New Problem:
At around the same time we were beginning to experience constant problems with our firewall. At first we did not know or realize that this problem was part of our lack of bandwidth control and knowledge. The log files would grow at a rate that the OS could not handle. This would cause the firewall to either freeze and hang or the hardrive designated for the log files would fill up and consequently shut down the firewall.

After researching the log files it was determined that the culprit was SMTP traffic initiating from internal clients (specifically students). There were two different options to solve this problem. Allow SMTP to go through the firewall which would propagate SMTP traffic to the outside world, or stop SMTP traffic at the internal core router. Our core router also served as our VLAN manager. We setup an ACL (Access Control List) to not allow student traffic to send SMTP traffic. This solution seemed to work. We began to experience problems with the core router less than a week into the implementation phase. The core router began to crash every 24 hours. Once the router was reloaded some SMTP traffic was still being filtered, but not all. It was agreed that we were going to not filter at the router level, and try to find the culprit students? At this point, I was not able to identify this problem as a miss management of bandwidth.

We decided that we would try to answer the following key questions, **Why? What ? Where? and How?.** **Why** monitor and secure bandwidth? **What** were we going to use to measure and secure bandwidth? **Where** did we need to monitor bandwidth? And **How** would we enforce these solutions?

Understanding the Importance of Securing Bandwidth

Before we can understand **Why** we should secure and manage bandwidth we must define bandwidth. Scientifically speaking,

> …bandwidth is the width of the range of frequencies that an electronic signal occupies on a given transmission medium. Any

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.