Packetshaping at TAMU

William Reading

November 21, 2004

1 Introduction

1.1 About this document

There has been a fair amount of discussion on various message boards and chat rooms on what CIS actually does with traffic on resnet and how it affects the end users. When the users find themselves unable to do certain things, unfound assertions are generally stated about the network and some derrogatory comment is made. The purpose of this document is to discuss what is and is not in place on the network and possible remedies.

The views and comments in this document in no way represent *Texas A&M University* and are simply observations made by the author.

1.2 Packetshaping vs. Firewalls

Drawbridge[1], the in-house firewall package created by Texas A&M after a string of attacks by a number of crackers is the subject of a very interesting story[2] that will not be mentioned at all.

This is because most of the things that resnet users complain about is unrelated to the firewall. The firewall policy is relatively sane[3] with nearly everything being allowed out of the firewall untouched.

Nearly all incoming UDP traffic is allowed, with the exception of protocols that might cause hosts to leak information, such as `snmp`. Most incoming TCP traffic is disallowed for resnet hosts, with the notable exception for traffic on ports 113 and 80. This is traffic for the `ident` and `http` protocols respectively. `http` traffic is only allowed inbound after checking the host for common vulnerabilities.

1.3 Packetshaping vs. NetSquid

Another common problem that ResNet users sometimes run into is ports being occasionally disconnected due to strange traffic patterns. This is sometimes caused by the rules used in NetSquid[4] that match patterns of common viruses. This system, while interesting, is also not discussed in this document, but is notable to mention.

2 Packet Shaping

2.1 About the Packet Shapers

Three *Packeteer PacketShaper®6500* units are installed at Texas A&M, two of which are used for the purposes of shaping ResNet and one of which is used for shaping the Cisco VPN Concentrator. The latter one is probably installed in that location because a number of ResNet users discovered that it was possible to circumvent policy by passing unshaped IPSec traffic over the ResNet shapers. The choice of hardware was not a bad one (the devices being are able to pass 100mbit of traffic in real time), though the MSRP for one of these devices is approximately $14,000. The devices are also able to tell the types of traffic being passed, regardless of the port it travels upon.

[1] http://drawbridge.tamu.edu
[2] http://drawbridge.tamu.edu/tamu-security.pdf
[3] http://firewall.tamu.edu
[4] http://netsquid.tamu.edu

2.2 Configuration

Packetshaping is very minimally discussed on the TAMU Networking Group's web page[5], so a Texas Open Records request[6] was placed for this information in October 2004 to learn more details.[7].

As expected, the rules are sane and reasonable, resolving all but the most absurd conspiracy theories regarding packet shaping on campus.

The packetshaper is told that its inbound and outbound rates are 100mbit [8]

2.2.1 Inbound Min and Max

The Inbound partition[9] is currently set to 2 Gigabit, meaning that if the line is eventually upgraded to 2 Gigabit, then it will allow that amount of traffic. Of course, the PacketShaper®6500 is unable to do more than 100mbit, so the rule really just says to never shape regular Inbound traffic. At the time of the information request, the current traffic being passed inbound was 33.5mbit, with a peak at 99mbit.

2.2.2 P2P

The P2P section sets a minimum partition of 0.95mbit and a maximum partition of 4.75mbit. This essentially means that P2P traffic is guaranteed to at least get a full megabit for all of ResNet, but may not exceed 4.75mbit. The packet shaper can detect a wide variety of protocols[10], but only common P2P protocols are actually shaped on ResNet: Aimster, BitTorrent, Blubster, Direct Connect, eDonkey, Furthurnet, Gnutella, Hotline, KaZaA, Napster, PeerEnabler, SoulSeek, and Winny. At the time of the snapshot for the information request, P2P was occupying all of the 5.0mbit allocated for it.

There are a few things that are notably missing from this partition. For instance, NNTP (Newsgroups) consumed 6.7mbit inbound at peak, likely indicating binary transfers. NetBIOS over IP consumed a whopping 59.3mbit inbound at peak, perhaps indicating that the filesharing done via the ever popular `hobbes.resnet.tamu.edu` still has heavy usage or that accessing home directories, etc. is popular over SMB/CIFS.

2.2.3 Games

Although the packet shaper does notice and classify them as such, games do not currently have any traffic shaping policy and were in fact using about 184kbit, with a peak of 8.4mbit inbound when the snapshot for the information request was made.

3 Current Traffic

3.1 P2P

Peer to peer traffic flagged by the P2P rule unsurprisingly consumes all of its 5mbit partition nearly all the time. It would undoubtably grow to a much larger amount without a cap, though how much is uncertain. A handful of individuals on ResNet running BitTorrent with popular files could easily consume all 100mbit.

3.2 Other Protocols

Perhaps something more interesting is the traffic that passes through unshaped. Before the advent of large P2P networks, files were commonly traded via NNTP, IRC, FTP and sometimes HTTP. Unfortunately, all of these have substantial educational uses[11], which poses a problem for policy makers–Should everyone suffer because some people use a large amount of bandwidth via these protocols?

NNTP, for instance, occupies about 6.7mbit of incoming bandwidth at peak times. IRC does nearly the same, occupying 10.7mbit at peak. FTP occupies 25.7mbit at peak, but HTTP dwarfs that by oc-

[5] http://net.tamu.edu/network/policy/trafficeng.html

[6] http://reading.is-a-geek.com/packetshaping.pdf

[7] Admittedly, it may have been possible to ask CIS directly

[8] Well, approximately–it looks like it might be misconfigured to only 95.3mbit, resulting in a loss of about 5mbit for all traffic, not just P2P and Games.

[9] In Packeteer parlance, a "partition" refers to the amount of bandwidth a particular class or division of traffic is allowed to occupy in any particular time.

[10] http://www.packeteer.com/resources/prod-sol/ApplicationDiscovery.pdf

[11] Arguably, anyway.

cuping a huge 92mbit at peak. Of course, separating academic use from other, perhaps illegal use of the network is nontrivial.

It is hard to believe that these protocols were entirely not taken into account when constructing the rules, so the only reasonable conclusion to draw from this was that these have substantially non-infringing[12] uses compared to the other protocols.

Additionally, there are some protocols that do not appear in the configuration at all, such as Nullsoft's WASTE[13] or FreeNet[14].

4 Policy Circumvention

4.1 Introduction

Normally, the firewall policy helps ensure that the network is available for academic purposes. However, the question, "What if an academic resource is only available over one of the restricted protocols?" might arise. I was unable to find anything in the rules for students regarding the use of tunneling or disguising traffic to circumvent traffic shapers for the purposes of accessing academically related information, but that does not mean that such a rule does not exist or cannot be drafted. *I accept no responsibility for the improper use of this information, nor do I make any guarantees to its accuracy.*

The current policy is to not rate limit traffic not classified as P2P, so there are a number of ways to circumvent the packet shaping hardware.

4.1.1 SOCKS Tunnels via SSH

In this example, I would like to get a copy of Laurence Lessig's *Free Culture*, licensed under the Creative Commons[15] from the Legal Torrents[16] site. Unfortunately, the book is downloaded at too slow of a speed to be usable.

This poses a minimal problem using two free pieces of software: `OpenSSH` and `tsocks` installed onto a Linux 2.6 system. I configure `tsocks` to use the local host and port 1080, which is commonly reserved for SOCKS traffic. Now I do the following to get my file:

```
sudo ssh bill@off-campus-host.com -D 1080
wget http://www.legaltorrents.com \
    /bit/freeculture.zip.torrent
tsocks btdownloadcurses.bittornado \
    freeculture.zip.torrent
```

Using this method, I downloaded the book in about three seconds. Without a tunnel, the book took about ten or minutes. For small amounts of data, such as a 2 Megabyte book, this isn't a problem. However, for larger sets of data, it becomes infeasible to transfer files. It should be possible to use this method for on-campus hosts, but the majority of them have policies that restrict the use of using the machine for the purpose of connecting to other hosts.

Different organizations on campus have different opinions of this kind of thing. For instance, the Computer Science department has the following policy:

> **3.4.3** "Chained" sessions, where one connects to one system and then connects to another are not allowed. [Connection might be by telnet, rlogin, etc.] It is recognized that there will be times when brief connections like this are helpful, but users should minimize the time. Connect directly from your originating device whenever practical.

[12] sic
[13] http://sourceforge.net/projects/waste
[14] http://freenet.sourceforge.net
[15] http://www.creativecommons.org
[16] http://legaltorrents.com