



Part 1 of the Network Threat Landscape discussed the actual type and quantity of threats during a 5 day period. This report will focus on applications during the same period of time from Monday November 16 at 6 a.m. to Friday November 20 at 6 p.m.

Traditional firewalls are generally port based meaning they are aware of traffic using http (port 80) but are not aware of what applications use that port. Next generation firewalls are "**application aware**" and do not rely on port only technologies. In this study the PaloAlto firewall tells us exactly what applications are being used, what risks are associated with them, and how much valuable bandwidth those applications are consuming.

If school districts are aware of "**what applications**" are running on their networks and "**what threats**" are associated with those applications, they can create accurate acceptable use policies and make informed network security risk management decisions regarding what applications or services users are allowed to participate in.

In addition to noting the threats associated with each application, bandwidth consumption is also noted in the report. Bandwidth usage is certainly a valid concern for many school districts.

***This document will no doubt generate more questions than provide answers. It will however, provide the layperson a basic overview of how complex the threat landscape has become.***

### **1. Applications.**

Below are the top 20 applications the PaloAlto firewall identified during the 5 day period. The applications are sorted by bytes so that the top bandwidth consuming applications are first in the list.

Lets analyze the first entry. In lay terms the NewNet 66 school districts did over 57 million web-browsing sessions consuming just over 1.2 terabytes of bandwidth. There were just over 4.4 million threats associated with the application web-browsing which the firewall blocked. Threats are defined in two basic categories, Spyware and Exploits.

For clarity, NewNet 66 provides a very brief description of each application.

Application		Top 20 Applications			Applications	
	Risk	Application	Sessions	Bytes	Threats	
1	4	web-browsing	57,128,034	1,296,777,780,532	4,402,670	Regular Web Browsing
2	4	flash	3,746,349	872,292,874,562	214	Adobe Flash Player, streaming news etc.
3	4	ms-update	3,557,073	357,681,886,195	5	Adobe Flash Player, streaming news etc.
4	4	ssl	6,417,524	240,379,921,905	0	https secure traffic. Email, secure shopping.
5	4	rtmp	48,825	179,880,378,034	0	Adobe streaming audio and video.
6	5	http-audio	393,608	104,826,855,181	7	Streaming audio- Real Media, Internet Radio.
7	1	unknown-tcp	245,090	96,952,102,059	1	Traffic that is unidentified by PaloAlto.
8	4	rtmpt	252,802	94,352,024,674	0	Streaming media over port 80 (http).
9	4	adobe-update	23,414	93,474,435,676	9	Software updates for Adobe products.
10	3	apple-update	101,221	89,815,728,534	0	Software updates for Apple products.
11	5	http-video	34,285	68,017,737,571	0	Streaming video- Windows Media Player etc.
12	3	grooveshark	238,182	65,754,264,895	0	Web based music application.
13	5	smtp	2,820,472	61,181,509,574	247	Simple Mail Transfer Protocol- Email.
14	5	youtube	95,964	60,559,208,923	0	Free video sharing web site.
15	5	asf-streaming	10,386	58,240,178,732	0	Microsoft streaming media.
16	3	symantec-av-update	57,340	52,306,779,184	62	Symantec antivirus update.
17	4	itunes	86,730	33,851,204,220	1	Digital media application.
18	4	rtmpe	5,422	30,659,875,334	0	Adobe encrypted data streams.
19	5	rss	792,056	26,959,322,255	0	Blogs, news feeds, podcasts.
20	4	limelight	17,094	24,821,460,201	2	Hosted content delivery. Streaming media.

### What we can learn from application usage.

This year, 09-10, is the year of bandwidth consumption due to the quantity of new on line services being offered to K-12. No one has unlimited Internet bandwidth so school districts must be aware of exactly **"what"** applications are consuming valuable bandwidth. The Top 20 report above denotes that 11 of the 20 applications are in the streaming media category. This translates to bandwidth consumption at rates that leave many schools with fully saturated Internet connections resulting in very slow network access for school related business. Posting on line grades can certainly be affected.

## 2. Application Sub Categories.

Below are the top 20 application categories sorted by bandwidth consumption. Reviewing the categories presents some interesting thoughts. Are the applications are school related? Are they exposing the school district to unnecessary threats or are they consuming valuable bandwidth?

Application		Sub Categories			
	App Sub Category	App Category	Sessions	Bytes	Threats
1	internet-utility	general-internet	66,753,228	2,237,488,005,579	4,402,884
2	photo-video	media	1,137,758	634,023,907,185	2
3	software-update	business-systems	3,870,307	593,960,520,518	76
4	audio-streaming	media	917,394	246,065,445,101	8
5	encrypted-tunnel	networking	6,578,820	242,150,812,811	0
6	unknown	unknown	785,333	103,188,592,604	341,409
7	email	collaboration	3,620,705	92,433,402,898	281
8	file-sharing	general-internet	1,828,953	42,327,213,892	12
9	infrastructure	networking	40,497,498	12,744,118,245	2,832
10	social-networking	collaboration	440,916	11,510,721,516	1
11	remote-access	networking	17,756	4,696,866,621	0
12	instant-messaging	collaboration	452,562	3,592,025,296	0
13	general-business	business-systems	1,668,119	3,466,363,530	0
14	gaming	media	25,200	3,345,705,814	0
15	internet-conferencing	collaboration	681	1,926,226,984	0
16	internet-utility	collaboration	33,372	1,292,797,958	3
17	web-posting	collaboration	111,189	1,131,888,592	0
18	voip-video	collaboration	177,168	993,767,125	0
19	management	business-systems	180,764	794,886,878	0
20	database	business-systems	650,755	635,112,070	0
21	proxy	networking	24,986	544,300,065	0
22	office-programs	business-systems	8,345	421,936,171	0

# Summary

## Why this information is useful.

Providing a safe learning environment for students and staff is the number one priority for all K-12 school districts. This applies to both physical and virtual environments at school.

The physical environment has long been addressed using technology. Security camera systems are a good example.

The virtual environment is the challenge today. Content filtering, firewalls, and physical security of servers are all types of common security methods implemented today. However, with so many new services running on school networks it is almost impossible for schools to secure the data without re-thinking network security. It is important to remember that "everything" runs on the network. Grades, testing, financials, DVR security cameras, and many other services run on the network and many are being migrated to the Internet.

Understanding what applications are running on school networks is critical in providing security for students and staff. Understanding the threats associated with those applications is where the real effort must be implemented.

## How do we face these new challenges?

Budgets are shrinking, so addressing network security will be a tough challenge. Many school districts do nothing until a major security breach occurs and then react by mandating new policies or purchasing new technologies they should have purchased years ago. The key element is to be "proactive" with respect to network security.

Below are some of the basic best practices schools must implement in order to survive in the threat environment today.

1. **Educate your staff and students about Internet threats.** Every staff member must clearly understand how they can help with network security. Network security is a team effort.

2. **Know where everything lives by IP address.** If a network security event occurs, often times a workstation is the culprit. Knowing the IP address of the offending workstation is critical. If you know where it lives, you can address the event.

3. **Implement and manage traditional firewalls.** Implementing is easy, maintaining and managing firewalls is critical. Reviewing firewall logs is the most neglected practice.

4. **Implement "next generation firewalls"** that have the ability to identify threats by application. Then create policies that prevent use of applications that present the greatest risk. Monitoring Internet traffic is critical. What works one day may change the next so complacency is your worst enemy.

5. **Adjust AUPs** (acceptable use policies) to fit your school district based on application and enforce those policies.

At the end of the day, network security is all about Risk Management. Knowing what risks to manage is the key to success in providing a safe learning environment for your students and staff.