



The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

Fall Edition, 2008

Palo Alto Networks
232 East Java Dr.
Sunnyvale, CA 94089
Sales 866.207.0077
www.paloaltonetworks.com

Table of Contents

Executive Summary	3
Introduction.....	4
Why should we care?	4
Palo Alto Networks Application Visibility and Risk Report	5
Findings.....	5
Major Trends.....	6
HTTP is the Universal Application Protocol	7
Productivity applications delivered as a web service.....	8
Collaborative and business utility applications	8
Personal communications applications are as popular as ever.....	9
Applications That Facilitate Activity Concealment	10
Proxies and encrypted tunnel applications.....	10
Remote desktop control/access applications	11
Employees Keep Themselves Entertained	11
Video applications consume the bulk of the bandwidth	12
File sharing continues to be popular	13
Applications Are The Threat Vector to Worry About.....	14
The hidden iframe exploit is common.....	14
Threats that target media applications are increasing	14
Spyware and adware are universal	15
Summary	15
Appendix 1: Changes Between Application Usage and Risk Report Spring and Fall Editions (2008)	16
Appendix 2: Methodology.....	17
Appendix 3: Most Common Applications Found	18

Executive Summary

The Application Usage and Risk Report (Fall Edition, 2008) from Palo Alto Networks provides a view into enterprise application usage by summarizing application traffic assessments from 60 large organizations across financial services, manufacturing, healthcare, government, retail and education. The assessments were conducted between April 2008 and July 2008, representing the behavior of over 960,000 users consuming more than 63 terabytes of bandwidth. The report supports the notion that employee application usage within the enterprise is akin to the wild west where anything and everything is fair game.

HTTP has become the universal application protocol.

- Of the 424 applications found, 56% or 236 use HTTP in some way, shape or form, and together, those HTTP applications consume 64% of enterprise bandwidth.
- HTTP application bandwidth consumption broken down by underlying technology shows that web browsing and browser-based applications consume 46% of HTTP traffic and client server applications consume 54% of HTTP traffic.
- Browser-based applications aren't simple web browsing – applications like Apple-update, MS-Update, WebEx, and others download full-fledged clients on top of the browser. Existing IT policies and controls miss the significance of these applications.

Obvious attempts at activity concealment continue.

- As outlined in the first *Application Usage and Risk Report (Spring Edition, 2008)* employee use of proxies, encrypted tunnel, and remote desktop control applications continued and in fact, showed increased usage as a means of concealing activity.

Streaming video is consuming significant enterprise bandwidth.

- Streaming media (video/audio) applications, social networking and online games were found in 100% of the organizations and consume 10% of the aggregate bandwidth observed.
- In contrast to media applications, file sharing applications, both P2P (e.g. BitTorrent, eMule) and browser-based (e.g. MegaUpload, YouSendIt!) variants were found in nearly 100% of the organizations, but consumed less than 1% of the aggregate bandwidth observed. In other words, streaming media applications consumed 30x the bandwidth that file sharing applications consumed.
- P2P technology continues to make inroads as a delivery mechanism for streaming video, appearing in 43% of the organizations and contributing to increased media application usage.

Applications are the major uncontrolled threat vector.

- While nearly all organizations studied had application-level threats present, 86% of organizations had one threat in particular, a hidden iframe exploit, which is the entry point for all sorts of other threats including spyware, botnets, and other exploits.
- Media threats were found in 62% of the organizations. Threats that focused on Real, Flash, and iTunes were found, corresponding to extremely high media application usage.
- Every organization in the sample had adware and spyware, possibly due to the heavy penetration of iframe/drive-by download exploits, with the sample containing nearly 200 different types of adware and spyware.

At first glance, the applications found on enterprise networks were not that surprising. What was surprising was that, while IT had an idea of what was on the network, they were all surprised by the number of applications, both in terms of quantities and percentage of bandwidth. In each of the customer engagements, Palo Alto Networks' next-generation firewalls gathered data for up to a week, providing visibility into as many as 290 applications traversing the network.

Introduction

Perhaps the most significant finding in this report is that it reinforces the assertions made in the previous Application Usage and Risk Report, (Spring Edition, 2008) – employees use what ever applications they want. Some types of applications found, like audio and video media applications, were predictably discovered on every network. Other types, such as remote desktop access applications commonly used by IT and proxies, typically used at a corporate level, were being used by employees more frequently than expected, leading some organizations to investigate exactly who is using these applications and why.

Why should we care?

The question that arises is why enterprises care about, much less control the applications traversing the network? It would be hard to refute the statement that no one works 100% of the time they are at work. So if it is a historical given that some employee time is spent engaged in non-work activities, why start caring now?

Enterprises should be concerned now, more than ever before, because web-enabled employees have access to an unprecedented number of applications, both personal and business oriented, that can bypass traditional security infrastructures. Moving forward, the time spent using these applications will only increase, given the influx of new, web-savvy employees and the growth in applications that can bypass security. The result is that organizations are exposed to a wide range of business risks including:

- Data loss as a result of unauthorized or unmonitored file transfer through email, IM, P2P, online file storage/transfer, and more.
- Non-compliance with internal policies or external regulations as a result of employees using unapproved applications, such as the use of unrecorded IM in financial services companies, which can result in significant fines.
- Operational cost overruns driven by excessive bandwidth and IT manpower consumption that are the result of heavy and potentially non-work related media (video, audio) or file transfer application usage.
- A decrease in employee productivity caused by excessive personal application usage that may include email, IM, blog posting, online games as well as media applications.
- Business continuity placed at risk through application or network downtime, brought on by propagation of malware or application vulnerability exploits. Because the web provides an assortment of unmonitored applications and web sites, the risk of introducing a threat that places the business continuity at risk is significant.

The potential risks seem relatively obvious to the typical end user, thus raising the question: are they aware of the security and business risks they undertake each time they use the application? If yes, then what type of a mental check list do they go through to justify using applications like BitTorrent? Do they assume that corporate security controls can protect them from inadvertent threat propagation, possible data loss and possible compliance violations? If the answer is no, then what reasoning do they use when they launch their favorite media, email, IM or file sharing application? The answers may change depending on the user, but the reason behind the answers remains the same – simply put, because they want to and they know they can.

Organizations are aware that many of these applications are on their networks; some have even begun taking steps toward gaining a more accurate picture of their networks in hopes of becoming more informed in the event of a security incident. The usage patterns may be what they deem acceptable, and as long as blatant abuse is not occurring they allow the applications to be used. Accordingly, these companies might limit their application controls to only those they deem a critical risk—P2P and encrypted tunnel applications are possible examples.

On the other end of the extreme are companies who must care because they are in highly regulated markets, such as financial services and healthcare, where the risk of sizable per-incident fines dictate that they exert granular control over the applications that are used. For example, applications that can transfer files while evading detection (IM and webmail, P2P, etc) are not allowed or are strictly controlled on financial services company networks, yet they were both detected during this traffic assessment.

Palo Alto Networks Application Visibility and Risk Report

The Palo Alto Networks Application Visibility and Risk assessment involves deploying a Palo Alto Networks' next-generation firewall within the customer network, in either tap mode or virtual wire mode, where it monitors the application traffic traversing the Internet gateway.

Administrators are able to gain a more complete picture of their network traffic by combining the application identity with the category and subcategory it belongs in, its underlying technology and what the application's behavioral characteristics are. The behavioral characteristics provide data points about the application's file transfer capabilities, whether it has had any known vulnerabilities, its ability to evade network security detection, the propensity to consume bandwidth and its capacity to transmit/propagate malware. Using these data points, administrators can quickly determine what the application is and its potential risks, and then proceed to the next step in a more informed manner.

At the end of the data collection period, usually one to seven days, an *Application Visibility and Risk Report* (AVR Report) is generated that analyzes the application traffic by looking at the overall security risk rating, delving into the business risk assessment and providing a more accurate picture of how the network is being used. The report closes with a detailed look at how effective the existing technologies are at supporting and enforcing the customer application usage control policies. The data in this report is a summary of the 60 organizations that went through the AVR Report process.

It is important to point out that the identification of the applications traversing the network is to provide visibility first and foremost, as opposed to passing a value judgment on the application's business value or the security risk. Once identified, the security team, in conjunction with end user groups, can assess what the application is, how it is being used and how it should be controlled. Enabling the controlled and secure use of applications is an increasingly popular alternative to both wide open and tightly controlled networks.

Findings

None of the 60 organizations (representing the behavior of over 960,000 users, consuming more than 63 terabytes of bandwidth) that went through *The Application Visibility and Risk Report* process were overly surprised with what was found on their networks, but they were all concerned with the security and business risks that the applications represented. In a few cases, within the first 30 minutes of the traffic analysis, user names were submitted and actions were taken to address inappropriate application usage. The majority of the organizations were elated to finally have a tool to identify and, if desired, control the applications on the network.

The findings in *The Application Usage and Risk Report, (Fall Edition, 2008)* focus on three different areas: HTTP is the avenue of choice for all manner of applications; media as opposed to P2P is a significant consumer of corporate bandwidth; and the uncontrolled use of applications remains a significant threat vector.

Major Trends

As outlined in *The Application Usage and Risk Report, (Spring Edition, 2008)*, enterprise policies for appropriate application usage are inconsistent. Policies may exist, but they are unenforced or merely given lip service. More often than not, the answer to the question of application usage policy is “what policy?” While every customer engagement varied in terms of the scope of their application usage, there were several common themes.

- **HTTP is the universal application protocol.** Of the 424 applications found, 56% use HTTP in some way, shape or form, either as its underlying protocol or as a means of tunneling another application. Interestingly, the applications that use HTTP are consuming 64% of the total bandwidth observed. On one end of the spectrum are obvious business applications such as Microsoft SharePoint and Microsoft-Update, and on the other end were those that are being used for personal communications (IM, webmail and VoIP).
- **Obvious attempts at activity concealment continue.** Following along the lines of how HTTP is commonly used to bypass the firewall, employee use of proxies, encrypted tunnel, and remote desktop control applications showed increased usage as a means of concealing activity.
- **Employees are staying entertained at work.** The data collected for this study provides a glimpse of how employees stay entertained at work. While the finding may not be new, what is new is the number of different applications employees are using to entertain themselves and the amount of bandwidth being consumed. Media applications as a whole consumed 10% of the 63 terabytes observed during the study period. For comparison sake, the combination of both P2P file sharing and online storage/sharing applications only consumed 0.34% of the overall bandwidth. Put another way, media applications consumed more than 30 times as much bandwidth as file sharing.
- **Applications continue to be the major uncontrolled threat vector.** Some might say that this is not new information, but there is a definite correlation between the amount of non-work related application usage and the high incidence of threats, like the hidden iframe drive-by vulnerability as well as the high incidence of streaming media applications and related threats.

Enterprises are rapidly becoming more aware that they have to address their growing application visibility and control problems. In every customer engagement, the security team had an inkling of what was happening on their network, it was merely a matter of seeing exactly how bad it actually was.

In some cases, the findings mapped closely to what IT felt was happening, with respect to application usage. In many cases, however, IT was surprised to see that it was worse than they had expected. In some cases, 33% of the top 100 applications found on the network, ranked in terms of bandwidth, were considered to be non-work related (music, video, webmail, IM, social networking, P2P, gaming, etc).

HTTP is the Universal Application Protocol

At the risk of stating the obvious, HTTP presents application developers with an open avenue into corporate networks because firewalls tend to treat it as web browsing. Less obvious, is exactly how widespread the use of HTTP is for all types and manners of applications. HTTP applications run the gamut of purely work-related to obvious entertainment and purposeful evasion. Of the 424 applications found, 236 or 56% used HTTP either as its underlying protocol or as a means of tunneling another application, yet the HTTP applications found were consuming 64% of the all bandwidth observed.

Another interesting data point that supports the “HTTP is the universal transport” statement is the fact that not all HTTP applications are browser-based. Interestingly, only 141 of the 236 HTTP applications are browser-based, and they consumed only 46% of the bandwidth while the 64 client-server applications consumed 54% of the bandwidth.

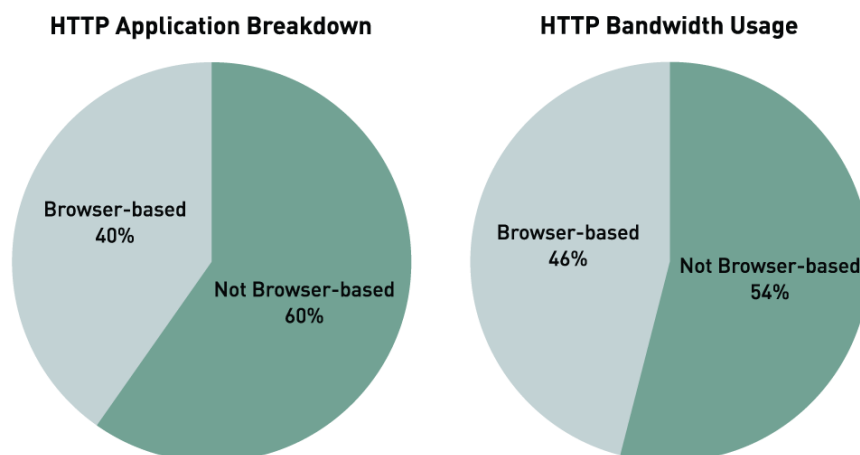


Figure 1: A comparison of the number of HTTP applications by technology and the percentage of bandwidth being consumed.

Some examples of applications that were observed include Microsoft SharePoint, Tivoli-Storage Manager, Siebel and Lotus Notes, all of which use HTTP in one way or another but are client-server based, which provides some explanation of the differences in bandwidth consumption. Even Yahoo!IM and WebEx, application that clearly uses HTTP yet still download a client, making them client-server applications, as opposed to a browser-based application.

Probing more deeply into the category breakdown of HTTP applications shows that they fall into three distinct areas: productivity applications, collaborative/business utility applications and personal communications.

Productivity applications delivered as a web service

In some ways, the findings in this section support the efforts by Google and others to gain a foothold in the “office productivity application as a service market.” These applications are accessible via the web and all of them can provide business value. The challenge then becomes determining if the applications belong on the network and how best to enable their safe usage.

Office productivity applications, delivered as a web-enabled service, were found frequently across all organizations. Google Calendar and Google Docs were most commonly detected at 95% and 88% of the organizations, while the suite of Zoho applications were found in a range of organizations. In terms of underlying technology, they are all considered browser-based, but make no mistake, these applications are robust, full-fledged office applications and employees are using them with or without IT approval. The challenge with these applications is that they fall outside the realm of IT support, but they will only increase in usage and popularity. For comparison sake, this class of application was found only 60% of the time in *The Application Usage and Risk Report*, (Spring Edition, 2008).

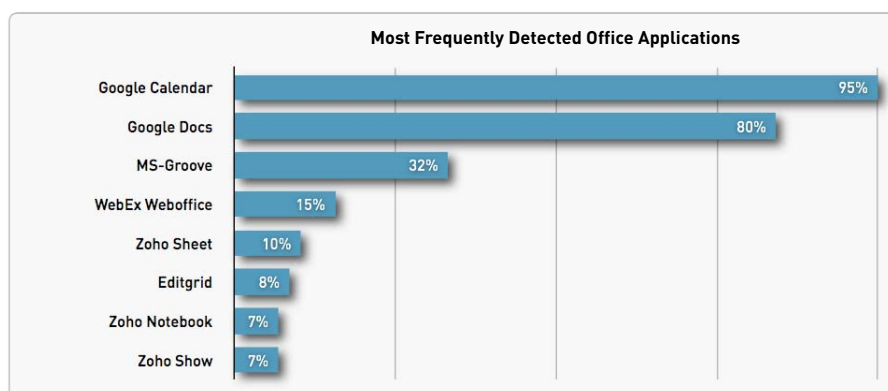


Figure 2: Breakdown of most common office productivity applications found across all 60 organizations.

Collaborative and business utility applications

Like the office productivity applications, a range of utility, business or conferencing applications that use HTTP were found in a majority of the organizations. Most of the applications in this group would be considered to be corporate IT sponsored and supported. Examples of applications found include Netspoke, GoToMeeting and Live Meeting, all of which are conferencing applications. Google Desktop and RSS, applications that straddle the line between business and personal use were detected 83% and 95% of the time respectively.

Many of the utility and collaborative applications discovered will use the browser as the presentation vehicle, but under the covers they are client/server applications. In some ways, this group of applications exemplifies the fact that HTTP does not necessarily mean browser-based. Of the 34 applications found, 18 were client/server and 16 were browser-based, yet all of them used HTTP in some shape or form.

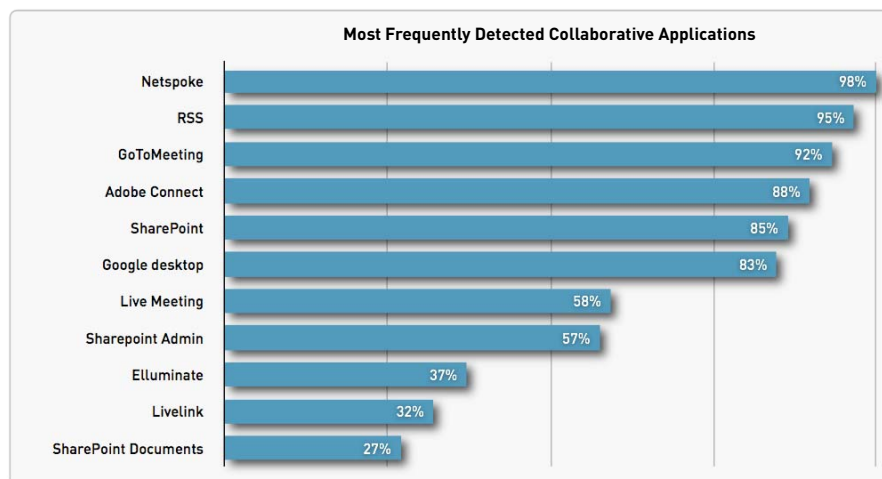


Figure 3: Breakdown of most common collaborative and utility applications found across all 60 organizations.

Personal communications applications are as popular as ever

The findings showed that instant messaging and webmail applications remain two of the more commonly detected applications and it is no surprise that both types of applications utilize HTTP as a means to simplify access and coincidentally, bypass most firewalls. Specifically, 30 different instant messaging applications appeared across 97% of the organizations with Yahoo! Webmessenger, AIM Express, MSN and AIM appearing most frequently.

On the email/webmail front, 24 different email applications (Outlook Web Access and Lotus Notes excluded) appeared 100% of the time with Hotmail, Yahoo! Mail, Gmail and AOL Mail being the most popular.

The most significant change in the personal communications area is the frequency that VoIP applications are being used. Showing a sizable increase, VoIP appeared in 97% of the organizations compared to 75% in the previous *Application Usage and Risk Report*. The most popular VoIP applications were Yahoo! Voice and MSN Voice appearing most commonly at 67% and 62% respectively. While it falls outside of the HTTP categorization, Skype was also detected quite frequently at 73%.

Who cares if employees use these applications to keep in touch? On one hand, keeping in touch with family, friends and even co-workers might result in higher employee morale, bringing productivity improvements. On the other hand, these applications are known to evade traditional security technologies and as such can expose the organization to possible compliance, business continuity, data loss and productivity related business risks that may affect the bottom line.

Applications That Facilitate Activity Concealment

In some ways, the use of HTTP can be seen as a positive in that it facilitates deployment and simplifies access. It can also be viewed as a negative in that it makes inspection by traditional security infrastructures more difficult, if not impossible. Then there are those applications that are primarily designed to conceal user activity. Proxies and encrypted tunnel applications are the first two types of applications that come to mind, but they are now joined by remote desktop access applications. To be clear, the fact that proxies/encrypted tunnel applications were detected at 97% does not mean activity concealment was the primary goal, but make no mistake, TOR (The Onion Router) and UltraSurf's sole purpose is to conceal activity through the use of encryption and they are aggressively marketed as such. In most organizations, the use of either of these applications has only one purpose – conceal activity. Other applications, such as SSH, MS-RDP and LogMeIn! could be part of the IT department's toolkit for supporting end users, but there were cases where the intrepid employee chose to use one of these applications to access their home machine from work for personal use.

Proxies and encrypted tunnel applications

Excluding HTTP proxy, which may be a corporate-supported infrastructure component, 17 different proxy applications were found across 80% of the organizations. Including HTTP proxy bumps the usage to 97% of the organizations. A realistic number is somewhere in between 80% and 97%. The most startling fact, outside of the overall frequency is the sheer number of different proxies found in some of the organizations—there were several organizations where as many as eight different non-IT supported proxies were found.

The most common examples outside of the traditional, corporate endorsed HTTP proxy were CGIproxy and PHPProxy which were found in 65% and 55% of the organizations, and it is a safe assertion that these applications are being used to conceal some type of user activity or bypass existing URL filtering policies. In comparison, in *The Application Usage and Risk Report, (Spring Edition, 2008)*, proxies of all types (HTTP proxy included) were detected in 80% of the organizations. Looking at encrypted tunnel applications, SSH was found 85% of the time, which is not a surprise, given its popularity and usefulness as an IT tool. What the survey does not indicate is whether or not some of the SSH usage is a computer savvy (non-IT) employee who is accessing their home PC at work, which was found in several of the organizations.

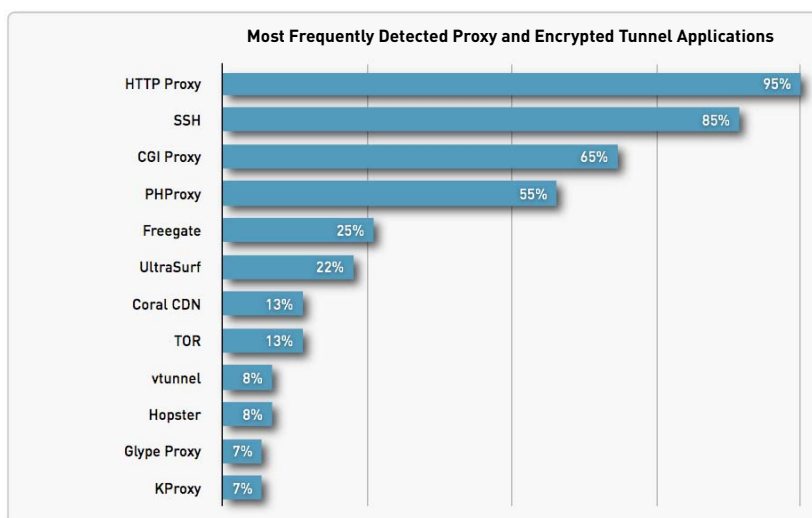


Figure 4: Most commonly detected proxies and encrypted tunnel applications across all 60 organizations.

Remote desktop control/access applications

As originally designed, these applications allowed support personnel to remotely control an end-user machine for the purposes of fixing a problem and they are still invaluable for that purpose. But the number of non-IT supported remote control applications found, indicates employees are using them for potentially non-work related purposes. Eliminating applications such as L2TP, PPTP, and X11, a total of 18 different remote desktop control applications were found across 93% of the organizations. Most commonly found was MS-RDP at 82% with telnet and LogMeIn! at 72% and 60% respectively. In the previous edition of the *Application Usage and Risk Report*, remote control applications were detected in only 75% of the organizations. Why would a non-IT employee need an application like LogMeIn!? The answers may be that they are accessing another PC, perhaps their home machine, possibly troubleshooting a family member's PC or moonlighting at a second job. Whatever the reason, the use of these applications by non-IT staff will fall outside of most organizations' appropriate usage policies. SSH, and remote desktop access applications are excellent examples of applications that provide distinct, measurable business value, and that should be deployed in a secure and controlled manner.

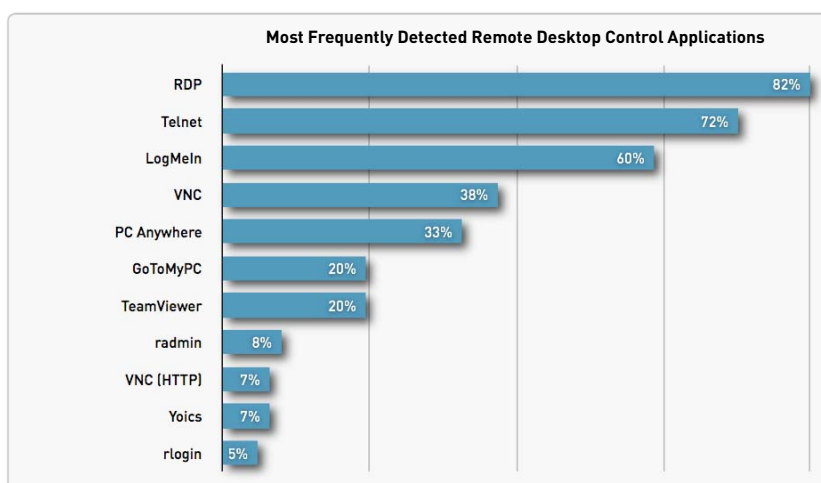


Figure 5: Breakdown of most common remote desktop control applications found across all 60 organizations.

Employees Keep Themselves Entertained

It is no surprise that some types of entertainment applications such as video, audio, games and social networking were found on every network inspected. Flash is a common tool for marketing and education, as is HTTP video and audio. What is surprising is that there were 61 different applications (8 audio, 10 gaming, 12 social networking and 31 photo/video) that were identified. Removing the fringe entertainment applications such as social networking lowers the number only slightly to 49. In some of the organizations, as many as 51 entertainment applications were detected.

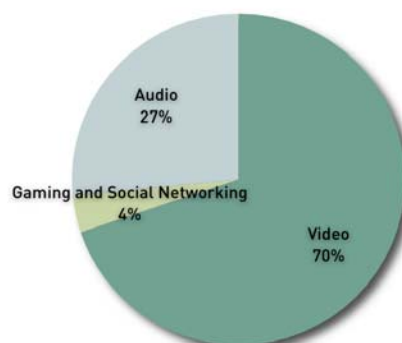


Figure 6: Breakdown of bandwidth consumed by entertainment applications.

The astonishing fact is that entertainment applications consumed 10% of the overall enterprise bandwidth. By comparison, notoriously bandwidth-hungry file sharing applications, inclusive of both those that are P2P-based and the increasingly popular browser-based (MegaUpload, YouSendit, etc), consumed only 0.34% of the overall bandwidth. To put it another way, media applications chewed through 30 times as much bandwidth as the file sharing applications consumed.

Video applications consume the bulk of the bandwidth

Delving deeper into the types of entertainment applications that were found, the 31 video applications were the most voracious consumers of bandwidth at 70% of the overall entertainment bandwidth observed. When looking at the underlying technology for the various video applications, the data shows that the use of P2P for commercial delivery of video is increasing. In 43% of the organizations, video applications that use P2P were found. In total, eight different P2P-based streaming media applications were detected, and as many as six of them were detected in several organizations. By comparison, P2P-based media applications were found in only 25% of the organizations summarized in the previous *Application Usage and Risk Report*, but it was noted as an area of growth.

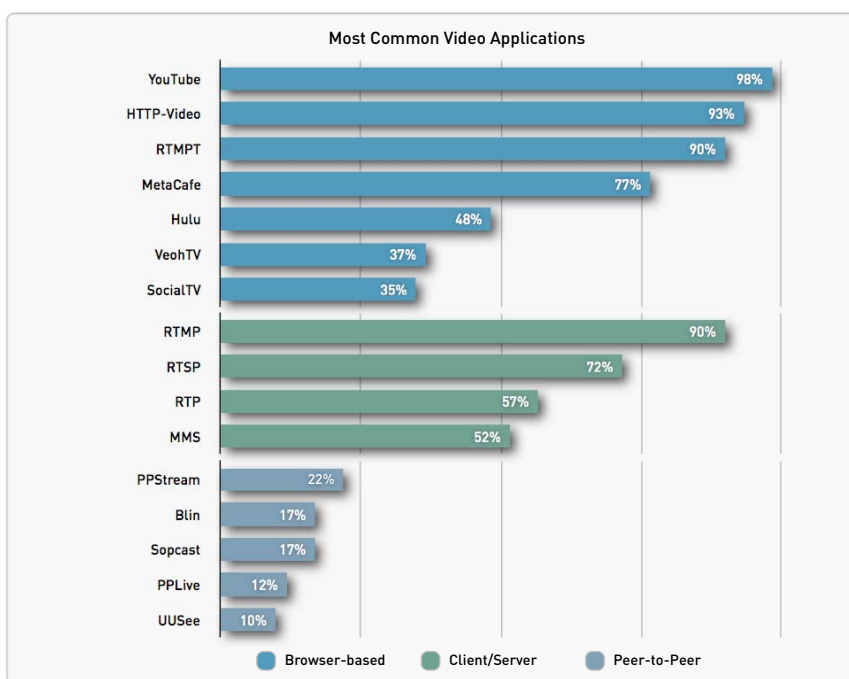


Figure 7: A comparison of client/server, browser-based and peer-to-peer video applications.

P2P, Looking at the 12 browser-based video applications, the most popular application was YouTube, appearing 98% of the time, with HTTP-video and RTMPT (HTTP encapsulated Flash) at 93% and 92% respectively. There were 11 client-server video applications also detected, of which RTMP (Flash) and RTSP (RealMedia, QuickTime) were the most popular at 90% and 72% respectively.

File sharing continues to be popular

While the bandwidth being consumed by file sharing applications was relatively small, the frequency that they were found warrants discussion from two perspectives. First off, P2P use remains high with 17 different variants found in 82% of the organizations. The astounding data point was that multiple P2P variants were found in almost every organization with 13 being the highest number of P2P variants detected. Put another way, the average number of P2P variants found in each account was five, leading one to safely believe that employees are ignoring the risks, along with any existing policies. These users must believe that they have configured the P2P application so that their whole hard drive is not shared, a task that has been shown to be far more difficult than it should be for the average user. The second interesting observation is that 18 different browser-based file sharing/transfer applications were found across 68% of the organizations – more than a 100% increase from the 30% outlined in the previous report. On average, four different browser-based file sharing variants were found in each account with the most popular being YouSendIt! and MegaUpload, both appearing in 48% of the organizations.

One common use for browser-based file sharing/transfer applications is as a means of centralized storage. Rather than lug a PC around, a user can store files in the cloud, accessing them from a kiosk, an internet terminal or even a smart phone. Other common uses are to bypass SMTP file size rules or to post a link to large files on personal pages in social networking sites. This works by posting a video to a storage site, then the URL is posted to the personal page, enabling visitors to view the file without violating space requirements. The challenge IT faces with these applications is that they represent a black hole through which data can be transferred while simultaneously providing a threat vector because of the common use of advertising (a known delivery mechanism for adware and spyware) as part of the supplier's business model. The result is an introduction of threats into the network, placing the business continuity at risk while increasing the operational costs required to address the threat propagation.

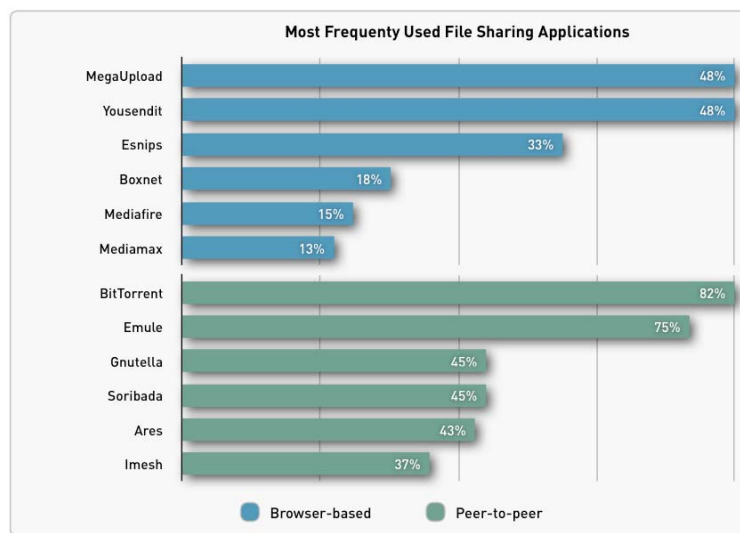


Figure 8: A comparison of the most commonly detected P2P and browser-based file sharing applications.

Applications Are The Threat Vector to Worry About

While many in the information security profession have postulated that application-level attacks and threats are the biggest concern for IT risk management staff, rarely has there been proof. On this topic, most discussions have revolved around the fact that our defenses are tuned to focus on infrastructure-level threats, and only recently have they started to focus on the fact that there are large numbers of actual application-level threat and incidents. Recently, SANS published a version of their Top 20 Threats, where 16 of the top 20 threats SANS says information security professionals should be concerned about were application-level threats. It makes sense: from a high level, information security professionals have done a pretty good job of securing the infrastructure both in how they manage it, and in forcing infrastructure vendors to build more secure products. Threat developers, however, move to easier targets – applications and their users.

Starting with this iteration of the *Application Usage and Risk Report*, Palo Alto Networks will look at threats traversing the networks of the organizations observed. During this edition of the study, Palo Alto Networks was able to confirm that the 60 organizations sustained a significant amount of application-level threat activity. The usual variety of exploits, viruses, and worms were detected along with a large number of application-level threats. The applications targeted included office applications (e.g. MS Word, Excel, PowerPoint, Adobe Acrobat, Outlook), Internet applications (e.g. IM, browsers, widgets) and utility applications (e.g. systems management, remote access, application servers). Here are a few key highlights worth noting in a long list of application-level threats.

The hidden iframe exploit is common

The first interesting component is the high incidence of hidden iframe exploits, which parallels the use of HTTP applications, detected in over 85% of the organizations, many of which were in large quantities. The scary piece of the hidden iframe exploit is that it's used for surreptitious drive-by downloads and installations of additional web-borne applications. Note that an iframe is a normal component of web applications so to most security devices they may appear as normal application traffic. Usually these applications are attacks, bots, spyware or adware.

Threats that target media applications are increasing

The second interesting component parallels the ubiquity of streaming media applications in the sample: threats targeting media applications are plentiful and were found in 62% of the sample. Threats targeting RealPlayer and Flash were most common, but other common media application threats targeted Windows Media Player, VLC, QuickTime and iTunes. Other media application level threats included playlist-encoded threats and threats targeting VLC (a multi-format media player).

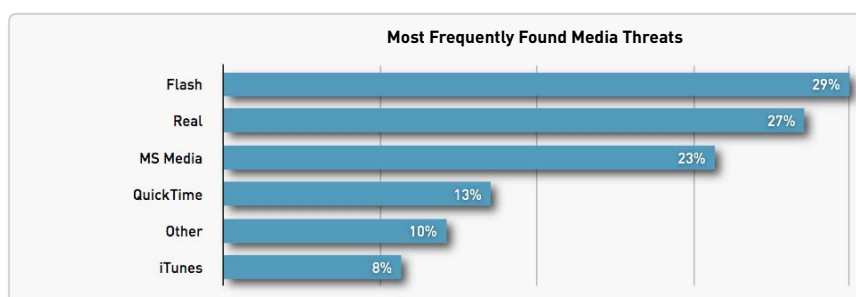


Figure 9: Most commonly detected streaming media threats.

Spyware and adware are universal

The third threat trend uncovered during this study was not a surprise, especially given the prevalence of the hidden iframe/drive-by download exploit. Spyware and adware are everywhere – there were significant numbers of the initial download and install and the “phone home” traffic. There were 194 different types of adware and spyware uncovered, ranging from keyloggers, to screen-scrappers, to redirectors and “toolbars.” Needless to say, 100% of the 60 account organizations had spyware or adware. Categorically, spyware and adware are interesting because they are threats. However, they’re also often full-blown applications in their own right, meaning that the importance of managing applications on enterprise networks has come full circle.

Summary

The findings in this report prove that the existence of end-user oriented applications on enterprise networks is a fact that most IT organizations have come to accept. The challenge then becomes determining the levels of application control necessary to mitigate the propagation of threats while balancing the end user requirements and business needs of the company.

The Palo Alto Networks Application Visibility and Risk Assessment process provides organizations with a view into the identity of the applications traversing the network, along with who is using them. This granular level of visibility is in turn helping companies regain control over their application usage and related threats.

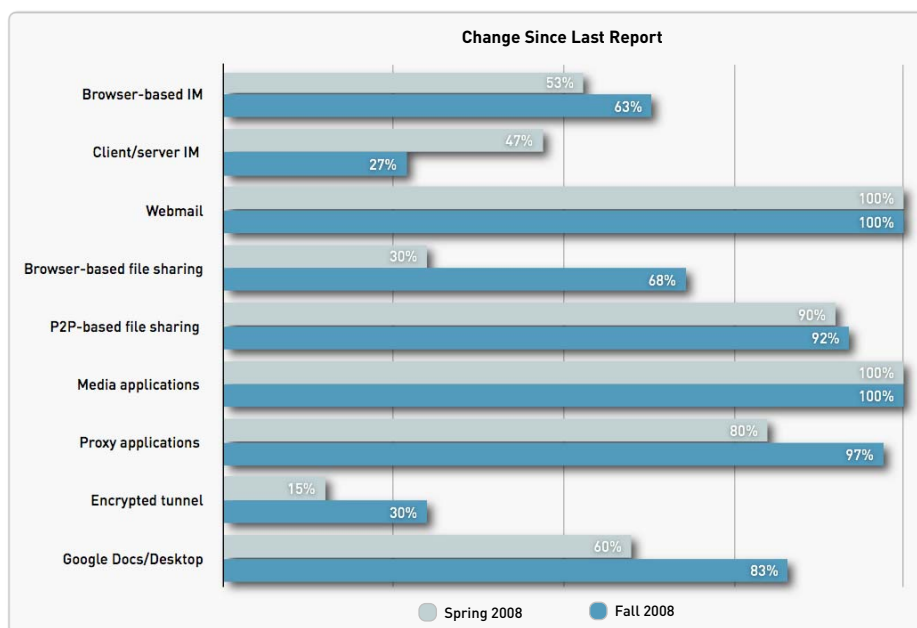
About Palo Alto Networks

Palo Alto Networks™ enables visibility and policy control of applications and content running on enterprise networks. Based on innovative App-ID™ application classification technology, the Palo Alto Networks family of next-generation firewalls accurately identifies applications – regardless of port, protocol, evasive tactic or even SSL encryption – at 10Gbps with no performance degradation. Enterprises can now set and enforce application usage policies to meet compliance requirements, improve threat mitigation and lower operational costs. For more information, visit www.paloaltonetworks.com

Appendix 1: Changes Between Application Usage and Risk Report Spring and Fall Editions (2008)

The changes between *Application Usage and Risk Report Version 1 (Spring Edition, 2008)* and *Version 2 (Fall Edition, 2008)* are summarized below.

- **Instant messaging:** Use of instant messaging overall went up slightly from 95% to 97%. Browser-based IM applications showed an increase from 53% to 63% while the use of client/server-based IM applications dropped from 47% to 27%.
- **Webmail:** There was no change in webmail usage – both studies show 100% usage.
- **Browser-based file sharing/storage:** These applications showed significantly increased usage, from three variants being found 30% of the time to 18 variants being found 68% of the time.
- **Peer-to-peer file sharing:** The use of P2P file sharing applications increased incrementally from 90% to 92%. The biggest change between the two reports was the number of P2P variants found—Version 1 saw only nine variants while Version 2 saw 18 variants.
- **Media applications:** Very little change overall at close to 100% for audio and video. The underlying technology showed some changes as P2P showed some increased popularity. Of the 38 audio and video applications found, 21% (eight) are based on P2P, 34% (13) are client/server based and 34% (17) are browser-based.
- **Proxies and encrypted tunnel:** Non-IT supported proxies and encrypted tunnel applications were found with greater frequency than in the previous report appearing 97% of the time (proxies) and 30% of the time (encrypted tunnel). The previous report showed proxies at 80% and encrypted tunnel at 15%.
- **Remote desktop control:** The previous report showed remote desktop control application usage at 75% while the new version shows usage jumping to 93%.
- **Google applications:** The earlier version of the report showed use of Google applications such as Docs and Desktop, increasing from a mere 60% to 80% and 83% respectively.



Appendix 2: Methodology

The data in this report is generated by the Palo Alto Networks Application Visibility and Risk assessment process when a Palo Alto Networks next-generation firewall is deployed within the customer network, in either tap mode or virtual wire mode, to monitor traffic traversing the Internet gateway. At the end of the data collection period, usually one to seven days, an *Application Visibility and Risk Report* is generated that presents the findings along with the associated business risks and a more accurate picture of how the network is being used. The data from each of the AVR Reports is then aggregated and analyzed, resulting in *The Application Usage and Risk Report*.

The application visibility that Palo Alto Networks' next-generation firewalls provides is delivered by a patent-pending technology called App-ID. Designed to address security evasion tactics commonly used in many of today's new applications, App-ID uses as many as four identification techniques to determine the exact identity of applications flowing in and out of the network.

Application visibility does not stop with application identity. If it did, the application identity would not help the administrator make more informed decisions about how to treat the application. Presented with the name of an application never before seen on the network, of which there may be many, an administrator may be inclined to block it. It is not about telling an administrator that an application is "bad" and should be blocked. The more effective approach is to present a complete picture of what the application is and how it is being used. With the Palo Alto Networks solution, administrators are presented with the application name, a description, its characteristics and its underlying technology, allowing administrators to make much more informed security policy decisions.

To facilitate the decision making process on how to treat an application, Palo Alto Networks provides additional background for more than 700 applications including a detailed description, alternative sources of information and which port(s) are commonly used. To help keep administrators more informed, eight different application characteristics are provided.

The accurate identification of the application by App-ID solves only part of the visibility and control challenge that IT departments face with today's Internet-centric environment. Inspecting permitted application traffic becomes the next significant challenge and one that is addressed by Content-ID.

Content-ID melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing. Content-ID works in concert with App-ID, leveraging the application identity to help make the content inspection process more efficient and more accurate.

To view details on all 700 applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications located here <http://www.paloaltonetworks.com/arc/>.

Appendix 3: Most Common Applications Found

Listed below are all of the applications found across all 60 organizations, ranked in terms of frequency. Note that there is a mix of consumer or end-user oriented applications along with a wide range of business and networking applications. To view details on all 700 applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications located here <http://www.paloaltonetworks.com/arc/>.

1. SSL	64. YAHOO-IM	128. BLOGGER-BLOG-POSTING	191. YAHOO-WEBCAM
2. DNS	65. SNMP-TRAP	129. NETFLOW	192. ORB
3. FLASH	66. METACAFE	130. GRE	193. AZUREUS
4. WEB-BROWSING	67. SKYPE-PROBE	131. TEREDO	194. SECOND-LIFE
5. ICMP	68. IPSEC-ESP-UDP	132. ORACLE	195. UPNP
6. HOTMAIL	69. EMULE	133. RDT	196. IPV6
7. SOAP	70. GMAIL-CHAT	134. IMEEM	197. SYMANTEC-SYST-CENTER
8. NTP	71. RADIUS	135. CISCOVPN	198. X11
9. SNMP	72. MSSQL-MON	136. WEBEX	199. LOTUS-NOTES
10. YOUTUBE	73. MYSPACE-MAIL	137. CITRIX	200. SEVEN-EMAIL
11. MS-UPDATE	74. LIVEJOURNAL	138. VNC	201. SSDP
12. HTTP-AUDIO	75. SKYPE	139. IMESH	202. ICQ
13. GMAIL	76. KERBEROS	140. SUBSPACE	203. SCPS
14. YAHOO-MAIL	77. RTSP	141. MEDIUM-IM	204. DAYTIME
15. SMTP	78. TELNET	142. VEOHTV	205. PPSTREAM
16. FTP	79. WEBSHOTS	143. H15	206. ULTRASURF
17. NETBIOS-NS	80. SQUIRRELMAIL	144. TRENDMICRO	207. RIP
18. GOOGLE-SAFEBROWSING	81. ORKUT	145. TACACS-PLUS	208. NETMEETING
19. AIM-MAIL	82. LIVE365	146. SLP	209. ICHAT-AV
20. WEBDAV	83. REUTERS-DATA-SERVICE	147. LPD	210. DIRECT-CONNECT
21. NETBIOS-DG	84. YAHOO-VOICE	148. SOCIALTV	211. KAZAA
22. RSS	85. MSSQL-DB	149. ESNIPS	212. POGO
23. YAHOO-TOOLBAR	86. POP3	150. MSN-WEBMESSENGER	213. JIRA
24. GOOGLE-CALENDAR	87. MSN-TOOLBAR	151. QQ	214. GOTOMYPC
25. HTTP-PROXY	88. CGIPROXY	152. NETSPOKE	215. TEAMVIEWER
26. FACEBOOK	89. ACTIVE-DIRECTORY	153. MEEVEE	216. FRIENDFEED
27. AIM-EXPRESS	90. WEB-CRAWLER	154. MYSPACE-VIDEO	217. NFS
28. YAHOO-WEBMESSENGER	91. NORTON-AV-BROADCAST	155. PCANYWHERE	218. BOXNET
29. GOOGLE-TOOLBAR	92. MS-NETLOGON	156. DOTMAC	219. NEONET
30. HTTP-VIDEO	93. MSN-VOICE	157. HORDE	220. SUBVERSION
31. MYSPACE	94. CITRIX-JEDI	158. IPSEC-ESP	221. USERPLANE
32. RTMPT	95. LOGMEIN	159. LIVELINK	222. GTALK-FILE-TRANSFER
33. FLEXNET-INSTALLANYWHERE	96. XM-RADIO	160. JABBER	223. AUTOBAHN
34. LDAP	97. TWITTER	161. YAHOO-FILE-TRANSFER	224. WHOIS
35. MSN	98. LIVE-MEETING	162. YUM	225. L2TP
36. GOOGLE-ANALYTICS	99. WORLDOWARCRAFT	163. MS-GROOVE	226. OSPFIGP
37. RTMP	100. SHAREPOINT-ADMIN	164. PHOTOBUCKET	227. FRIENDSTER
38. APPLE-UPDATE	101. GOOGLE-TALK	165. SHOUTCAST	228. COOLTALK
39. ADOBE-CONNECT	102. RTP	166. CORBA	229. GTALK-VOICE
40. MSRPC	103. MSN-FILE-TRANSFER	167. IRC	230. MAIL.COM
41. SSH	104. TIME	168. BLACKBOARD	231. SEND-TO-PHONE
42. SHAREPOINT	105. PHPROXY	169. DEALIO-TOOLBAR	232. GOOGLE-LIVELY
43. GOOGLE-PICASA	106. MEEBOME	170. FOLDING-AT-HOME	233. ILOVEIM
44. STUMBLEUPON	107. IMAP	171. PPTP	234. AIM-FILE-TRANSFER
45. OUTLOOK-WEB	108. MEEBO	172. MEDIAWIKI-EDITING	235. SAP
46. ATOM	109. MMS	173. BLACKBERRY	236. VMWARE
47. GOOGLE-DESKTOP	110. MEGAUPLOAD	174. PANDO	237. DAILYMOTION
48. SYSLOG	111. YOUSENDIT	175. LWAPP	238. BLIN
49. ITUNES	112. HULU	176. IPP	239. SOPCAST
50. BACKWEB	113. PORTMAPPER	177. MYSQL	240. EIGRP
51. BITTORRENT	114. HP-JETDIRECT	178. FACEBOOK-MAIL	241. H.245
52. STUN	115. PANDORA	179. XUNLEI	242. SIGHTSPEED
53. GOOGLE-EARTH	116. GNUTELLA	180. SHAREPOINT-DOCUMENTS	243. FASTMAIL
54. MS-RDP	117. SORIBADA	181. RPC	244. MEDIAFIRE
55. MS-DS-SMB	118. MYSPACE-IM	182. SLING	245. SHAREPOINT-CALENDAR
56. GOOGLE-DOCS	119. COX-WEBMAIL	183. OPTIMUM-WEBMAIL	246. WINS
57. SPARK	120. TFTP	184. VERIZON-WSYNC	247. RADIUSIM
58. MS-EXCHANGE	121. ARES	185. BOMBERCLONE	248. GOTOMEETING
59. IKE	122. MOVE-NETWORKS	186. NNTP	249. JASPERSOFT
60. AIM	123. SIP	187. FREEGATE	250. ECHO
61. COMCAST-WEBMAIL	124. BLOG-POSTING	188. MCAFEE	251. WEBEX-WEBOFFICE
62. DHCP	125. SALESFORCE	189. WEBSense	252. ZIMBRA
63. NETBIOS-SS	126. EBUDDY	190. LOGITECH-WEBCAM	253. TOR
	127. FACEBOOK-CHAT		254. DEPOSITFILES

255. DOCSTOC	329. ZOHO-SHOW	403. SCTP
256. FOLDERSHARE	330. PNA	404. UNASSIGNED-IP-PROT
257. MEDIAMAX	331. GLYPE-PROXY	405. WCCP
258. STEAM	332. KPROXY	406. AVAYA-PHONE-PING
259. YOUSEEMORE	333. VNC-HTTP	407. WRITEBOARD
260. NETVMG-TRACEROUTE	334. YOICS	408. RTCP
261. YPSERV	335. RPING	409. CIRCUMVENTOR
262. MOUNT	336. TIKIWIKI-EDITING	410. MEGAPROXY
263. MS-WINS	337. RUCKUS	411. PRIVAX
264. LOTUS-SAMETIME	338. HUSHMAIL	412. JAP
265. CUPS	339. GROUPWISE	413. PINGFU
266. MS-SMS	340. QQ-DOWNLOAD	414. BEINSYNC
267. CORALCDN-USER	341. PERFORCE	415. NETVIEWER
268. RSH	342. MESSENGERFX	416. BGP
269. XOBNI	343. ZOHO-IM	417. NDMP
270. KASPERSKY	344. MS-OCS	418. TOKBOX
271. TIVOLI-STORAGE- MANAGER	345. POWNCE	419. VSEE
272. H.323	346. FINGER	420. OOVVOO
273. FILEMAKER-PRO	347. ALTIRIS	421. VENTRILO
274. SYBASE	348. CPQ-WBEM	422. MSN-MONEY-POSTING
275. TWIG	349. ZELUNE	423. SHAREPOINT-WIKI
276. 100BAO	350. SOCKS	424. YAHOO-FINANCE- POSTING
277. POKER-STARS	351. RLOGIN	
278. MS-WIN-DNS	352. EGP	
279. NCP	353. MOBILE-ME	
280. PPLIVE	354. CAMFROG	
281. CARBONITE	355. ZOHO-WIKI	
282. MOZY	356. DABBLEDB	
283. RSYNC	357. DB2	
284. SCCP	358. ILOHAMAIL	
285. CVS	359. QQ-MAIL	
286. NETEASE-MAIL	360. SECURESERVER-MAIL	
287. OPEN-WEBMAIL	361. ZENBE	
288. SECURE-ACCESS	362. LOTUS-NOTES-ADMIN	
289. DROP.IO	363. SUGAR-CRM	
290. SOULSEEK	364. INFOREACH	
291. SOURCE-ENGINE	365. PARTY-POKER	
292. APC-POWERCHUTE	366. ICCP	
293. APPLE-AIRPORT	367. T.120	
294. YUGMA	368. ICQ2GO	
295. ETHERIP	369. SPARK-IM	
296. RSVP	370. CAMPFIRE	
297. ZOHO-SHEET	371. RAZOR	
298. UUSEE	372. IP-IN-IP	
299. MSN-VIDEO	373. MS-SCHEDULER	
300. IPSEC-AH	374. RSTATD	
301. 4SHARED	375. WLCCP	
302. FS2YOU	376. ZOHO-WRITER	
303. RAPIDSHARE	377. MEABOX	
304. ELLUMINATE	378. MIRO	
305. DISCARD	379. HTTP-TUNNEL	
306. MS-DTC	380. DESKTOPTWO	
307. EDITGRID	381. CROSSLOOP	
308. TVU	382. IGMP	
309. JOOST	383. IGP	
310. VTUNNEL	384. FILEMAKER- ANOUNCEMENT	
311. HOPSTER	385. GDS-DB	
312. RADMIN	386. INFORMIX	
313. XDMCP	387. POSTGRES	
314. BACKUP-EXEC	388. INNOVATIVE	
315. SIEBEL-CRM	389. DROPBOKS	
316. FILEDROPPER	390. DYNAMICINTRANET	
317. XDRIVE	391. MS-FRS	
318. YOURFILEHOST	392. IMHAHA	
319. GNUNET	393. MEETRO	
320. MANOLITO	394. MS-OCS-FILE-TRANSFER	
321. WOLFENSTEIN	395. BBN-RCC-MON	
322. CONCUR	396. CPNX	
323. KOOLIM	397. HOST	
324. IMVU	398. IPCOMP	
325. EBAY-DESKTOP	399. IPLT	
326. MS-IIS	400. MFE-NSP	
327. SOPHOS-UPDATE	401. PGM	
328. ZOHO-NOTEBOOK	402. RESERVED	