The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

7th Edition, May 2011

Palo Alto Networks
www.paloaltonetworks.com

Table of Contents

Executive Summary

The *Application Usage and Risk Report (7th Edition, May 2011)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing 1,253 application traffic assessments conducted between October 2010 and April 2011.

This edition of the report looks at application traffic from three very different perspectives. First, an analysis of the associated business and security risks that are effectively hidden within a wide range of applications that can use of SSL in some way, shape, or form, or can hop from port-to-port. The second section will discuss the increasingly social aspects of the workplace. Finally, the third section will analyze the question of whether the historical business and security risks associated with filesharing and file transfer applications will repeat themselves as browser-based filesharing offerings battle for market share.

Key findings include:

Hidden application traffic: more than 40% of the applications can use SSL or hop ports; consuming roughly 36% of the overall bandwidth observed.

- Applications using SSL in some way, shape or form represent 25% (262) of the applications found and 23% of the overall bandwidth used. This segment of applications will continue to grow as more applications follow Twitter, Facebook and Gmail, who all have enabled SSL either as a standard setting or as a user-selectable option.

- Dynamic applications (aka, port hopping) represent 16% (171) of the applications found and 13% of the bandwidth consumed. In general, the types of applications that hop ports are consumer oriented and include instant messaging, P2P, and photo video. There is no reason to expect the use of port hopping as an accessibility feature by application developers to decrease.

The work place: it has become more social.

- Contrary to popular opinion, social networking has not meant the death knell of instant messaging (IM) and webmail. Compared with 12 months ago, IM traffic, as a % of overall traffic has more than doubled; webmail and social networking increased nearly 5 fold.

File transfer applications: will history repeat itself?

- The progression from FTP, to P2P, to browser-based file sharing all show strikingly similar risk and reward characteristics. These applications, found with 92%, 82%, and 91% frequency respectively, each provide business value, but represent security and business risks that may include exploits, malware vectors, and data loss (intentional or otherwise).

- As browser-based filesharing applications leverage peer-based technology and add clients as a "premium offering", the question arises: will the business and security risks introduced by browser-based filesharing follow the same path as those that were introduced by P2P.

The traffic analyzed in this report is collected as part of the Palo Alto Networks customer evaluation methodology where a Palo Alto Networks next-generation firewall is deployed to monitor and analyze the network application traffic. At the end of the evaluation period, a report is delivered to the customer that provides unprecedented insight into their network traffic, detailing the applications that were found, and their corresponding risks. The traffic patterns observed during the evaluation are then anonymously summarized in the semi-annual Application Usage and Risk Report.

Introduction

With a sample size of 1,253 participating organizations, a number that is nearly double that of the previous report, and a view into more than 28 exabytes (28,046,165,463,032,900,000) worth of data, the latest edition of the Application Usage and Risk Report (May 2011) is, arguably, the largest application analysis of its kind.

In this edition of the report, several assumptions about the types of traffic traversing corporate networks; the associated business and security risks and the claimed growth rates are either confirmed refuted.

The assumption that organizations equate tcp/443 solely to applications that can use SSL is shattered. In fact, as the analysis shows, many applications can use SSL on a range of ports and are indeed browser-based, yet they may or may not use tcp/443.

The massive growth in social networking has instilled the assumption that the growth is at the expense of other collaborative applications (IM and email), or worse yet, employee productivity. Here too, the assumption is proven to be just that; an erroneous assumption that is not based on fact. The facts show that despite the 5 fold growth of social networking, other applications, predicted to slow as a result, have actually grown significantly.

Finally, the assumption that the simplicity and value of browser-based filesharing applications are less risky than their FTP- and P2P-based counterparts also be analyzed and proven baseless.

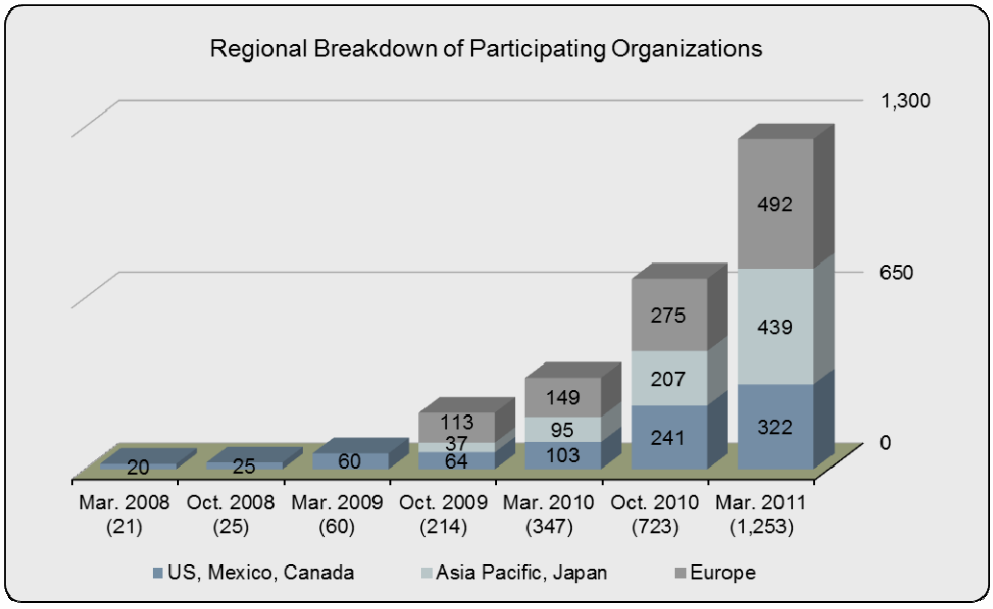


Figure 1: Geographic distribution of participating organizations.

SSL and Port Hopping Applications: The Elephant in the Room?

The analysis shows that applications that can use SSL in some way, shape or form, or can hop ports represent a large, yet often ignored segment of traffic traversing the network. Collectively, this segment of traffic represents 41% (433) of the 1,042 applications and consumes over one-third of the bandwidth.

SSL is commonly viewed as a means of encrypting traffic to keep it secure. Financial transactions, healthcare interaction, retail purchases and collaboration are the most common examples of where SSL is used, but in fact, it is used far more widely than expected. In some cases, the use of SSL is to hide content, such as threats or stolen data. In other cases, it is used merely as a means of evading detection. Both of these cases exemplify why organizations should be more aware of which applications are using SSL and how often.

A similar argument can be made around those applications that can hop ports. From an accessibility perspective, this feature makes complete sense as it helps eliminate barriers to use and in turn, can ensure success. There are examples of both business and end-user oriented applications that fit into this group. Unfortunately, some of the applications that can hop ports can introduce malware, or can result in the loss of confidential data.

The remainder of this section will discuss the use of SSL and port hopping as follows:

1. SSL on tcp/443 or any other port is the largest group of applications, many of which are end-user oriented (non-work). Accordingly, this group of applications represents the highest risk.
2. Those applications that can use SSL only on tcp/443 represent a small, yet heavily used set of applications including SSL, SSL VPN and a range of business applications.
3. The applications that can use SSL on any other port except tcp/ are an even smaller group of primarily business applications.
4. The second largest group of applications is those that can port hop. The types of applications in this group are both business and end-user oriented and as such, introduce their own business and security risks.

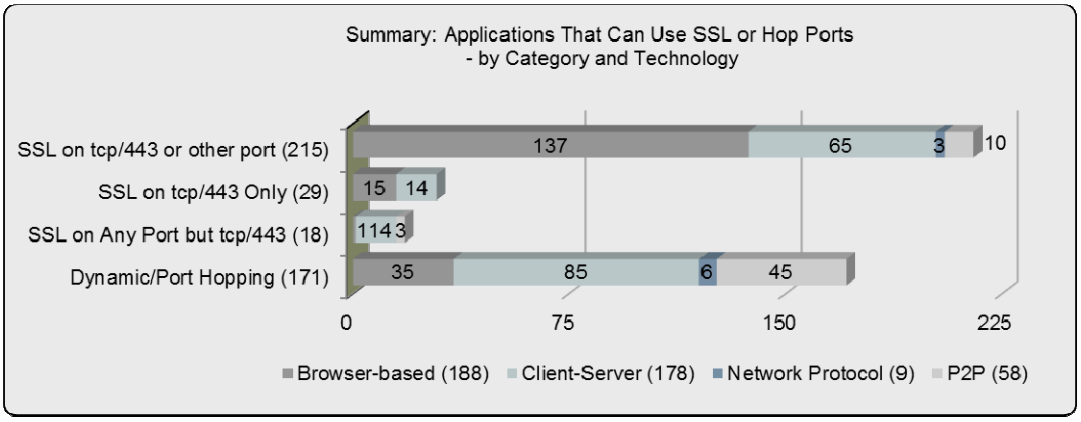


Figure 2: Applications that can use SSL or hop ports – broken out by category and underlying technology.

The interesting takeaway from figure 2 is the fact that over half of the applications (57%) that can use SSL do not use the browser, which can either be viewed as support for, or to dispel the concept that the browser is the next OS. However, one undisputed fact that the 57% re-affirms is that the strict adherence to the tcp/80, tcp/443 equals browser-based application development methodology is no longer adhered to.

While the number of applications that fall into this definition (can use SSL or hop ports) is higher than expected, the volume of traffic that already exists on an organization's network is even more surprising, and the amount, specifically the use of SSL, is only expected to grow. More application vendors are following the examples set by Gmail, Twitter, and Facebook who now allow users to access the respective applications via either HTTP (unsecured) and HTTPs (secured via SSL). The use of SSL will be further accelerated by the recent *HTTPS Now* initiative put forth by the Electronic Frontier Foundation (EFF) and Access, a digital freedom activist group. These groups are encouraging end-users to apply pressure on application vendors to support HTTPs as a default.

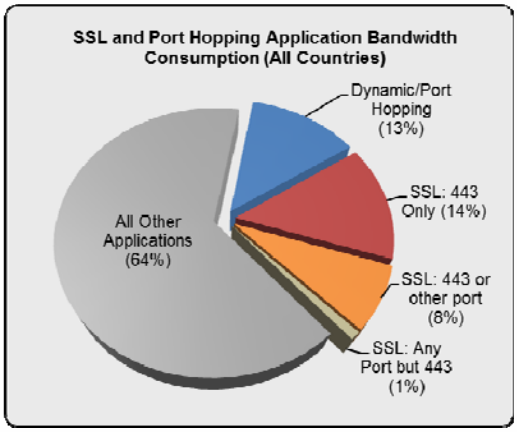


Figure 3: Bandwidth consumed by applications that can use SSL or hop ports.

As shown in figure 3, this group of applications consumed 36% of the overall bandwidth observed. More specifically applications that are capable of using SSL in some way represent nearly a quarter (23%) of the overall traffic – a significantly higher number than originally thought. Applications that can hop ports make up 16% (171) of the applications found, and they are consuming 13% of the overall bandwidth.

One of the challenges that an organization faces with SSL traffic is the inability to see inside to determine if the encrypted traffic is business, personal or threat oriented. Dynamic applications, also known as those that can port-hop, also pose lack of visibility problem but more from the perspective that the port that the application traversed during the last use may not be the same one used the next time.

SSL on tcp/443 or Other Ports: The Majority of the Applications and Potential Risks

Defined as the set of applications that can use SSL over tcp/443, or any other port including port 80, or can hop ports, this largest group of applications (215) epitomizes the duplicitous use of SSL and/or tcp/443 as both a security feature and an accessibility feature. Specifically, these applications **can** use SSL, they may not use it by default. Surprisingly this group of applications did not consume the most bandwidth, a mere 8% when compared to the 14% consumed by those applications that use SSL only on tcp/443.

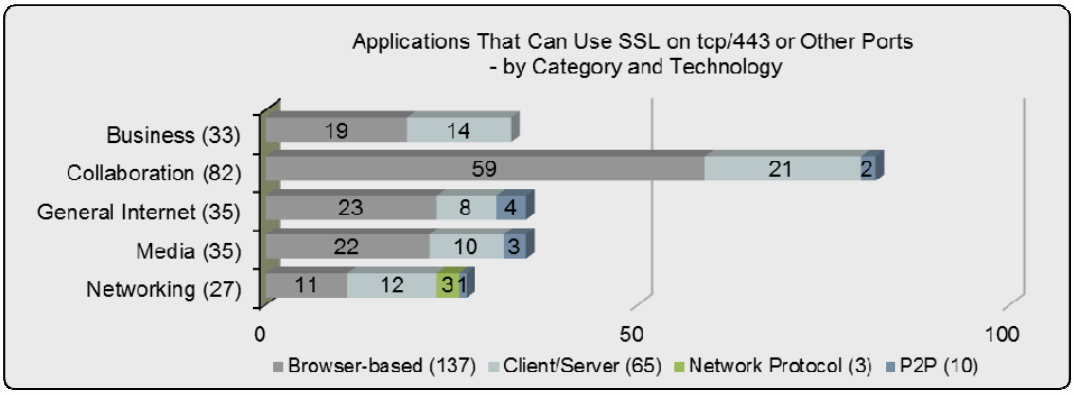


Figure 4: Category and technology breakdown of 215 applications that can use SSL on any port.

Some examples of the applications in this group include most all of the Google applications, as well as Facebook, Twitter and several software update and backup applications. As with the previous group, the dark side of this group of applications includes a wide range of external proxy, remote access and file-sharing (P2P, client-server and browser-based) applications.

The consumer-oriented nature of this set of applications means that the risks, both business and security, are significant. For example, Google-Docs, Facebook and Twitter are all used for both personal and professional use. Yet they are also known vectors for malware delivery; they are known to be used for botnet command and control; and they can be used for social engineering. The business risks include the question of whether or not they are "approved for use" as the potential loss of confidential data.

SSL on tcp/443 Only: A Small, but Significant Set of Applications

Applications that can use SSL on tcp/443 exclusively are a small (29), but significant set of applications. Examples of applications within this group range from SSL itself , to those that are clearly business focused (NetSuite, SalesForce.com, GoToMeeting), to several software update services. These types of applications are expected to be found flowing across tcp/443 in a secure manner. They have all been designed to use the web (HTTP and HTTPs) as a key element of their infrastructure.

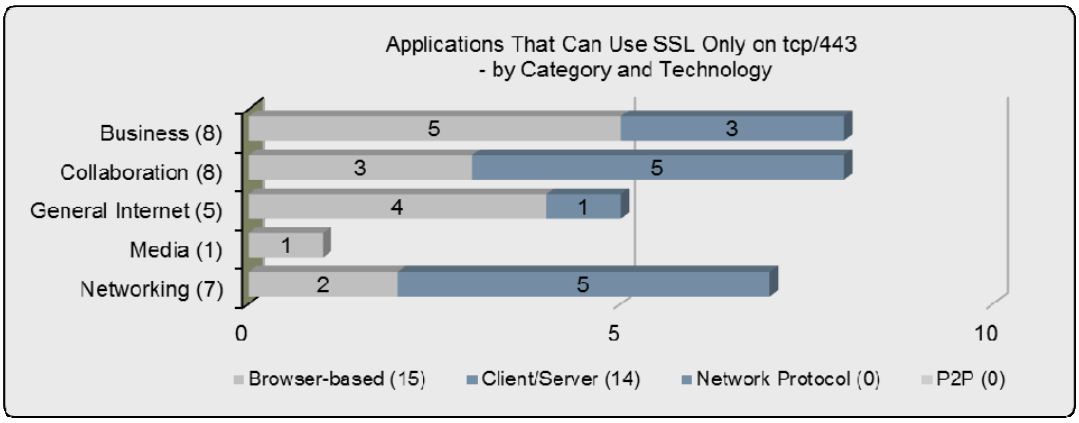


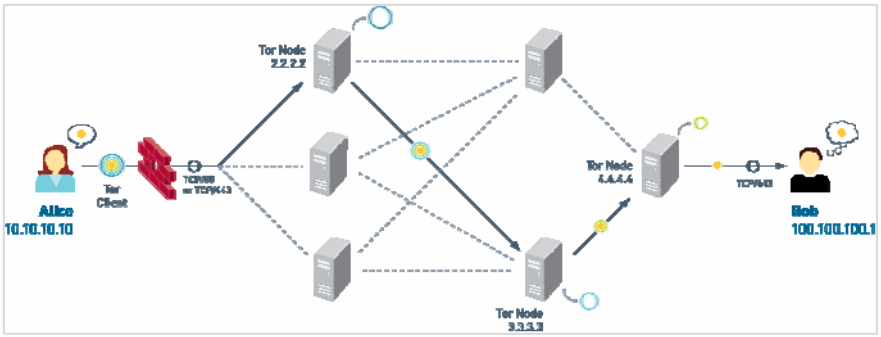
Figure 5: ***Category and technology breakdown of 215 applications that can use SSL on any port.***

Also included in this set of applications are some that may be considered to be consumer-class, task-enabling applications such as Dropboks and Foldershare (filesharing applications), which have also been designed to utilize the Internet as their infrastructure. The risk that these applications represent is the plain fact that they are invisible to traditional security infrastructure, making the possible transmission of confidential date or malware a very real possibility.

The darker side of applications that can use SSL on port tcp/443 shows that Tor was found in 15% of the 1,253 organizations analyzed. Typically, Tor has little or no business use and is a very evasive application.

Designed by U.S. military, Tor leverages the Internet and uses a combination of layered encryption (like an onion) and random paths to ensure privacy.

Figure 6: How Tor ensures privacy using random paths and layered encryption.



When a message is sent, sender's Tor client (a SOCKS proxy) communicates with directory server to determine random path to intended recipient via series of Tor nodes. Client then encrypts payload using keys from each of the relays successively. At each node, a layer of encryption is removed (via the node's private key) and then sent to next node. The message is ultimately delivered to the recipient in clear text.

SSL on Dedicated, Non-Standard Ports: Some Business, Some Purposely Evasive

This group of applications is the smallest group (18) and consumes only 1% of the overall bandwidth. Included in this group of applications are business applications such as Cisco VPN, and Microsoft Exchange. Also included are several applications that are several instant messaging applications which can span both business and personal use.

As with the previous groups of applications, there are several that are known to be used to evade security, including UltraSurf one of the most evasive applications on the market. Teamviewer, a very popular opensource remote desktop access application, with a client for nearly every type of device and Gotomypc also appear in this group.

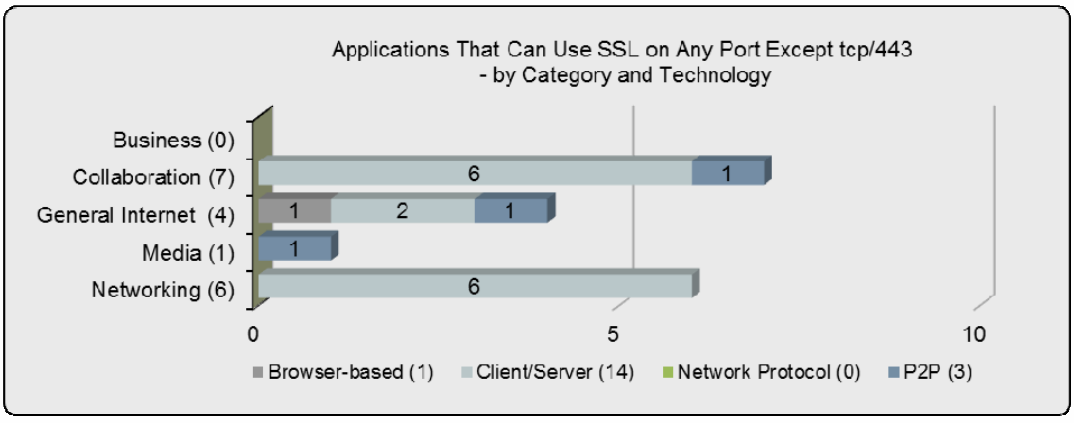


Figure 7: Category and technology breakdown of applications that can use SSL on any port EXCEPT tcp/443.

Applications That Can Use SSL: A Discussion of Risk vs Reward

To be clear, the SSL discussion is not meant to imply that SSL is bad and should not be used. Indeed, it helps protect our identity, our data, our financial transactions and much, much more. The purpose of the discussion was to highlight just how many applications can use SSL and the bandwidth that they are consuming. However, there are many obvious cases where the use of SSL is duplicitous. On one hand, it is meant to secure the payload, while on the other, it is used because it will easily traverse a firewall because it can use a commonly open port. It is important for organizations to consider policy adjustments to account for those applications that can use SSL in some way, shape or form.

Applications That Port Hop: The Ultimate Accessibility Feature?

Building an application, particularly one that is consumer focused, that hops ports as a feature makes good business sense because it means that the application is easier to use wherever the user is. This fact may explain why port-hopping represent 16% (171) of the applications found and 13% of the bandwidth consumed. One of the very first applications to implement port hopping as a means of improving access was AOL Instant Messaging (AIM). Now, many other instant messaging applications, along with P2P filesharing, gaming and streaming media fall into this group of applications.

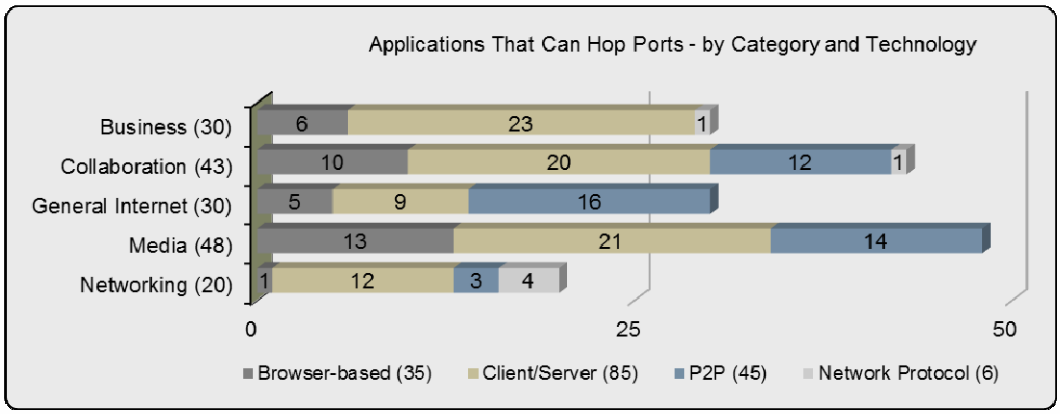


Figure 8: Category and technology breakdown of the 171 port hopping applications observed.

The slippery nature of applications that can hop ports means that organizations will continually struggle to identify and control them. The consumer-oriented nature of port hopping applications means that the business and security risks are similar to those discussed in the earlier SSL on any port section. From a security perspective, many of these applications are known to have vulnerabilities and can act as a malware vector. The business risks include the question of whether or not they are "approved for use" and many of them, in particular, the P2P filesharing applications, introduce the potential risk of loss of confidential data.

Also included within this group of applications are a wide range of purely business applications such as Microsoft Sharepoint, Netflow, and several VoIP applications. In these cases, there is a subtle yet important distinction in how port hopping is being used – it is not a means of evading detection, it is more a function of how the application operates and it is a requirement.

Work is Increasingly Social

Many social networking proponents have predicted that the rapid rise of social networking will lead to the death of instant messaging (IM) and webmail (all browser-based email excluding outlook-web and Gmail Enterprise). As Mark Twain was once have said, *"the report of my death was an exaggeration,"* so too has been the rumored death of instant messaging and webmail at the hands of social networking. The data shows the exact opposite; despite the growth of social networking, both IM and webmail have shown fairly significant growth rates. Compared with 12 months ago, instant messaging traffic, as a percentage of overall bandwidth, has more than doubled; webmail and social networking have increased nearly 500%.

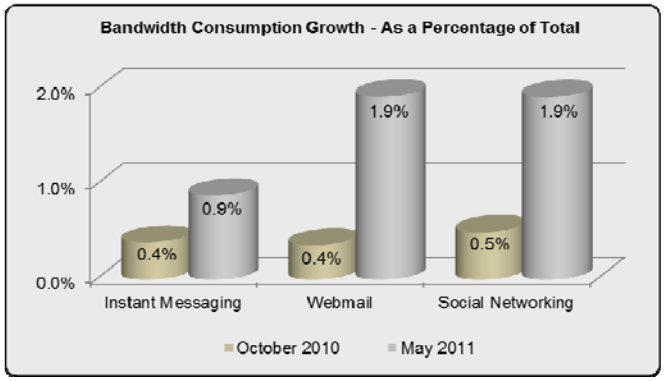


Figure 9: Growth comparison for instant messaging, webmail and social networking.

	April 2010			May 2011		
	Applications Found	Bandwidth (Terabytes)	Percentage of Total Bandwidth	Applications Found	Bandwidth (Petabytes)	Percentage of Total Bandwidth
Instant Messaging	62	2.3 TB	0.4%	75	249.8 PB	0.9%
Webmail	42	2.1 TB	0.4%	40	541.9 PB	1.9%
Social Networking	36	2.9 TB	0.5%	62	540.7 PB	1.9%
Subtotal	140	7.3 TB	1.3%	177	1,332.4 PB	5%
Totals	742	578.0 TB	--	1,042	28,046.2 PB	--

The collective 5% of the overall bandwidth is a very small percentage, but the growth rates are significant. Looking more deeply into the IM and webmail categories shows that while Facebook Mail and Facebook Chat are commonly used, neither of them contributed significantly to the overall category growth, which indicates that the usage was largely distributed across the top 5 applications shown below.

Application	Frequency	Bytes Consumed	Percentage of Webmail Traffic
Gmail	95%	213 Petabytes	39%
Hotmail	92%	178 Petabytes	33%
Yahoo-mail	90%	137 Petabytes	25%
Facebook-mail	83%	9 Petabytes	2%
Linkedin-mail	48%	735 Terabytes	0.1%

In some respects, the growth of social networking may have a certain influence on the growth of IM and webmail. While there is nothing specific in the data that supports this assertion, an argument could be made that IM and webmail can be used to share with those who have not yet been assimilated into the Facebook community. Additionally, an argument can also be made that those who become accustomed to the concept of sharing on Facebook, will do so on IM and webmail as well.

Social Networking: Big Growth for a Select Few

The increase in instant messaging and webmail shows that this application segment is still healthy and strong but the nearly 5 fold growth (based on % of bandwidth consumption) in social networking is largely attributed to a select few vendors; namely Facebook, Linkedin, and Twitter.

The dominance of these three applications is best shown through a comparison with the last *Application Usage and Risk Report, (6th Edition, Fall 2010)* where the statistics showed the dominance of Facebook collectively consuming 78% of the overall social networking bandwidth, leaving a mere 22% for the other social networking applications to battle over.

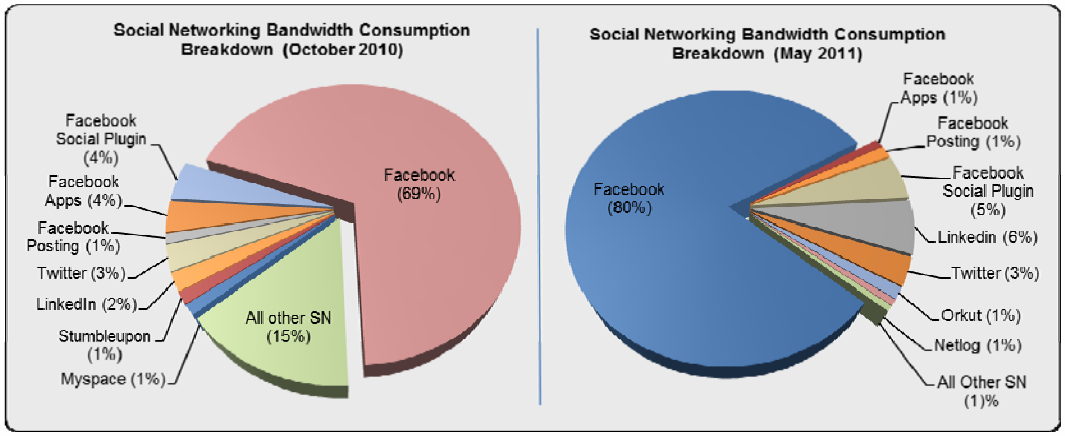


Figure 10: Social networking bandwidth consumption comparing six month usage ending October 2010 and May 2011.

The latest report shows the Facebook juggernaut gaining speed to the point where 87% of all social networking bandwidth is Facebook related. Of the 62 different social networking applications found, Linkedin and Twitter use the next closest amount of bandwidth at 6% and 3% respectively. More importantly is the fact that after the top eight social networking applications, there is a mere 1% of the bandwidth being shared among the remaining 54 social networking applications.

The Facebook traffic pattern within the organization remains one that is relatively passive as shown by the relatively small numbers associated with Facebook-posting and Facebook-apps. This data point weakens the argument that social networking is a productivity drain. Users are working while their Facebook page is open. Nothing more.

The growth in social networking is remarkable. A year ago, the bulk of the Facebook use could be attributed, in large part, to non-work related activity. Now, corporations have increased their presence dramatically with efforts (and spending) predicted to grow significantly in 2011 as shown in the report, *the state of corporate social media in 2011* from usefulsocialmedia.com.

- The majority of companies expect social media to become integrated into more than just marketing throughout 2011.
- 89% of the companies expect social media budgets to increase over 2011.
- The most common corporate social media use is for marketing (88%) and communications (93%).
- By the end of 2011, the biggest change in corporate use of social media will be the growth of companies using it for customer service (73%), employee engagement (59%) and product development (52%).

Missing from the growth in corporate social media use discussion is how to manage the associated business and security risks. The business risks include what employees can and should post, or say about themselves, the projects they work on and the company. The security risks are fairly well known, applications such as Facebook, Twitter, and Linkedin, all are commonly used as information sources for social engineering and they are all commonly used as avenues for malware delivery.

File Transfer/Sharing Applications: Will History be Repeated?

Transferring or sending large files is, and has been, an integral part of the business world for many years. An argument could be made that without the ability to transfer files electronically, business would be significantly more difficult; files would be sent on CD or disk drive via US mail, or other means, thereby slowing key business processes such as batch inventory reporting, manufacturing/supply chain data, manufacturing/design, IT files, claim processing.

The analysis showed that FTP (client-server), P2P, and browser-based file sharing applications were found with 92%, 82% and 91% frequency respectively. The analysis shows that while FTP is very popular and heavily used, browser-based filesharing has grown in terms of the number of variants (now at 60), popularity and bandwidth usage.

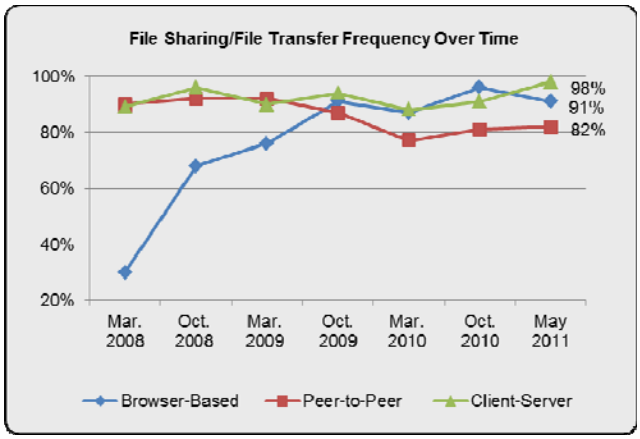


Figure 11: Historical frequency that file sharing/file transfer applications were found in use within an organization.

The dark side of the growth in popularity and usage are the business and security risks, which show all the signs of being similar to those associated with P2P and, in some respects, FTP. Viewed from a bandwidth consumption perspective, filesharing applications as a category (peer-to-peer, browser-based and client-server), consumed nearly 9% of the overall bandwidth. While 9% is a relatively small number, out of a possible 26 different application categories, filesharing consumed the 5th highest amount, as shown in figure 12.

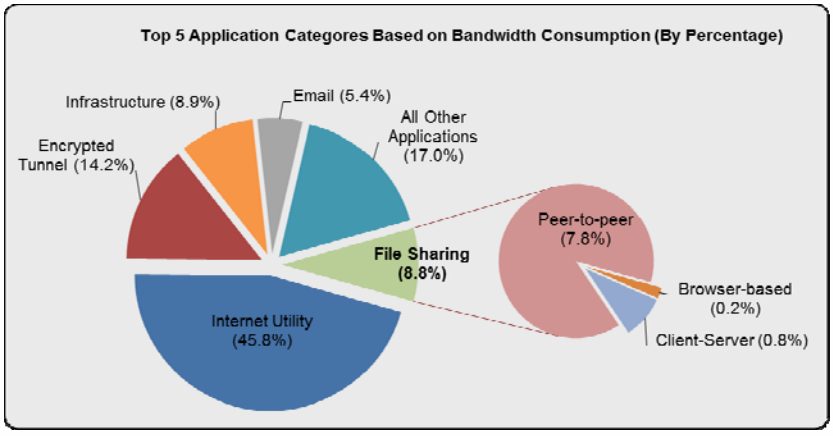


Figure 12: Percentage of total bandwidth consumed by top categories observed.

Each of these applications provides business value, but all of them carry security and business risks that may include exploits, malware vector, data loss (intentional or otherwise).

FTP: The Original File Transfer Application

Viewed historically, FTP is one of the original file transfer applications and it required a server, a network and a client to operate properly. Moving a file was done using command line interface via put and get commands, making use by a non-technical or causal user, at times, challenging. FTP, as originally designed, was never meant to be used in a modern Internet-based world, which only adds to the range of challenges that FTP introduces which may include:

- Misconfiguration of client or server, leading to open or insecure access. It is fairly easy for knowledgeable user to find open FTP sites proprietary files on them.
- Due in part because it is an application that is not designed for use in an internet-based era, FTP is susceptible to a wide-range of application level attacks including brute-force, DoS, code-execution, and buffer overflows.

Peer-to-peer (P2P): A Powerful Technology With a Bad Reputation

P2P file-sharing applications were never meant to replace FTP, however, they do enable efficient transfer of large files and BitTorrent is a known source for Linux binaries. The original intent of P2P technology was indeed for researchers to move large files.

Like FTP, P2P applications require a client and a server, which are commonly viewed as the same, along with a network. Common challenges that P2P applications introduce are similar to those found with FTP.

- Client and server may be misconfigured, leading to data loss either through inadvertent distribution of confidential data or purposeful searching for posted files. One of the more significant risks associated with the P2P one-to-many publication model is the fact that once a file has been uploaded, either purposely or otherwise, it is nearly impossible to delete it.
- Other notable challenges include illegal distribution of copyrighted materials, vulnerability exploits and a known vector for malware delivery.

Browser-based filesharing: Many Business Benefits; Many Potential Risks

One of the fastest growing, and most rapidly evolving application segments, browser-based filesharing applications show all the signs of introducing risks that are similar to those found in FTP and P2P. Initially, browser-based file sharing applications were an easy to use alternative to FTP. Using YouSendIt!, a few clicks of a mouse enables a large file to be quickly delivered to the recipient via HTTP or HTTPs via a URL.

One of the initial benefits that browser-based filesharing applications have over FTP or P2P applications is that there is no need for a client or server to be configured, seemingly eliminating the associated (mis)configuration risks. The user is accessing a cloud-based service via the browser which means that the risk of inadvertent data loss is minimized.

Moving forward, several examples of classic market expansion (new competitors or added services) will increase the risks associated with browser-based filesharing applications.

- **Premium services:** As a means of differentiation, many of the browser-based file sharing applications are beginning to offer premium services such as an option to index the file, making it searchable by anyone (RapidShare, MegaUpload, others). Other offerings (YouSendIt, DropBox, RapidShare) are providing users with an option to install a client, making the upload/download process easier.

- **Mixing underlying technologies:** Recent new offerings have begun augmenting the HTTP-based connection with other technologies to increase transfer speeds or to make the connection more peer-based. **Sendoid** is a recently released example that highlights this trend. Using RTMFP (Real Time Media Flow Protocol), a technology that establishes a direct connection between two individuals, Sendoid is able to send large files with amazing speeds. Essentially, when the recipient clicks on the file URL, they are connecting directly to the sender's PC via RTMFP to get the file. The Sendoid server, hosted by Amazon, is bypassed and a direct, peer-based connection is established. Sendoid is browser-based but a client version is said to be coming soon. Note that RTMFP is the same technology used for **ChatRoulette,** the live streaming video application.

In both of these market expansion examples, the business and security risks will undoubtedly increase as users are more directly exposing their PC, and the files stored therein, to outside users.

Summary

The traffic traversing an organizations' network has changed dramatically over the years and there is no reason to assume the rate of change will decrease. Users assume that it is acceptable to access any application, personal or work related, at any time, from anywhere. In many cases, the underlying features-accessibility, configuration or otherwise-are of little or no concern to the users, so long as the application is delivering the intended value. This [expected] user behavior introduces certain business and security risks, which is why organizations should be aware of these applications, and how much they are being used. This knowledge can then be applied to making more informed decisions on how to best treat the applications.

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its next-generation firewalls enable unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 20Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. Enterprises can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. Most recently, Palo Alto Networks has enabled enterprises to extend this same network security to remote users with the release of GlobalProtect™. For more information, visit www.paloaltonetworks.com.

Appendix 1: Methodology

The data in this report is generated via the Palo Alto Networks Application Visibility and Risk assessment process where a Palo Alto Networks next-generation firewall is deployed within the network, in either tap mode or virtual wire mode, where it monitors traffic traversing the Internet gateway. At the end of the data collection period, usually up 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.

Delivered as a purpose-built platform, Palo Alto Networks next-generation firewalls bring visibility and control over applications, users and content back to the IT department using three identification technologies: App-ID, Content-ID and User-ID.

- **App-ID:** Using as many as four different traffic classification mechanisms, App-ID™ accurately identifies exactly which applications are running on networks – irrespective of port, protocol, SSL encryption or evasive tactic employed. App-ID gives administrators increased visibility into the actual identity of the application, allowing them to deploy comprehensive application usage control policies for both inbound and outbound network traffic.

- **Content-ID:** A stream-based scanning engine that uses a uniform threat signature format detects and blocks a wide range of threats and limits unauthorized transfer of files and sensitive data (CC# and SSN), while a comprehensive URL database controls non-work related web surfing. The application visibility and control delivered by App-ID, combined with the comprehensive threat prevention enabled by Content-ID, means that IT departments can regain control over application and related threat traffic.

- **User-ID:** Seamless integration with enterprise directory services (Microsoft Active Directory, LDAP, eDirectory) links the IP address to specific user and group information, enabling IT organizations to monitor applications and content based on the employee information stored within Active Directory, eDirectory, LDAP or a range of terminal services solutions. User-ID allows administrators to leverage user and group data for application visibility, policy creation, logging and reporting.

- **Purpose-Built Platform:** Designed specifically to manage enterprise traffic flows using function-specific processing for networking, security, threat prevention and management, all of which are connected by a 20 Gbps data plane to eliminate potential bottlenecks. The physical separation of control and data plane ensures that management access is always available, irrespective of the traffic load.

To view details on more than1,250 applications currently identified by Palo Alto Networks, including their characteristics and the underlying technology in use, please visit Applipedia, the Palo Alto Networks encyclopedia of applications.

Appendix 2: Applications Found

The complete list of the 1,042 unique applications found, ranked in terms of frequency are listed below. To view details on the entire list of 1,200+ applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications at http://ww2.paloaltonetworks.com/applipedia/

1. dns (100%)
2. ssl
3. web-browsing
4. ping
5. ntp
6. netbios-ns
7. ms-update
8. google-analytics
9. flash
10. icmp
11. twitter
12. facebook
13. gmail
14. soap
15. rss
16. snmp
17. google-safebrowsing
18. adobe-update
19. http-audio
20. youtube
21. smtp
22. webdav
23. http-proxy
24. sharepoint
25. http-video
26. hotmail
27. facebook-social-plugin
28. ftp
29. photobucket
30. flickr
31. google-toolbar
32. silverlight
33. google-translate
34. rtmpt
35. yahoo-mail
36. atom
37. google-app-engine
38. linkedin
39. ldap
40. yahoo-im
41. ms-ds-smb
42. apple-update
43. netbios-dg
44. facebook-chat
45. rtmp
46. facebook-mail
47. itunes
48. google-calendar
49. google-docs
50. msn-webmessenger
51. limelight
52. facebook-posting
53. office-live
54. google-picasa
55. google-talk-gadget
56. vimeo
57. skype
58. ms-rdp
59. stumbleupon
60. symantec-av-update
61. ssh
62. facebook-apps
63. msrpc
64. yahoo-toolbar
65. meebo
66. asf-streaming
67. msn
68. google-cache
69. flexnet-installanywhere
70. google-desktop
71. dailymotion
72. mobile-me (75%)
73. myspace
74. t.120
75. netbios-ss
76. ocsp
77. skype-probe
78. kerberos
79. pop3
80. dhcp
81. skydrive
82. salesforce
83. stun
84. yahoo-webmessenger
85. babylon
86. bittorrent
87. web-crawler
88. twitpic
89. ipsec-esp-udp
90. google-earth
91. teamviewer
92. msn-voice
93. mssql-mon
94. telnet
95. google-talk
96. ike
97. syslog
98. sip
99. active-directory
100. ooyala
101. 4shared
102. rtmpe
103. ms-netlogon
104. mediafire
105. metacafe
106. mssql-db
107. ustream
108. megaupload
109. time
110. mail.ru
111. gmail-chat
112. shoutcast
113. docstoc
114. megavideo
115. last.fm
116. gmail-enterprise
117. logmein
118. rtp
119. myspace-video
120. friendfeed
121. boxnet
122. rtsp
123. sky-player
124. adobe-media-player
125. squirrelmail
126. teredo
127. dropbox
128. netlog
129. outlook-web
130. ms-sms
131. slp
132. citrix
133. rapidshare
134. hp-jetdirect
135. live365 (50%)
136. filestube
137. lpd
138. aim-express
139. hulu
140. plaxo
141. webshots
142. linkedin-mail
143. orkut
144. flixster
145. napster
146. twitter-posting
147. aim-mail
148. hotfile
149. bbc-iplayer
150. msn-file-transfer
151. clearspace
152. yousendit
153. rtcp
154. friendster
155. channel4
156. tidaltv
157. linkedin-posting
158. ssdp
159. livejournal
160. daum
161. emule
162. justin.tv
163. eset-update
164. ms-exchange
165. ebuddy
166. fotki
167. imap
168. lotus-notes
169. tudou
170. jabber
171. snmp-trap
172. nintendo-wfc
173. blackboard
174. vnc
175. coralcdn-user
176. yahoo-voice
177. backweb
178. akamai-client
179. blogger-blog-posting
180. depositfiles
181. vkontakte
182. oracle
183. blog-posting
184. brighttalk
185. yum
186. radius
187. msn-toolbar
188. grooveshark
189. ares
190. xunlei
191. shutterfly
192. divshare
193. horde
194. flashget
195. gotomeeting
196. pandora
197. ciscovpn
198. paloalto-updates
199. tftp
200. evernote
201. sharepoint-admin
202. 360-safeguard-update
203. millenium-ils
204. google-docs-enterprise
205. facetime
206. twig
207. meebome
208. youku
209. pandora-tv
210. sina-weibo
211. aim
212. portmapper
213. vbulletin-posting
214. gnutella
215. avaya-webalive
216. zimbra
217. kaspersky
218. steam
219. ms-groove
220. sendspace
221. yahoo-douga
222. upnp
223. worldofwarcraft
224. reuters-data-service
225. adobe-meeting
226. ppstream
227. sightspeed
228. irc
229. trendmicro
230. gre
231. sharepoint-documents
232. xobni
233. esnips
234. playstation-network
235. badongo
236. ipv6
237. mysql
238. azureus
239. myspace-im
240. cyworld
241. alisoft
242. seesmic
243. logitech-webcam
244. qq-mail
245. computrace
246. qq
247. iheartradio
248. yourminis
249. hyves
250. netvmg-traceroute
251. imvu (25%)
252. mogulus
253. hi5
254. imeem
255. netease-mail
256. imesh
257. phproxy
258. stickam
259. deezer
260. ichat-av
261. webex
262. pptp
263. trendmicro-officescan
264. qvod
265. echo
266. kaixin001
267. freenet
268. imo
269. netsuite
270. bugzilla
271. norton-av-broadcast

272. mediawiki-editing
273. xing
274. blackberry
275. yandex-mail
276. pogo
277. subversion
278. pplive
279. veohtv
280. live-meeting
281. ipsec-esp
282. rhapsody
283. oovoo
284. h.323
285. glype-proxy
286. open-vpn
287. comcast-webmail
288. stagevu
289. lokalisten
290. roundcube
291. zango
292. icq
293. hamachi
294. second-life
295. bet365
296. myspace-mail
297. mms
298. socks
299. 2ch
300. gmx-mail
301. freegate
302. activesync
303. isatap
304. capwap
305. h.245
306. google-wave
307. secureserver-mail
308. qqlive
309. lwapp
310. rpc
311. qqmusic
312. vmware
313. lineage
314. netflix
315. iloveim
316. tikiwiki-editing
317. source-engine
318. cgiproxy
319. classmates
320. bebo
321. files.to
322. netflow
323. yahoo-file-transfer
324. garena
325. corba
326. tvu
327. yoono
328. tor
329. ifile.it
330. nimbuzz
331. dotmac
332. whois
333. pcanywhere
334. qq-download
335. pando
336. evony
337. ipp
338. kaixin
339. mibbit
340. megashares
341. kazaa
342. flumotion
343. google-buzz
344. sharepoint-calendar
345. nfs
346. rsvp
347. daytime
348. octoshape
349. apple-airport
350. baofeng
351. h.225
352. ebay-desktop
353. qq-file-transfer
354. dcinside
355. kugoo
356. ultrasurf
357. mixi
358. open-webmail
359. niconico-douga
360. gtalk-voice
361. nntp
362. funshion
363. yammer
364. discard
365. drop.io
366. qq-games
367. itv-player
368. kkbox
369. fileserve
370. myspace-posting
371. spotify
372. gotomypc
373. babelgum
374. send-to-phone
375. netload
376. sopcast
377. odnoklassniki
378. timbuktu
379. l2tp
380. me2day
381. yourfilehost
382. web-de-mail
383. websense
384. simplite-msn
385. jaspersoft
386. rip
387. vkontakte-mail
388. instan-t-file-transfer
389. quora
390. tales-runner
391. cygnet-scada
392. uusee
393. rsync
394. weather-desktop
395. yahoo-webcam
396. citrix-jedi
397. tacacs-plus
398. filesonic
399. sap
400. jira
401. editgrid
402. xdmcp
403. veetle
404. chatroulette
405. teachertube
406. qq-audio-video
407. msn-video
408. msnshell
409. direct-connect
410. carbonite
411. adrive
412. studivz
413. hotspot-shield
414. sflow
415. socialtv
416. viadeo
417. sybase
418. rping
419. ezpeer
420. sina-webuc
421. mcafee-update
422. fastmail
423. hangame
424. radmin
425. concur
426. filemaker-pro
427. all-slots-casino
428. wins
429. rpc-over-http
430. battlefield2
431. sakai
432. nate-mail
433. gadu-gadu
434. netviewer
435. gogobox
436. mount
437. baidu-webmessenger
438. finger
439. camfrog
440. microsoft-dynamics-crm
441. dcc-antispam
442. daum-mail
443. xbox-live
444. move-networks
445. boxnet-editing
446. clip2net
447. warcraft
448. poker-stars
449. plugoo-widget
450. afp
451. nateon-im
452. youtube-safety-mode
453. mozy
454. mixi-posting
455. libero-video
456. sccp
457. tonghuashun
458. google-docs-editing
459. woome
460. ncp
461. tudou-speedup
462. orb
463. medium-im
464. palringo
465. autobahn
466. panos-web-interface
467. git
468. wolfenstein
469. freeetv
470. ntr-support
471. messengerfx
472. bomgar
473. cisco-nac
474. regnum
475. ospf
476. zoho-im
477. svtplay
478. feidian
479. clubbox
480. filedropper
481. boxnet-uploading
482. naver-mail
483. neonet
484. gamespy
485. ms-scom
486. tv4play
487. gtalk-file-transfer
488. foxy
489. x11
490. xunlei-kankan
491. backup-exec
492. diino
493. ali-wangwang
494. genesys
495. hopster
496. vnc-http
497. cups
498. tivoli-storage-manager
499. gmail-video-chat
500. ms-win-dns
501. kaixin001-mail
502. lotus-sametime
503. checkpoint-cpmi
504. zoho-writer
505. rsh
506. hyves-chat
507. netspoke
508. cloudmark-desktop
509. dameware-mini-remote
510. mydownloader
511. webqq
512. t-online-mail
513. vtunnel
514. yantra
515. kontiki
516. panda-update
517. ndmp
518. postgres
519. symantec-syst-center
520. megashare
521. cvs
522. sling
523. meinvz
524. cox-webmail
525. fs2you
526. maplestory
527. ameba-now
528. avira-antivir-update
529. aim-file-transfer
530. eve-online
531. ms-wins
532. folding-at-home
533. zoho-sheet
534. spark
535. jango
536. soribada
537. soulseek
538. dealio-toolbar
539. aol-proxy
540. livelink
541. kino
542. miro
543. live-mesh
544. manolito
545. transferbigfiles
546. elluminate
547. cgi-irc
548. vkontakte-chat
549. gmail-call-phone
550. magicjack
551. youtube-uploading
552. hyves-mail
553. mgoon
554. streamaudio
555. twtkr
556. inforeach
557. dl-free
558. optimum-webmail
559. storage.to
560. dazhihui
561. afreeca
562. db2
563. fortiguard-webfilter
564. sophos-update
565. fetion
566. razor
567. unassigned-ip-prot
568. rdt
569. ameba-blog-posting
570. odnoklassniki-messaging
571. winamp-remote
572. nateon-file-transfer
573. pp-accelerator
574. qdown
575. userplane
576. earthcam
577. showmypc
578. ms-dtc
579. netmeeting
580. wikispaces-editing
581. yy-voice
582. renren-im
583. nate-video
584. zoho-wiki
585. informix
586. mediamax
587. forticlient-update
588. emc-networker
589. taku-file-bin

590. union-procedure-call
591. scps
592. runescape
593. hyves-games
594. ms-iis
595. crashplan
596. mail.ru-mail
597. call-of-duty
598. ibm-director
599. leapfile
600. ibm-bigfix
601. cpq-wbem
602. webex-weboffice
603. air-video
604. sbs-netv
605. livestation
606. kproxy
607. bebo-posting
608. youseemore
609. eigrp
610. hushmail
611. wiiconnect24
612. popo-im
613. tcp-over-dns
614. google-location-service
615. gds-db
616. ip-messenger
617. bacnet
618. cooltalk
619. ilohamail
620. 100bao
621. yy-voice-games
622. acronis-snapdeploy
623. groupwise
624. innovative
625. xfire
626. fc2-blog-posting
627. filemail
628. steekr
629. unreal
630. emc-documentum-webtop
631. mcafee-epo-admin
632. live-mesh-sync
633. winamax
634. sosbackup
635. seeqpod
636. ariel
637. mail.ru-moimir
638. fogbugz
639. paradise-paintball
640. mail.ru-webagent
641. koolim
642. live-mesh-remote-desktop
643. tokbox
644. packetix-vpn
645. bomberclone
646. ms-ocs
647. zoho-show
648. adobe-online-office
649. nateon-audio-video
650. mikogo
651. mekusharim
652. mail.com
653. fotoweb
654. igmp
655. iscsi
656. daum-cafe-posting
657. naver-blog-posting
658. secure-access
659. endnote
660. thinkfree
661. your-freedom
662. netop-remote-control
663. usermin
664. icq2go
665. proxeasy
666. pullbbang-video
667. pna
668. pim
669. sina-weibo-posting
670. viber
671. zoho-crm
672. party-poker
673. apc-powerchute
674. nateon-desktop-sharing
675. keyholetv
676. odnoklassniki-apps
677. yahoo-finance-posting
678. big-brother
679. adnstream
680. tagoo
681. naver-ndrive
682. doof
683. ibm-websphere-mq
684. rlogin
685. flexnet-publisher
686. cvsup
687. hp-data-protector
688. turboupload
689. imhaha
690. yuuguu
691. icap
692. zoho-notebook
693. hopopt
694. vsee
695. dcinside-posting
696. verizon-wsync
697. ovation
698. swapper
699. dimdim
700. writeboard
701. ammyy-admin
702. telenet-webmail
703. korea-webmail
704. outblaze-mail
705. ifolder
706. peerguardian
707. iccp
708. glide
709. ameba-now-posting
710. zoho-mail
711. gigaup
712. mercurial
713. avaya-phone-ping
714. diodeo
715. dabbledb
716. totodisk
717. ali-wangwang-file-transfer
718. webconnect
719. crossloop
720. pownce
721. google-docs-uploading
722. meabox
723. ironmountain-connected
724. 2ch-posting
725. xm-radio
726. drda
727. hyves-music
728. lotus-notes-admin
729. ms-ocs-file-transfer
730. fetion-file-transfer
731. bigupload
732. hovrs
733. wccp
734. etherip
735. graboid-video
736. seven-email
737. gbridge
738. meebo-file-transfer
739. sugar-crm
740. vagaa
741. apple-location-service
742. ms-scheduler
743. tvants
744. cddb
745. ibackup
746. sharebase.to
747. synergy
748. x-font-server
749. zenbe
750. turboshare
751. fasp
752. eatlime
753. ypserv
754. trinoo
755. usejump
756. http-tunnel
757. yahoo-blog-posting
758. egloos-blog-posting
759. wikidot-editing
760. siebel-crm
761. sina-uc-file-transfer
762. hl7
763. blin
764. igp
765. asterisk-iax
766. bebo-mail
767. war-rock
768. ibm-clearcase
769. arcserve
770. baidu-hi
771. ventrilo
772. aruba-papi
773. ip-in-ip
774. zelune
775. daap
776. filemaker-anouncement
777. mobility-xe
778. fileguri
779. bonpoo
780. baidu-hi-games
781. magister
782. reserved
783. wlccp
784. zoho-planner
785. camo-proxy
786. megaproxy
787. gizmo
788. tistory-blog-posting
789. realtunnel
790. ms-virtualserver
791. jap
792. mgcp
793. steganos-vpn
794. yugma
795. zabbix
796. mcafee
797. ipsec-ah
798. share-p2p
799. baidu-hi-file-transfer
800. msn2go
801. laconica
802. zoho-meeting
803. kryptolan
804. chaos
805. altiris
806. wetpaint-editing
807. secure-access-sync
808. warez-p2p
809. esignal
810. eroom-host
811. vyew
812. emcon
813. netbotz
814. modbus-read-holding-registers
815. meevee
816. yoics
817. egp
818. badoo
819. vidsoft
820. noteworthy
821. filer.cx
822. little-fighter
823. tradestation
824. ms-frs
825. caihong
826. ipcomp
827. modbus
828. dnp3
829. noteworthy-admin
830. rdmplus
831. perfect-dark
832. perforce
833. propalms
834. radiusim
835. webaim
836. eroom-net
837. argus
838. vmtp
839. r-exec
840. bgp
841. daum-blog-posting
842. bluecoat-auth-agent
843. knight-online
844. neptune
845. pharos
846. rediffbol
847. rwho
848. iso-ip
849. reliable-data
850. pup
851. pnni
852. exp
853. modbus-read-coils
854. zoho-share
855. suresome
856. surrogafier
857. idrp
858. isis
859. motleyfool-posting
860. callpilot
861. swipe
862. fluxiom
863. file-host
864. we-dancing-online
865. bluecoat-adn
866. rediffbol-audio-video
867. instan-t-webmessenger
868. spark-im
869. sctp
870. host
871. prm
872. sun-nd
873. cbt
874. xns-idp
875. hmp
876. bbn-rcc-mon
877. mux
878. emc-smartpackets
879. trendmicro-safesync
880. tacacs
881. ad-selfservice
882. tinyvpn
883. wixi
884. woofiles
885. ip-messenger-file-transfer
886. homepipe
887. foldershare
888. sharepoint-blog-posting
889. jxta
890. evalesco-sysorb
891. im-plus
892. oridus-nettouch
893. private-enc
894. mobile
895. rvd

896. fire
897. ipv6-frag
898. visa
899. merit-inp
900. vines
901. xnet
902. narp
903. track-it
904. clarizen
905. voddler
906. joost
907. dostupest
908. pcvisit
909. sina-uc-remote-control
910. techinline
911. unyte
912. dsr
913. tuenti
914. moinmoin-editing
915. tvtonic
916. maxdb
917. vnn
918. centriccrm
919. zoho-people
920. sugarsync
921. ants-p2p
922. fufox
923. aim-express-file-transfer
924. subspace
925. oracle-bi
926. dynamicintranet
927. distcc
928. iperf
929. daum-touch
930. airaim
931. ipv6-icmp
932. vrrp
933. nvp-ii
934. lan
935. qnx
936. 3pc
937. wb-expak
938. crtp
939. modbus-read-input-registers
940. spirent
941. nagios
942. modbus-write-multiple-registers
943. rusers
944. meeting-maker
945. socks2http
946. splashtop-remote
947. fastviewer
948. idpr-cmtp
949. fetion-audio-video
950. aim-audio
951. sip-application
952. ruckus
953. remobo
954. firephoenix
955. nakido-flag
956. sina-uc
957. netop-on-demand
958. gopher
959. tlsp
960. iplt
961. activenet
962. larp
963. sscopmce
964. dccp
965. mobilehdr
966. dcn-meas
967. rstatd
968. gnu-httptunnel
969. skydur
970. desktoptwo
971. rypple
972. schmedley
973. yosemite-backup
974. aim-video
975. simplify
976. zoho-db
977. kaixin-mail
978. ssh-tunnel
979. wallcooler-vpn
980. dclink
981. lawson-m3
982. stealthnet
983. gridftp
984. dropboks
985. filecatalyst-direct
986. wuala
987. gmail-drive
988. clickview
989. rmi-iiop
990. carefx
991. google-lively
992. kaixin-chat
993. octopz
994. srp
995. sprite-rpc
996. netblt
997. aris
998. secure-vmtp
999. sm
1000. pgm
1001. leaf-1
1002. uti
1003. i-nlsp
1004. ttp
1005. encap
1006. irtp
1007. trunk-1
1008. ipx-in-ip
1009. st
1010. iso-tp4
1011. smp
1012. dfs
1013. bna
1014. ipip
1015. mfe-nsp
1016. dgp
1017. xtp
1018. mtp
1019. crudp
1020. ggp
1021. sat-expak
1022. nsfnet-igp
1023. netware-remote-console
1024. loglogic
1025. estos-procall
1026. peercast
1027. gyao
1028. pingfu
1029. circumventor
1030. fly-proxy
1031. avoidr
1032. bypassthat
1033. webex-desktop-sharing
1034. orsiso
1035. ali-wangwang-audio-video
1036. sharepoint-wiki
1037. socialtext-editing
1038. msn-money-posting
1039. backpack-editing
1040. zwiki-editing
1041. ragingbull-posting
1042. howardforums-posting