The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

5th Edition, Spring 2010

Palo Alto Networks
232 E. Java Dr.
Sunnyvale, CA 94089
408.738.7700
www.paloaltonetworks.com

Table of Contents

Executive Summary

The *Application Usage and Risk Report (5th Edition, Spring 2010)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing application traffic assessments conducted between September 2009 and March of 2010. This edition of the report shows that application usage from both a geographic and a vertical industry perspective is remarkably consistent. Globally, the barriers to accessing an application are minimal, enabling rapid worldwide adoption, regardless of where the application was developed. Viewed within select vertical industries, the adoption rate remains consistent, yet the levels of business and security risks vary greatly, depending on the industry.

Key findings include:

Application use of all types is consistent, irrespective of geography or industry, yet the level of risk varies based on the specific industry.

- Viewed from an overall, geographical, or vertical industry perspective the data shows that applications of all types, both business and personal, are being used with remarkable consistency.
- Application usage is amazingly consistent between financial and healthcare networks and universities or other more traditionally open networks, but the risks are much greater in many cases.

Intensity of Enterprise 2.0 application usage continues to increase.

- Enterprise 2.0 applications are being used at very high levels across all organizations. Overshadowing the frequency of usage is the increased intensity of usage, measured by bandwidth consumed on a per organization basis. Categorically, social networking and collaborative applications showed steady upward growth in terms of bandwidth consumed per organization, strengthening the theory that these applications are quickly integrating into the mainstream of enterprise applications.
- All of the 22 Google applications identified by Palo Alto Networks show consistent usage in terms of frequency. Usage of both Google Docs and Google Calendar showed increased intensity in terms of session and bandwidth consumption.

Applications are not always what they seem to be.

- Almost two-thirds of the applications found (65%) can hop from port to port, use port 80, or port 443. The real surprise within this data point is the fact that 190 of these applications are either client-server or peer-to-peer based, a fact that dispels the assertion that port 80/443 equals browser-based traffic.
- Applications that can tunnel other applications, for good or bad, expand far beyond SSH, SSL, and VPN (IPSec or SSL) applications. There are 177 applications that are capable of tunneling other applications. Many of these applications do so unintentionally, by using port 80 as a means of enhancing accessibility. Examples include software updates, instant messaging and webmail - all of these use port 80 or 443 but are not considered web browsing. Other applications, such as UltraSurf, TOR, Gpass and Gbridge tunnel as a means of hiding the real nature of the application activity.

Introduction

The inaugural version of the Palo Alto Networks Application Usage and Risk Report (1st Edition, Spring 2008) was published with a sample size that was more than 20 organizations that were located solely in the United States. At that time, Palo Alto Networks identified more than 550 applications, of which more than 150 were found on the participating 20+ networks.

The latest edition of the Application Usage and Risk Report (Spring 2010) covers a sample size that has grown more than 15 fold to 347 and is truly global (Figure 1). Since the Spring 2008 Report, the number of applications Palo Alto Networks identifies has grown to nearly 1,000 with nearly 750 of them found during the six month period analyzed in this report (September 2009 to March 2010).

The larger sample size not only provides a global view, it also enables the analysis of application usage patterns within specific vertical industries such as financial services, healthcare, and higher education (universities). The data highlights the rapid dissolution of barriers to application access which makes rapid and widespread application adoption very easy, as evidenced by the fact that applications of all types are being used with remarkable consistency – regardless of the sample size, geography, or vertical industry. Consistency is a double edged sword – on one hand it shows a certain level of predictability, while on the other hand, it introduces very different levels of business and security risk, in different organizations.

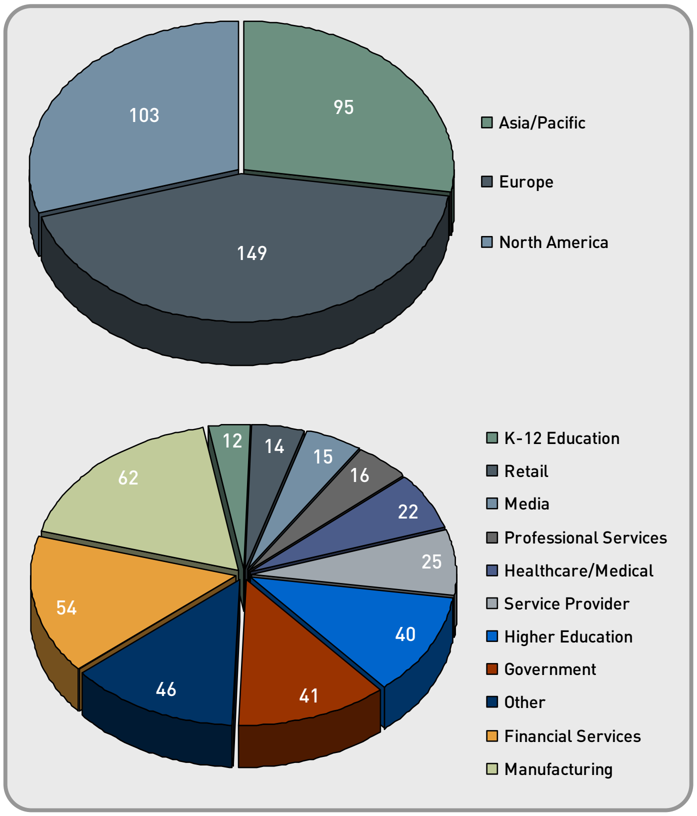

Figure 1: Geographic and industry breakdown of participating organizations.

Application Usage Is Consistent

At the risk of stating the obvious, applications of all types are being used in a very consistent pattern. Figure 2 displays a geographical view of the frequency[1] that the application category or an individual application was detected. The high level of consistency demonstrates that no one geography is different than another in terms of application usage.

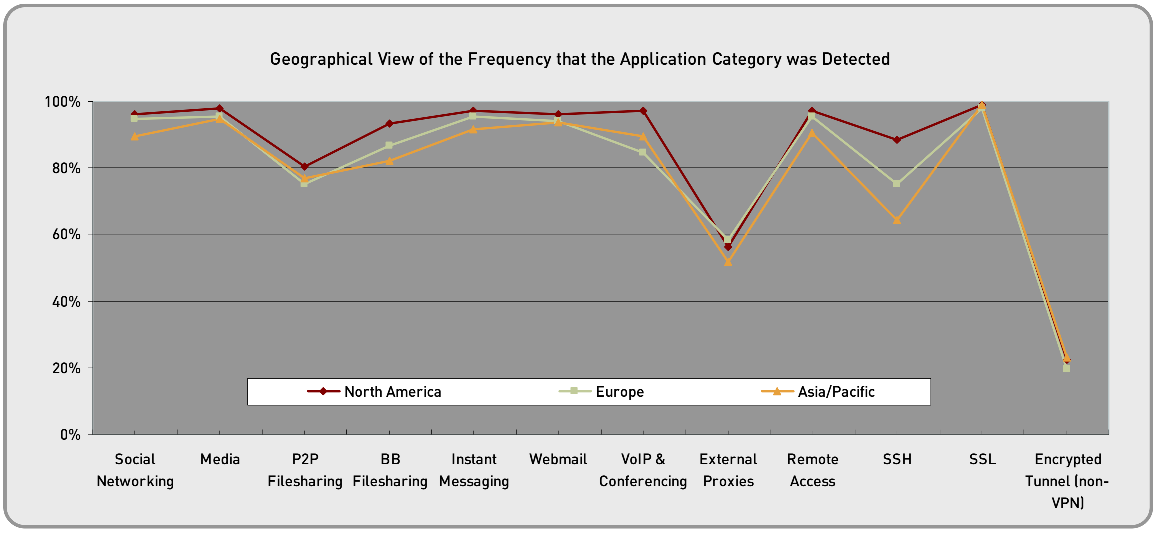

Figure 2: Geographic view of the frequency that applications were found within participating organizations.

Figure 2 shows that webmail, instant messaging, social networking and file sharing are all being used with equal consistency. The most significant difference is in the use of SSH. Interestingly, the use of technologies that enable a user to avoid detection appear with equal consistency. External proxies (CGI Proxy, KProxy, etc.) are found worldwide, as are encrypted tunneling applications such as TOR, UltraSurf, Hamachi, Gbridge, and Gpass. A view of the applications found (figure 3) within each of the different regions (by category) shows that there is significant overlap (and consistency) in both a total number of applications and within each of the different five main categories.

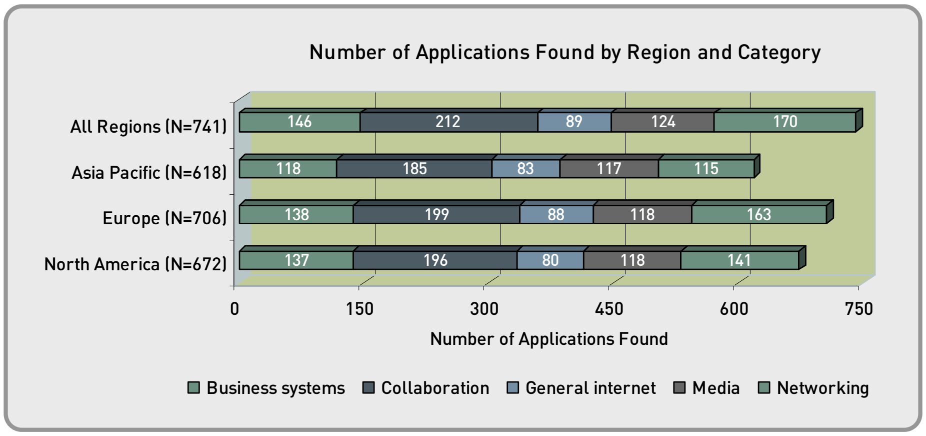

Figure 3: Categorical breakdown of all applications found regionally.

[1] Note that the frequency is based on a given application appearing at least once on the given network – the number of users, the number of applications within the category, and the number of times the application is used is not a factor in determining frequency.

The global view provides additional insight into individual applications that may be geographically specific. Examples include:

- Facebook, developed in the U.S., is the most popular social networking application in the world – included as an example and as a point of reference.
- BBC iPlayer, a European-based application is a browser-based streaming media player that uses port 80 or port 443 and is used worldwide.
- Skyplayer, also a European-based application is client-server media application that uses port 80 or port 443 and is popular worldwide.
- Hyves, the most popular social networking application in several Nordic countries, is accessed worldwide.
- Xunlei, a file sharing application that port hops and is the most popular P2P application in China, but is used consistently in North America and Europe.
- Spotify, shows the most significant regional use when compared to the other regions. Spotify is a client-server based, streaming audio application that is dynamic (hops ports).

Every one of these applications is being accessed in all geographies, indicating a certain level of universal appeal. BBCiPlayer, and Hyves, both of which are Euro-centric applications, were the only two that showed measurable differences from a geographic perspective. Figure 3 below highlights that the application landscape is global; its development location does not limit its geographic appeal.

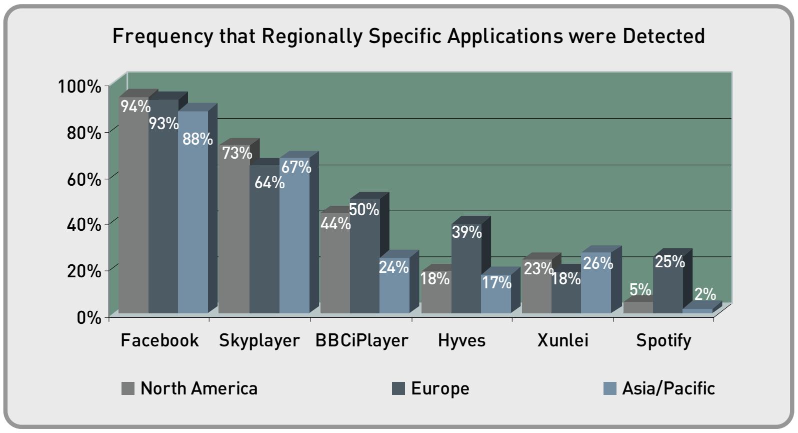

Figure 4: Frequency that geographically specific applications were found.

Homogeneous Use, Heterogeneous Risk—A Vertical View

Viewed from an industry specific perspective, consistent use of an application can introduce very different business and security risks. In a university, the use of social networking, instant messaging and webmail are almost a pre-requisite. In the financial services and healthcare industries, the use of the same set of applications can introduce business and network security risks such as non-compliance, data loss, and threat propagation.

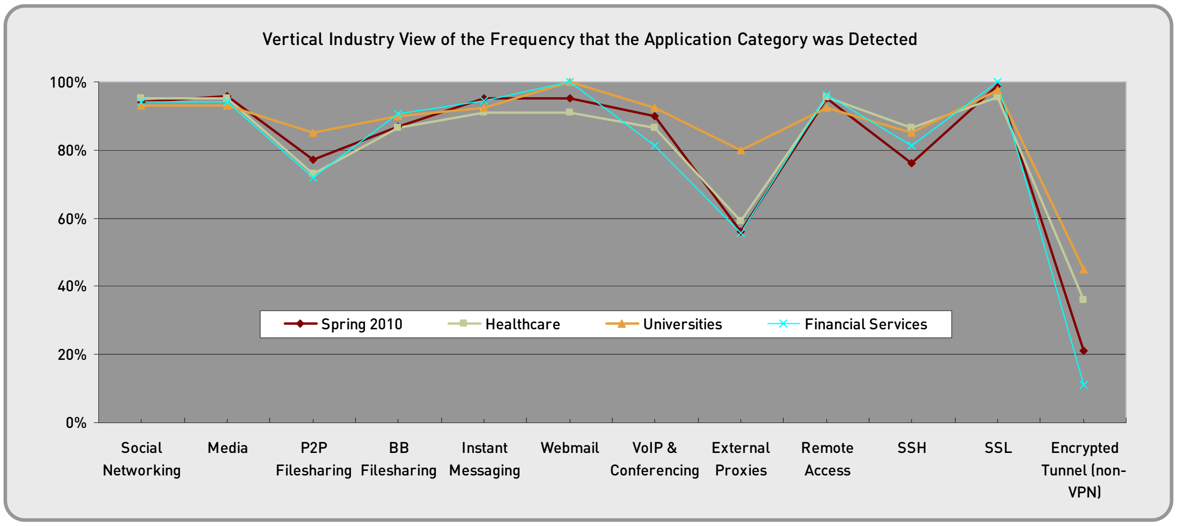

Figure 5: Frequency that applications were found within specific industries.

As a means of re-emphasizing the fact that application use of all types is consistent—even within specific industries, figure 5 shows the frequency with which the applications were detected within universities, financial services and healthcare industries. (The Spring 2010 view is included as a reference point). As shown earlier with the global view, the consistent frequency that the applications were used is supported by the overlap in the number of applications found, as shown in figure 6 below.

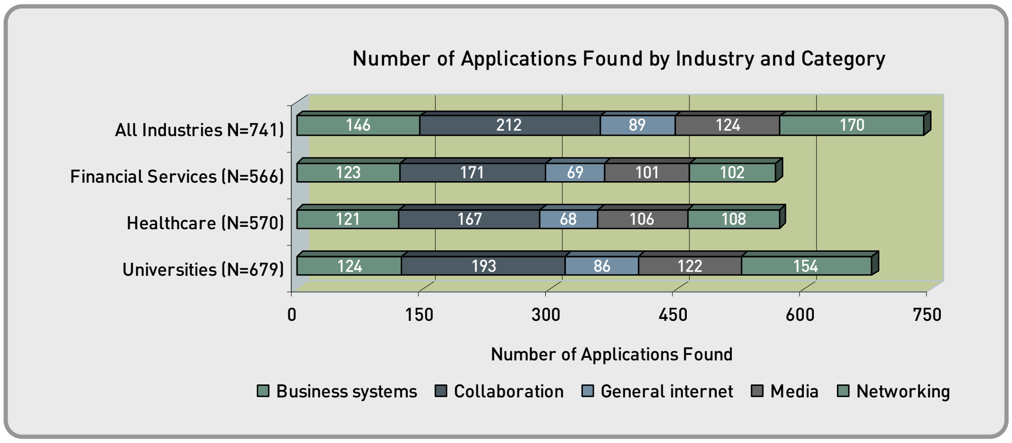

Figure 6: Categorical breakdown of all applications found within specific industries.

Financial Services and Healthcare Users Love to Socialize

In the financial services industry, regulations are in place to control and monitor the information flow across email and instant messaging applications as a means of protecting investors. A recent regulatory update published by the Financial Industry Regulatory Authority (FINRA 10-06) states that similar steps need to be taken with respect to social networking. In the healthcare industry, (PCI, HIPAA, N3, etc.)[2] are designed to protect patient data of all types (financial, personal, medical). The analysis of 54 financial services and 22 healthcare organizations around the world shows that the use of applications that can be viewed as violations of, or lead to violations of the associated rules and regulations were used with great frequency and intensity. Compliance and regulatory challenges aside, the use of these applications can introduce malware to the network through too much "socializing" or through more clandestine measures such as drive-by downloads.

- Instant messaging (IM) applications were detected in over 90% of the healthcare and financial services organizations, which is not surprising given the acceptance of IM as a business tool. The somewhat startling fact was the number of variants and the bandwidth consumed.

Use of Instant Messaging	All Industries	Financial Services	Healthcare
Frequency detected	95%	94%	95%
Total bandwidth consumed	2 TB	81 GB	71 GB
Total number of variants detected	62	51	46
Underlying technology	31 browser-based 25 client server 6 peer-to-peer	28 browser-based 18 client server 5 peer-to-peer	24 browser-based 18 client server 4 peer-to-peer
Average number of variants per organization	12	15	15
Top 5 most commonly detected	1. YahooIM 2. Facebook Chat 3. Gmail Chat 4. MSN 5. Meebo	1. YahooIM 2. Meebo 3. Gmail Chat 4. Facebook Chat 5. Google Talk Gadget	1. Gmail Chat 2. YahooIM 3. Google Talk Gadget 4. Facebook Chat 5. MSN

Within the top 5 IM applications found in healthcare and financial services organizations, two are client-server applications; MSN and Yahoo! Instant Messenger (distinct from Yahoo! Webmessenger which is identified as a different application), with the others using the browser as the underlying technology. Google Talk Gadget, one of the top 5 IM applications, uses a Flash-based plugin within the browser to perform the same functions as the client-server based Google Talk. The challenge that IM applications present to financial services and healthcare environments is that many of the IM applications use the browser (and either port 80 or port 443), making the traffic appear to be web traffic, which in turn means that any control or monitoring requirements become more difficult.

- Social networking: Overall, a mix of 35 different social networking applications were detected with at least one variant appearing in 94% of the participating organizations. Bandwidth consumed was nearly 3 terabytes (TB). Use of social networking within the healthcare and financial services industries was consistent with other industries, yet the implied business and security risks are quite different.

[2] Payment Card Industry Digital Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), N3 Network Security Initiative (N3)

Both industries manage significant amounts of private or confidential data and the use of social networking applications makes protecting that data even more challenging for two reasons. First, the traffic is flowing through port 80 or port 443 so it appears as web traffic. Second, the use of social networking at work is an assumed right—so reigning in the use as a means of protecting data may introduce employee dissatisfaction. Or worse yet, employees may find a way around the control mechanisms.

Use of Social Networking	All Industries	Financial Services	Healthcare
Frequency detected	94%	94%	95%
Total bandwidth consumed	2.9 TB	99 GB	128 GB
Number of variants detected	35	26	31
Average number of variants per organization	14	15	11
Top 5 most commonly detected	1. Facebook 2. Twitter 3. Myspace 4. LinkedIn 5. Flixster	1. Facebook 2. LinkedIn 3. Twitter 4. Myspace 5. Friendfeed	1. Facebook 2. Twitter 3. Myspace 4. LinkedIn 5. Imeem

- File sharing: In both the financial services and healthcare industries, P2P and browser-based file sharing applications are used with relatively high frequency. Across all industries, the frequency that browser-based file sharing applications are used exceeds that of P2P file sharing. While overall P2P bandwidth consumed is greater than that of browser-based, the industry specific view shows a different picture. In both financial services and healthcare industries, the bandwidth consumed by browser-based file sharing is greater than that of P2P.

Use of Peer-to-Peer File Sharing	All Industries	Financial Services	Healthcare
Frequency detected	77%	72%	73%
Total bandwidth consumed	46 TB	113 GB	67 GB
Number of variants detected	24	16	16
Average number of variants per organization	5	4	4
Top 5 most commonly detected	1. Bittorrent 2. Emule 3. Ares 4. Gnutella 5. Azureus	1. Bittorrent 6. Emule 7. Gnutella 8. Ares 9. Xunlei	1. Bittorrent 2. Emule 3. Gnutella 4. Ares 5. Imesh

Use of Browser-based File Sharing	All Industries	Financial Services	Healthcare
Frequency	87%	91%	86%
Total bandwidth consumed	11 TB	399 GB	143 GB
Number of variants detected	31	19	20
Average number of variants per organization	6	8	8
Top 5 most commonly detected	1. Skydrive 2. MegaUpload 3. Docstoc 4. Rapidshare 5. Mediafire	1. Skydrive 2. Docstoc 3. Megaupload 4. Filestube 5. Rapidshare	1. Skydrive 2. Mediafire 3. Filestube 4. Rapidshare 5. Megaupload

The high number of browser-based file sharing application variants and the bandwidth consumed supports the notion that browser-based applications have rapidly become a popular means of addressing three legitimate business needs; sending large files to an individual or small set of individuals (MegaUpload); finding and/or publishing business documents such as a legal form or rental agreement (DocStoc); or performing a hard drive or folder backup (xDrive). The one-to-one delivery nature of these applications minimizes the risk of inadvertent data loss/leakage, but does nothing to stop the purposeful movement of confidential data. Like IM and webmail, browser-based file sharing applications use port 80 or port 443, yet are clearly not web browsing—it is file transfer. In many cases, the use is for business purposes, making policy controls somewhat counterproductive.

In contrast, the most common use case (perceived or real) for P2P applications is the widespread sharing of audio, video and graphics materials. P2P applications are difficult to detect and control because they use common evasion tactics including non-standard ports, port hopping, and proprietary encryption. The broadcast nature of P2P applications and the difficulty in configuration makes the risk of inadvertent data leakage fairly high (as evidenced by many highly publicized data disclosures), particularly when compared to browser-based file sharing.

- Webmail: Out of the 41 different email applications found, 26 browser-based variants were found in both financial services and healthcare industries. This subset of applications is most commonly used for personal email (Outlook Web Access was excluded), yet the bandwidth consumed was 152 GB. Widespread use of webmail represents a combination of business (compliance, data leakage productivity) and security risks (malware propagation) for both the healthcare and financial services industries.

Use of Webmail	All Industries	Financial Services	Healthcare
Frequency detected	95%	93%	95%
Total bandwidth consumed	2 TB	152 GB	220 GB
Total number of variants detected	32	26	26
Average number of variants per organization	15	11	15
Top 5 most commonly detected	1. Gmail 2. Hotmail 3. Yahoo Mail 4. Facebook Mail 5. AOL Mail	1. Gmail 2. Yahoo Mail 3. Hotmail 4. Facebook Mail 5. AOL Mail	1. Yahoo Mail 2. Gmail 3. Hotmail 4. AOL mail 5. Squirrelmail

University Users are Masking Their Activity

University networks are often viewed as “open”, indirectly encouraging the use of any application. Therefore, it is not surprising that file sharing, media, and social networking application usage was higher than average in all aspects. Across the 40 participating universities, the higher than average use of external proxies and encrypted tunneling applications was surprising, given the (perhaps erroneously) assumed nature of university networks.

- Proxies: The frequency with which external proxies (those not supported or endorsed by the IT department) were found within universities was significantly higher (80% vs 56%) than that of other industries overall. The higher than average usage indicates that students and employees are taking an extra step to hide their web surfing activity.

Use of External Proxies	All Industries	Universities
Frequency detected	56%	80%
Bandwidth consumed	59 GB	14 GB
Number of variants detected	21	20
Average number of variants per organization	4	6
Top 5 most commonly detected	1. CGIProxy 2. PPHProxy 3. CoralCDN 4. Freegate 5. Glype Proxy	1. CGIProxy 2. PPHProxy 3. CoralCDN 4. Glype Proxy 5. Freegate

- Encrypted Tunneling (Non-VPN Related) Applications: The frequency with which non-VPN tunneling applications were found on university networks was more than double that of other industries. This group of applications is defined as those that are not used for site-to-site (IPSec) or remote access (SSL) VPN connectivity. (Note that SSL and SSH proper are also excluded from this list/discussion). This is an admittedly small subset of applications (total of 9) whose primary purpose is to maintain anonymity and mask activity through an encrypted tunnel.

Use of Encrypted Tunneling Applications	All Industries	Universities
Frequency	21%	45%
Bandwidth consumed	18 GB	12 GB
Total number of variants detected	9	7
Top 3 most commonly detected	1. TOR 2. Hamachi 3. Gbridge	1. TOR 2. Hamachi 3. Gbridge

When these two groups of applications are viewed collectively, they pose a question as to why the students (and university employees) might feel compelled to take the somewhat extraordinary steps to mask their activity and/or maintain anonymity. Two reasons for this come to mind. Either they are using it to bypass security controls and policies that are in place to control applications such as P2P or they are extremely concerned about their personal privacy. If so, then why are they using social networking (34 different applications variants found consuming nearly 2 TB of data bandwidth)? Whatever the reason, their use makes protecting the network more difficult because the traffic, including possibly malicious payload, may be bypassing existing security controls.

Enterprise 2.0: Usage Is Consistent But Intensity Has Increased

With respect to those applications that are considered to be Enterprise 2.0, the level of consistency from both a historical and geographical perspective masks a more important trend which is the increased intensity of usage that is calculated on the bandwidth consumed on a per organization basis.

Looking back at the 2nd Edition of the Application Usage and Risk Report (Fall 2008), there were 12 social networking applications detected with at least one of them being detected in 95% of the participating organizations (N=60). To put it another way, the applications are used everywhere. On average, there were four variants detected and each organization consumed an average of 3.9 GB. Google applications were found with relatively high frequency but their resource consumption was low, indicating low intensity usage. The Spring 2010 version of the report shows that the number of unique social networking applications has increased to 36 and at least one of them was detected in 94% of the participating organizations (N=347). The average number of variants within each organization has increased slightly to 6 while the bandwidth consumed per organization doubled to 9 GB (figure 7).

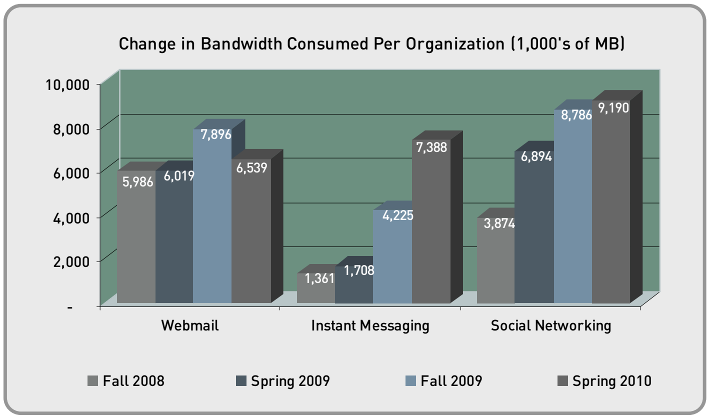

Figure 7: Change in bandwidth consumed by webmail, instant messaging and social networking applications.

Figure 7 highlights, at a categorical view, that social networking and instant messaging show regular increases in bandwidth consumed per organization while webmail (those email applications that are most likely to be used for personal purposes), is relatively flat. As a testimony to the ever-changing usage patterns from both a geographical and vertical industry perspective, figure 6 below shows the changes in bandwidth consumption per organization for a select group of popular applications. Sharepoint continues to show a steady adoption rate in terms of frequency of use and bandwidth consumed (per organization).

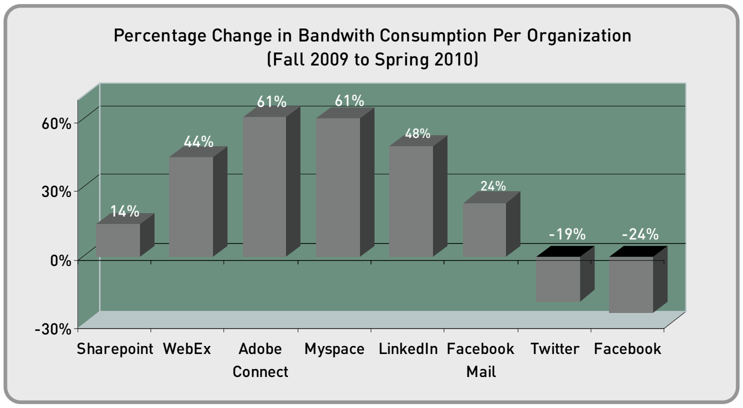

Figure 8: Percentage change in bandwidth consumption for select enterprise 2.0 applications (per organization).

Two applications that showed extreme growth rates in the Application Usage and Risk Report (Fall 2009), returned to more reasonable consumption rates, although Facebook was still shown to be consuming 4.9 GB of data per organization, a rate that is down from the previous report, yet still relatively high in terms of usage intensity.

Google Applications: The Epitome of Enterprise 2.0?

To a certain extent, many of the applications that Google publishes epitomize Enterprise 2.0 – Web 2.0 and internet-based applications that are used for business purposes. Palo Alto Networks identifies 22 Google applications that cover a wide functionality spectrum: productivity (Google Docs, Analytics, Calendar), social networking (Orkut), communications (Gmail, Gtalk, Voice) and entertainment (YouTube, Picasa). To highlight the speed with which Google applications are being used, the recently released Google Wave was found in 10% (~35) of the participating organizations.

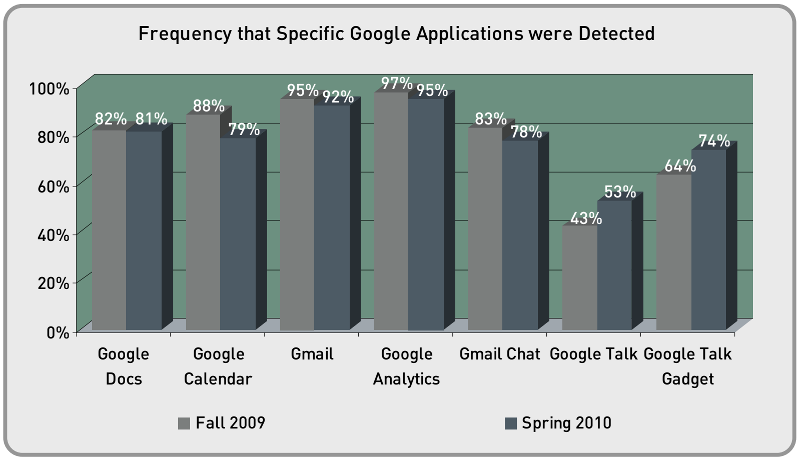

Figure 9: Frequency that select Google applications (productivity, analysis, communications) were found in participating organizations.

When compared to the Application Usage and Risk report (Fall 2009), two of the Google applications that fully support our assertion that Enterprise 2.0 showed increased usage.

- Resource consumption (bandwidth and sessions) per organization for Google Docs increased 55% and 42% respectively.
- Similarly, Google Calendar consumed 18% and 30% more bandwidth and sessions on a per organization basis.
- Bandwidth consumption for Google Talk Gadget shot up by 56% while Google Talk dropped 76%. Google Talk Gadget is a Flash-based browser plugin that performs the same functions as the client server-based Google Talk. The most significant difference is the fact that it is browser-based, and therefore is easier to use in environments where desktop controls limit application installation by end-users.

Applications Are Not Always What They Seem to Be

The Spring 2009 Application Usage and Risk Report introduced the analysis of applications that use port 80, port 443, or port hop as a feature in order to improve accessibility. To the application developer, accessibility makes the application easier to use, thereby increasing usage while decreasing user issues. For the end-user, it means the application can be used from anywhere, at anytime. Out of the 741 unique applications found in this analysis, 65% (479) were designed for accessibility.

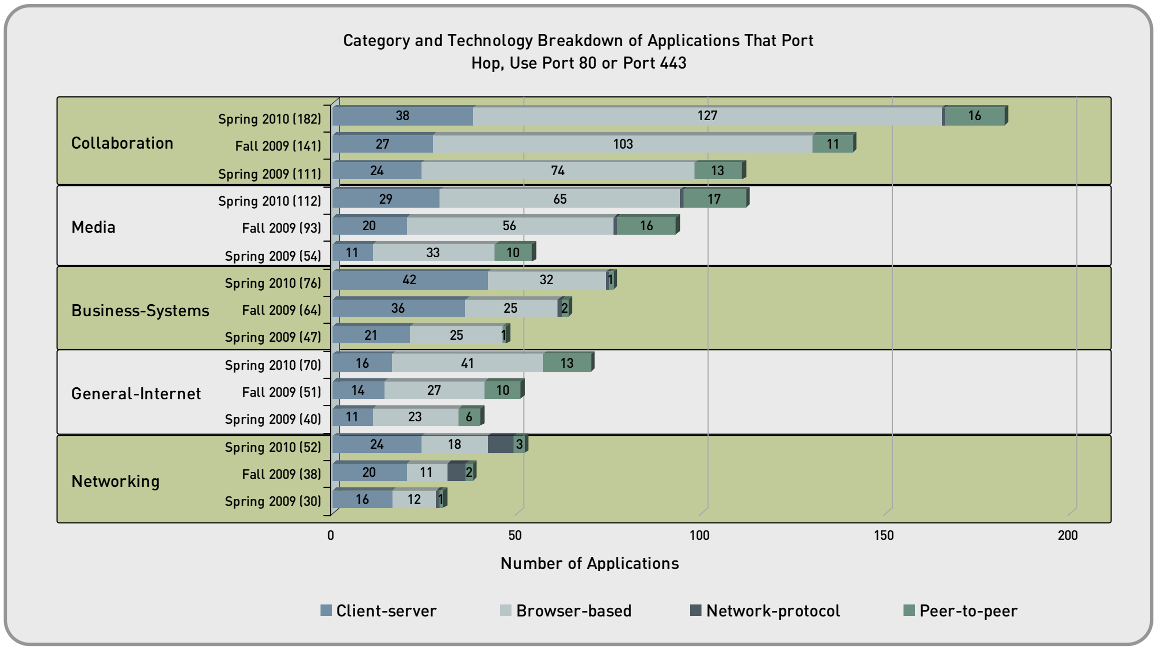

Figure 10: Comparative growth of applications with accessibility features.

The real surprise within this data point is the fact that 30% (149) of these applications are client-server based, a fact that contradicts the notion that "accessible" applications always use the browser.

A slightly different view of the applications with accessibility features shows that there are 105 applications (22%) that are capable of port hopping. Some, like RPC and Sharepoint do so because it is critical to how the application or protocol functions; it is not port hopping as a means of evading detection or enhancing accessibility. All the other applications listed will hop ports to improve accessibility and in so doing, evade detection.

Emphasizing the fact that applications are not what they seem to be, the most commonly found applications that can port-hop are a combination of business and personal use applications and only three are browser-based (Sharepoint, Mediafire, and Ooyla. The others are peer-to-peer or client-server.

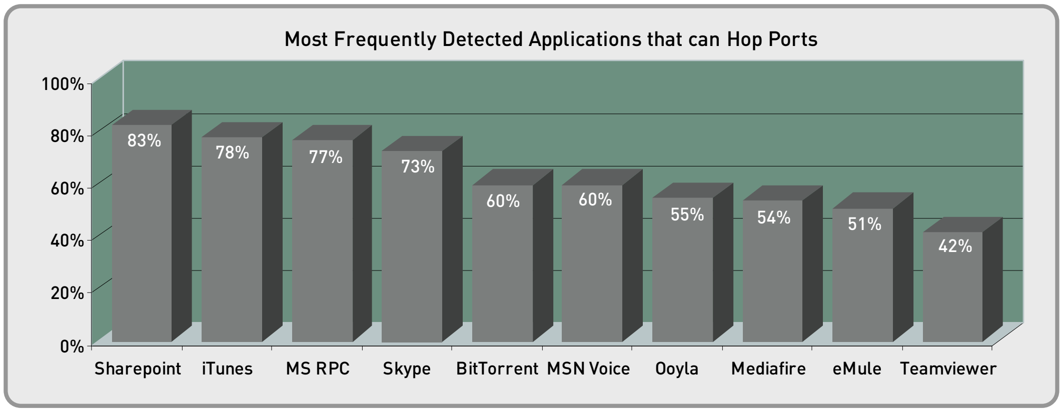

Figure 11: Most commonly detected applications that can hop ports.

The fact that these applications, all of which are commonly used for business purposes, are capable of hopping ports re-emphasizes the fact that the application landscape has evolved dramatically.

Tunneling—an Accessibility Feature or an Evasive Tactic?

Applications that can tunnel other applications, for good or bad, expand far beyond the traditional view of SSH, SSL and VPN (IPSec or SSL) related applications. Within this subset of applications (479), there are 177 applications that are capable of tunneling other applications. The most obvious example of this type of application is web browsing. Many years ago the antivirus vendors began using port 80 to update their pattern engines quickly and easily. To most security infrastructure components, this traffic appears as if it is web browsing.

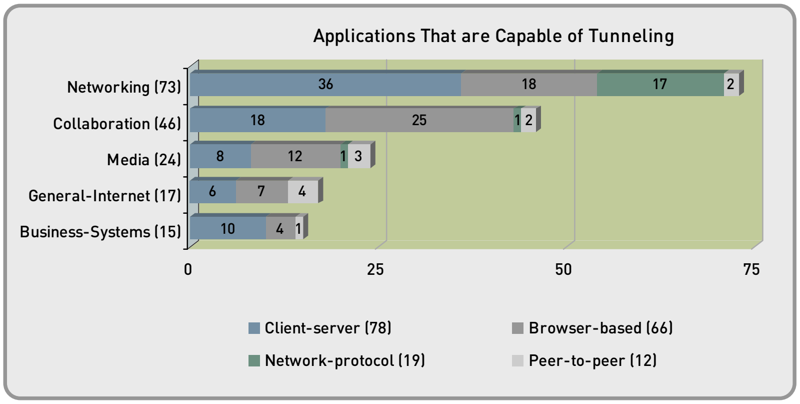

Figure 10: Breakdown of applications (category and underlying technology) that can tunnel.

Within the applications that use tunneling, many of them are a bit more clandestine, using encryption, non-standard ports and port hopping as a means of masking their activity. Examples include several P2P applications (Kazaa, Gnutella, Ares), media applications (Xbox Live, iTunes), and well known networking services such as MS-RPC and SMB.

Outside of traditional IPSec and SSL VPN applications, are those applications that use encryption (not SSL or SSH) and include TOR, UltraSurf, Gpass, and Gbridge, all of which provide tunnels as a means of hiding the real nature of the application activity.

Summary

In one respect, consistency can be quite boring, after all, how interesting can seeing the same thing day in and day out be, particularly when it is about application usage? The consistent use of all types of applications across different geographies is compelling because it means that the "we're different" statement made by various communities is becoming less and less relevant. Ubiquitous web connectivity and application development technology have nearly eliminated the barriers to application access that existed previously. If the application is "hot" then it will garner worldwide acceptance. From an industry-specific view, homogeneous use has heterogeneous risks, which, to the administrator, represents significant challenges. The network security team is challenged to help enable the applications use (and the business) while addressing security and business risks that the use may introduce.

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 10Gbps 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. 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. 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 10 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 than 950 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 741 unique applications found, ranked in terms of frequency are listed below. To view details on the entire list of 950+ applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications at http://ww2.paloaltonetworks.com/applipedia/

100% Frequency

1. ssl
2. dns
3. web-browsing
4. netbios-ns
5. ntp
6. ms-update
7. flash
8. google-analytics
9. youtube
10. icmp
11. webdav
12. rss
13. ping
14. soap
15. http-proxy
16. smtp
17. gmail
18. facebook
19. google-video
20. snmp
21. google-safebrowsing
22. photobucket
23. http-audio
24. hotmail
25. yahoo-mail
26. flickr
27. http-video
28. ftp
29. twitter
30. google-toolbar
31. rtmpt
32. netbios-dg
33. adobe-update
34. limelight
35. myspace
36. sharepoint
37. silverlight
38. yahoo-im
39. ms-ds-smb
40. linkedin
41. google-docs
42. atom
43. ldap
44. ms-rdp
45. facebook-chat
46. apple-update
47. google-calendar
48. dailymotion
49. gmail-chat
50. asf-streaming
51. itunes
52. msrpc
53. flexnet-installanywhere
54. ssh
55. google-picasa
56. google-app-engine

75% Frequency

57. msn
58. meebo
59. yahoo-toolbar
60. google-desktop
61. google-talk-gadget
62. skydrive
63. rtmp
64. netbios-ss
65. skype
66. office-live
67. kerberos
68. symantec-av-update
69. dhcp
70. sky-player
71. yahoo-webmessenger
72. myspace-video
73. facebook-mail
74. metacafe
75. mssql-mon
76. skype-probe
77. google-earth
78. hulu
79. ms-netlogon
80. babylon
81. salesforce
82. pop3
83. active-directory
84. last.fm
85. flixster
86. telnet
87. aim-mail
88. seesmic
89. msn-voice
90. bittorrent
91. megaupload
92. imeem
93. mssql-db
94. napster
95. webshots
96. friendfeed
97. facebook-apps
98. stun
99. mobile-me
100. web-crawler
101. ike
102. ipsec-esp-udp
103. yourminis
104. docstoc
105. orkut
106. rapidshare
107. stumbleupon
108. t.120
109. megavideo
110. plaxo
111. syslog
112. msn-file-transfer
113. citrix
114. ooyala
115. squirrelmail
116. outlook-web
117. shoutcast
118. twitpic
119. spark
120. mediafire
121. logmein
122. aim-express
123. google-talk
124. vbulletin-posting
125. ustream
126. rtmpe
127. filestube
128. msn-toolbar
129. emule
130. yousendit

50% Frequency

131. rtsp
132. livejournal
133. friendster
134. slp
135. ms-sms
136. 4shared
137. reuters-data-service
138. nintendo-wfc
139. blackboard
140. horde
141. lotus-notes
142. hp-jetdirect
143. ebuddy
144. time
145. webex
146. ms-exchange
147. backweb
148. snmp-trap
149. rtp
150. citrix-jedi
151. sharepoint-admin
152. blogger-blog-posting
153. teamviewer
154. justin.tv
155. sip
156. bbc-iplayer
157. imap
158. myspace-mail
159. hi5
160. oracle
161. clearspace
162. vnc
163. ssdp
164. radius
165. teredo
166. gotomeeting
167. ares
168. roundcube
169. myspace-im
170. tftp
171. gnutella
172. dropbox
173. mogulus
174. rtcp
175. live365
176. esnips
177. meebome

178. yahoo-voice
179. iheartradio
180. blog-posting
181. fotki
182. xobni
183. boxnet
184. sharepoint-documents
185. depositfiles
186. qvod
187. aim
188. zango
189. twig
190. zimbra
191. lpd
192. playstation-network
193. ciscovpn
194. bebo
195. jabber
196. tudou
197. rdt
198. msn-webmessenger
199. grooveshark
200. logitech-webcam
201. xing
202. pandora
203. cgiproxy
204. norton-av-broadcast
205. portmapper
206. open-vpn
207. phproxy
208. worldofwarcraft
209. jango
210. shutterfly
211. trendmicro
212. yum
213. sendspace
214. deezer
215. coralcdn-user
216. ipv6
217. adobe-connect
218. blackberry
219. pogo
220. hyves
221. stickam
222. youku
223. bugzilla
224. mysql

25% Frequency

225. iloveim
226. computrace
227. steam
228. gre
229. qq
230. sightspeed
231. upnp
232. azureus
233. irc
234. evony
235. mail.ru
236. veohtv
237. yandex-mail
238. rhapsody
239. imvu
240. second-life
241. netvmg-traceroute
242. echo
243. twitter-posting
244. ppstream
245. secureserver-mail
246. tvu
247. yahoo-douga
248. evernote
249. xunlei
250. qq-mail
251. kaspersky
252. classmates
253. ms-groove
254. netsuite
255. tidaltv
256. live-meeting
257. mediawiki-editing
258. mms
259. pando
260. mail.com
261. h.323
262. pptp
263. daytime
264. msn-video
265. socialtv
266. ipsec-esp
267. outblaze-mail
268. pandora-tv
269. pcanywhere
270. subversion
271. drop.io
272. icq
273. gmx-mail
274. vmware
275. h.225
276. h.245
277. imesh
278. gotomypc
279. imo
280. netspoke
281. rpc
282. blin
283. move-networks
284. tor
285. freegate
286. yahoo-file-transfer
287. jira
288. tacacs-plus
289. 2ch
290. ipp
291. messengerfx
292. pplive
293. stagevu
294. rsvp
295. yourfilehost
296. oovoo
297. ichat-av
298. carbonite
299. babelgum
300. sharepoint-calendar
301. netease-mail
302. glype-proxy
303. sopcast
304. dealio-toolbar
305. netflow
306. neonet
307. diino
308. hamachi
309. web-de-mail
310. open-webmail
311. dotmac
312. libero-video
313. apple-airport
314. corba
315. qqlive
316. gadu-gadu
317. kazaa
318. files.to
319. spotify
320. socks
321. flumotion
322. jaspersoft
323. wins
324. lwapp
325. sybase
326. rip
327. l2tp
328. channel4
329. whois
330. activesync
331. autobahn
332. source-engine
333. ebay-desktop
334. wolfenstein
335. qq-download
336. tikiwiki-editing
337. mozy
338. mixi
339. filemaker-pro
340. octoshape
341. woome
342. kaixin
343. finger
344. sap
345. discard
346. nntp
347. medium-im
348. badongo
349. cisco-nac
350. orb
351. yahoo-webcam
352. nfs
353. vtunnel
354. kugoo
355. fastmail
356. symantec-syst-center
357. google-wave
358. rpc-over-http
359. qqmusic
360. gtalk-voice
361. camfrog
362. websense
363. sophos-update
364. timbuktu
365. concur
366. rsync
367. uusee
368. kontiki
369. garena
370. yammer
371. dameware-mini-remote
372. ultrasurf
373. userplane
374. eigrp
375. freeetv
376. zoho-sheet
377. alisoft
378. cups
379. winamp-remote
380. lokalisten
381. kaixin001
382. veetle
383. editgrid
384. ms-win-dns

385. cox-webmail
386. tagoo
387. sccp
388. backup-exec
389. xdmcp
390. feidian
391. secure-access
392. zoho-im
393. mibbit
394. direct-connect
395. streamaudio
396. hopster
397. niconico-douga
398. checkpoint-cpmi
399. mount
400. livelink
401. cvs
402. netmeeting
403. x11
404. cpq-wbem
405. t-online-mail
406. vnc-http
407. radmin
408. kproxy
409. zoho-writer
410. ms-iis
411. folding-at-home
412. lotus-sametime
413. aim-file-transfer
414. hotspot-shield
415. nate-mail
416. tivoli-storage-manager
417. zoho-show
418. ncp
419. genesys
420. battlefield2
421. mediamax
422. viadeo
423. netviewer
424. kino
425. webqq
426. gtalk-file-transfer
427. ms-wins
428. ms-scom
429. unassigned-ip-prot
430. icq2go
431. 100bao
432. verizon-wsync
433. send-to-phone
434. informix
435. yahoo-finance-posting
436. rping
437. ospfigp
438. xbox-live
439. filedropper
440. bebo-mail
441. xm-radio
442. seeqpod
443. rsh
444. elluminate
445. dimdim
446. instan-t-file-transfer
447. hangame
448. fs2you
449. netop-remote-control
450. zelune
451. sling
452. livestation
453. webex-weboffice
454. gamespy
455. cooltalk
456. magicjack
457. ndmp
458. miro
459. ms-scheduler
460. koolim
461. subspace
462. poker-stars
463. soulseek
464. zoho-wiki
465. ms-dtc
466. avaya-phone-ping
467. radiusim
468. gnunet
469. groupwise
470. wikispaces-editing
471. pim
472. palringo
473. cgi-irc
474. foxy
475. optimum-webmail
476. simplify
477. rlogin
478. ibm-director
479. git
480. manolito
481. ifile.it
482. nateon-im
483. laconica
484. iccp
485. live-mesh
486. mcafee
487. forticlient-update
488. kaixin001-mail
489. acronis-snapdeploy
490. scps
491. msn2go
492. meebo-file-transfer
493. tales-runner
494. flashget
495. clip2net
496. foldershare
497. eatlime
498. innovative
499. seven-email
500. gds-db
501. db2
502. tuenti
503. tvants
504. razor
505. pownce
506. ip-messenger
507. imhaha
508. peerguardian
509. ovation
510. inforeach
511. hushmail
512. wetpaint-editing
513. tokbox
514. vsee
515. igmp
516. cddb
517. mcafee-epo-admin
518. big-brother
519. wccp
520. trinoo
521. xfire
522. google-lively
523. eve-online
524. soribada
525. usermin
526. postgres
527. asterisk-iax
528. sosbackup
529. mcafee-update
530. igp
531. zoho-notebook
532. ms-ocs
533. ypserv
534. fortiguard-webfilter
535. bomberclone
536. adrive
537. taku-file-bin
538. comcast-webmail
539. kkbox
540. hp-data-protector
541. egp
542. glide
543. circumventor
544. jap
545. pna
546. graboid-video
547. noteworthy-admin
548. etherip
549. nateon-file-transfer
550. perforce
551. all-slots-casino
552. zoho-crm
553. sugar-crm
554. packetix-vpn
555. ilohamail
556. filemaker-anouncement
557. dabbledb
558. ventrilo
559. gizmo
560. ibackup
561. gogobox
562. idrp
563. crossloop
564. surrogafier
565. meabox
566. writeboard
567. ariel
568. wlccp
569. rvd
570. mobile
571. yuuguu
572. esignal
573. apc-powerchute
574. wiiconnect24
575. party-poker
576. doof
577. siebel-crm
578. ameba-blog-posting
579. mekusharim
580. clubbox
581. hopopt
582. http-tunnel
583. adnstream
584. joost
585. thinkfree
586. sun-nd
587. ipcomp
588. fire
589. g.ho.st
590. ms-ocs-file-transfer
591. swipe
592. gbridge

593. lotus-notes-admin
594. fc2-blog-posting
595. 2ch-posting
596. iscsi
597. r-exec
598. privax
599. earthcam
600. zoho-planner
601. ip-in-ip
602. zoho-meeting
603. nimbuzz
604. swapper
605. mercurial
606. war-rock
607. drda
608. yahoo-blog-posting
609. bgp
610. x-font-server
611. showmypc
612. proxeasy
613. megaproxy
614. netflix
615. track-it
616. rusers
617. rstatd
618. bacnet
619. vmtp
620. visa
621. srp
622. mpls-in-ip
623. iso-ip
624. hmp
625. exp
626. dcn-meas
627. chaos
628. br-sat-mon
629. yugma
630. jxta
631. youseemore
632. gmail-drive
633. tcp-over-dns
634. secure-access-sync
635. ipsec-ah
636. gpass
637. zoho-mail
638. zenbe
639. google-finance-posting
640. backpack-editing
641. nateon-audio-video
642. trendmicro-earthagent
643. sdrp
644. isis
645. idpr-cmtp
646. dsr
647. yoics
648. meevee
649. netbotz
650. clarizen
651. altiris
652. vrrp
653. uti
654. trunk-1
655. tlsp
656. st
657. reserved
658. ptp
659. prm
660. private-enc
661. pipe
662. nvp-ii
663. nsfnet-igp
664. mux
665. mfe-nsp
666. leaf-1
667. lan
668. iso-tp4
669. ipx-in-ip
670. ipv6-icmp
671. ipip
672. ggp
673. emcon
674. dccp
675. crudp
676. crtp
677. cpnx
678. compaq-peer
679. bna
680. argus
681. rediffbol
682. instan-t-webmessenger
683. ms-frs
684. dnp3
685. webconnect
686. share-p2p
687. wixi
688. gigaup
689. dropboks
690. firephoenix
691. noteworthy
692. wikidot-editing
693. sharepoint-wiki
694. howardforums-posting
695. emc-smartpackets
696. idpr
697. bypassthat
698. gyao
699. keyholetv
700. meeting-maker
701. campfire
702. rediffbol-audio-video
703. kaixin-chat
704. modbus
705. maplestory
706. blokus
707. generic-p2p
708. bigupload
709. fluxiom
710. daap
711. zwiki-editing
712. socialtext-editing
713. motleyfool-posting
714. ms-ocs-audio
715. aim-video
716. aim-audio
717. afp
718. schmedley
719. techinline
720. desktoptwo
721. dontcensorme
722. pingfu
723. zoho-share
724. netware-remote-console
725. gkrellm
726. nateon-desktop-sharing
727. yoono
728. hovrs
729. ibm-clearcase
730. distcc
731. unreal
732. ants-p2p
733. fasp
734. divshare
735. zoho-people
736. wallcooler-vpn
737. realtunnel
738. kaixin-mail
739. tacacs
740. bluecoat-auth-agent
741. tvtonic