The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

April 5, 2008

Palo Alto Networks
2130 Gold Street, Suite 200
Alviso, CA 95002-2130
Main 408.786.0001
Fax 408.786.0006
Sales 866.207.0077
www.paloaltonetworks.com

Table of Contents

Executive Summary

The Application Usage and Risk Report from Palo Alto Networks summarizes application traffic assessments for 20 large organizations across financial services, manufacturing, healthcare, government, retail and education over the last 6 months, and represents the behavior of over 350,000 users. The report confirms that CIO/CSOs face an application landscape that has evolved in dramatic fashion.

End users are actively circumventing IT control mechanisms

- External proxies, the kind IT does not support, such as CGIProxy and KProxy, were present in 80% of the customer networks.
- Encrypted tunneling applications such as TOR (The Onion Router) was found 15% of the time.
- Web-based file transfer and storage applications such as Megaupload, YouSendIt and MediaMax were detected in 30% of the sites.

Port 80 isn't what you think it is.

- Over 90% of the applications traversing port 80 are not "web browsing".
- Most applications (over 50%) using port 80 and not business related.
- Webmail was found in 95% of the cases while IM use was found in 100% of the cases.
- Google applications such as Google Docs and Google Desktop are in use in 60% of the sites.

Bandwidth hogging applications are more common than ever.

- Video over HTTP is consuming significant bandwidth in 100% of the sites.
- Streaming audio was present in 95% of the cases.
- Peer-to-peer file sharing applications were found in 90% of the sites assessed, indicating that enterprise control efforts are falling short.
- Applications such as TvAnts and UUSee that use P2P as the underlying video streaming technology was found in 25% of the sites.

There are two possible explanations for the high incidence of these applications. First, they are being used for legitimate business purposes, either sponsored by the enterprise or adopted independently by users for a variety of professional and/or recreational reasons.
The second, and more likely reason for the high use, is because end users enjoy the freedom to choose which applications they use and want to use them at home or work, regardless of acceptable use policies. End users enjoy this freedom because applications have been built to bypass traditional security and control mechanisms, leaving IT with minimal visibility and even less control.

The lack of visibility and control over applications makes it very difficult to manage risk coherently on enterprise networks. IT department's attempts to control the new class of applications achieve mixed results as users become smarter and more capable at getting around IT either in a purposeful manner through the use of proxies or circumventors, or by using applications that have evasive traits like port hopping, encryption or tunneling built in to the product as a feature. Compounding the lack of visibility and control are some application providers that encourage users to circumvent IT.

IT departments are not sitting on their hands. Nearly every customer engagement summarized in this report was focused on finding and controlling these applications. Many are actively engaging with business units to discuss the business' application needs and how to enable use and minimize security risks.

By providing customers with an Application Visibility and Risk Report, generated by deploying a Palo Alto Networks PA-4000 Series, customers are able to balance the business benefits of supporting a new generation of applications with the associated risks.

Introduction

Fifteen years ago, it was easy for firewalls to control application traffic because it could easily be classified based on specific ports and protocols, but not anymore. Today's applications, some that are good for business and many that are not, have found creative ways to bypass the firewall and other network-based controls. Enterprise networks are rife with rogue applications that masquerade themselves as legitimate traffic, hop ports or sneak through using encrypted SSL tunnels. Perfect examples of these applications are social networking, instant messaging, web mail, P2P and RSS, all of which are designed to bypass existing detection technologies. As a result, IT has lost application visibility at an important point in the network – the Internet gateway – resulting in increased business risks:

- Risk of data loss through unmonitored and/or unauthorized file transfer.
- Risk to compliance efforts, both with internal policies and external regulations, through the lack of visibility into application usage.
- Risk of operational cost increases from higher bandwidth consumption and added IT expenses
- Risk of lost user productivity from excessive personal application usage.
- Risk to business continuity – business application downtime brought on by propagation of malware and/or application vulnerability exploits.

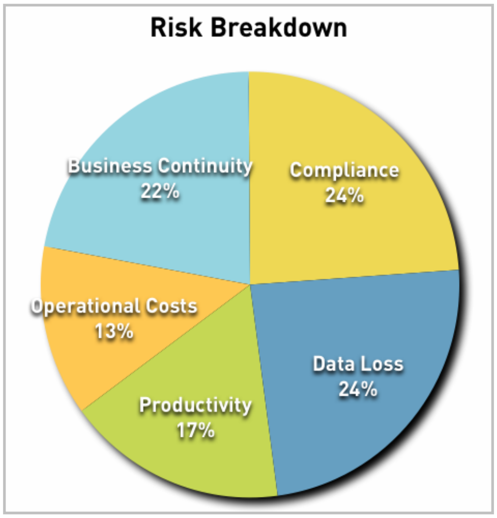

Figure 1: Business risk breakdown of all applications found on customer networks.

In the 20 most recent application visibility and risk assessments, Palo Alto Networks determined that the most prominent areas of business risk are business continuity, data leakage and compliance. As highlighted throughout this document, the application landscape is changing dramatically. Employees are using what ever application they want and bypassing IT controls, sometimes in a very purposeful manner. Other times, it is a built-in feature within the application that will bypass the firewall without the user knowing.

While the work-related value of some of the applications may be questionable, many employees, particularly recent entrants to the workforce, are demanding access to these applications, forcing a delicate balancing act between the IT department. An important conclusion is that the IT department can no longer afford to look strictly at the security risks in the traditional sense (e.g., business applications are low risk, non-business applications are high risk). Too many users are demanding access to a new generation of applications, driving IT toward the role of enabling employees to be more effective and in doing so, improving the bottom line.

Palo Alto Networks Application Visibility and Risk Report

The Palo Alto Networks Application Visibility and Risk assessment involves deploying a Palo Alto Networks PA-4000 Series firewall within the customer network, in either tap mode or virtual wire mode, where it monitors the application traffic traversing the Internet gateway. At the end of the data collection period, usually one to seven days, an Application Visibility and Risk Report (AVR Report) is generated that analyzes the application traffic by looking at the overall security risk rating, delving into the business risk assessment and providing a more accurate picture of how the network is being used. The report closes with a detailed look at how effective the existing technologies are at supporting and enforcing the customer application usage control policies.

Findings

In general, every organization that went through the Application Visibility and Risk Report process found some applications that did not belong on their network. The only difference from one case to another was the number and exact flavor of applications found. For enterprises relying on traditional security infrastructure this lack of application visibility and control can only increase as the application landscape continues to evolve in four different areas: Consumerization of enterprise networks and applications; tunneling applications used to mask user activities; use of encryption within applications as a security mechanisms or a masking agent; and enterprise applications now being used by consumers.

Major Trends

While every customer engagement varied in terms of scope of application usage, there were several common themes.

- **Acceptable application use policies are inconsistent.** Policies ran the gamut of completely absent, to existing several-year-old policies, to a fairly detailed policy that outlined specific applications and use cases. Enforcement of policies in nearly all of the cases was via lip service or a point solution that viewed only a small subset of the applications traversing the network. In all cases, one of the key goals that customers were working toward was the establishment and enforcement of an accurate, acceptable application usage policy.
- **Circumventors are being used frequently.** Applications designed specifically to circumvent security, in some cases via encryption, are on the upswing. Called anonymizers and circumventors, these applications hide a user’s identity by proxying the application, using encryption or both.
- **P2P is still used heavily.** Despite efforts to control it, P2P was found in nearly every account and while there may indeed be legitimate uses for P2P, none of the customers endorsed it as an acceptable application for use in IT or otherwise.
- **Port 80 is more than web traffic and applications.** There was a time when applications that used port 80 were primarily HTTP/browser-based applications. This is no longer true. Applications of all types are now using port 80 either as a default or as an alternative and many of them have nothing to do with the browser or web traffic. As an example, SharePoint, a Microsoft collaboration tool uses port 80/443 initially but can also move from port to port, much like any other port hopping application. Other examples of applications that may use port 80 (or any other port) include antivirus updates, all sorts of IM, P2P and iTunes.

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

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

Consumerization of Enterprise Networks and Applications

Defined as the use of consumer-oriented applications and supporting technologies within the enterprise, this trend has accelerated dramatically recently. The best example of a consumer application that is now common within the enterprise is instant messaging, an application that was initially targeted specifically at consumers but is found throughout organizations. Salesforce.com, AV updates, Skype and Google applications are just a few other examples of the use of consumer-oriented technologies (browsers as the client, HTTP, Port 80, etc) for enterprise applications. These applications represent a significant challenge for security teams because of the delicate balance required in controlling them. Restrict or block access to the application and users become unhappy, very possibly impacting productivity or worse yet, the business process. This leads to users finding a work-around for whatever security controls are stopping them.

Industry analysts, such as Gartner, are encouraging enterprises to figure out a way to embrace the use of new application technologies, but in order to do so, enterprises need more information on the applications in order to determine how to treat them. The default action of blocking is no longer appropriate due to the widespread use (often at the executive level) of some of these applications. A more pragmatic approach is to weigh the security risks against the business impact, then implement fine-grained enforcement. From a security perspective, enterprises need to look at the data loss, privacy, productivity and threat implications. From a business point of view, key criteria include whether or not the application will help in attracting new employees, its ability to help establish an improved work/life balance, to make employees be more productive, to reduce operational costs, and perhaps most importantly – will it generate more revenue?

Instant messaging: evasive features bring business and security risks.

Instant messaging is a powerful tool. As an example, two employees in different offices on a customer conference call can use IM to do on the fly strategizing. The downside of IM is that it also represents possible data loss, compliance and productivity risks because it bypasses most corporate tracking mechanisms, creating problems for regulated and intellectual property-centric industries. Many also now have file transfer capabilities, which cannot be tracked.

Instant messaging applications were originally targeted solely at consumers and deployed in an Internet-based, persistently installed client model, but are now migrating toward a browser-based model, bringing their evasive, port-hopping and file transfer capabilities with them in an effort to simplify use and possibly evade detection by corporate firewalls. Of the 36 IM applications identified by Palo Alto Networks, 19 are browser-based while 17 install their own client. Those that began life as an installable client (AIM) now have variants that are browser-based (AIM-Express). The mix of browser-based versus client-based IM applications found across the 20 sites was close at 75% and 90% respectively, but the prediction is that future versions of this report will show use of browser-based IM to exceed use of persistent client IM.

In most of the engagements, IT had all but given up trying to control IM due primarily to the fact that there are so many IM offerings and there are few, if any, effective ways to control it. Several customers had policies defining the use to specific IM applications, but only for certain groups. Palo Alto Networks' findings showed that the policies were ignored.

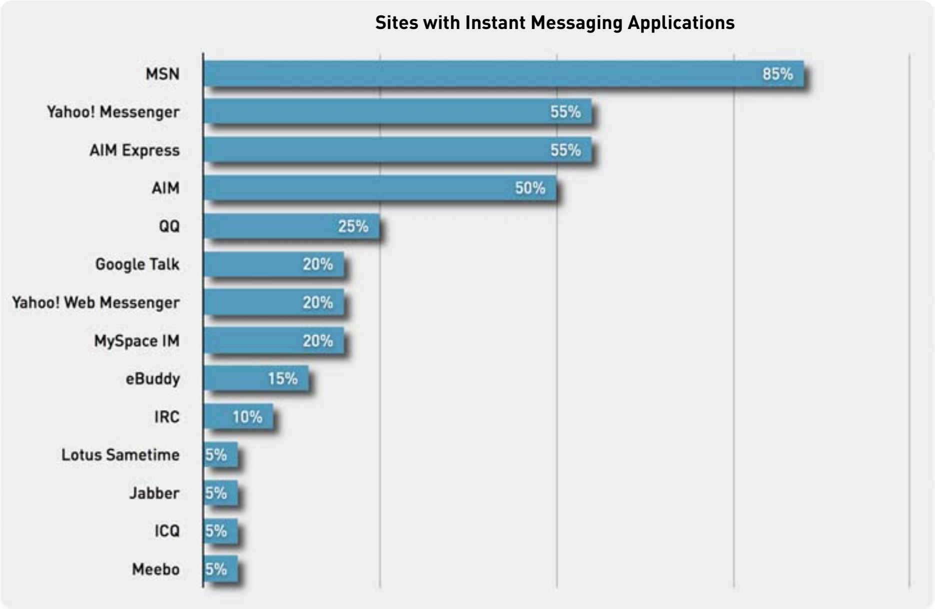

Figure 2: Breakdown of individual Instant Messaging applications found across all 20 sites.

Web mail: rampant use brings delicate balancing act of personal email on company time.

With 100% of the customers finding at least one web mail application on their networks, in some cases as many as five different variants, web mail follows closely on the heels of IM as an example of an application that is used in enterprises, although more for personal use than corporate use. AOL Mail was the most common variant with Gmail and Outlook Web tied as the second most common web-based email application. Outlook Web Access, is typically IT supported, while Gmail and any other web mail applications are typically not supported by enterprise IT. Like IM, web mail is undetected by most firewalls since it uses port 80, but may not be HTTP and therein lies the problem—tracking of activities and unseen file transfers represent compliance, data loss and business continuity risks.

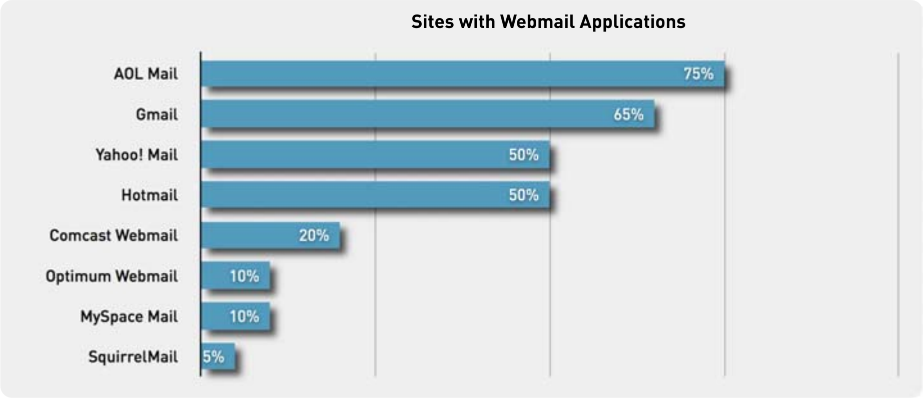

Figure 3: Breakdown of individual web mail applications found across all 20 sites.

Peer-to-peer applications: prevalent on enterprise networks, despite control efforts.

Multiple use cases, some good, most not, can be applied to peer-to-peer applications, but the primary reason that P2P technology was developed was to move large files around by leveraging distributed resources. While IT may in fact use P2P on a rare occasion for that express purpose (e.g., moving Linux binary files), in most cases, P2P on a corporate network means that an employee is using it to share files of some sort – music, video, graphics – any type of file is fair game. This is where the problems arise, as exemplified by the unintentional yet highly publicized distribution of employee data on several occasions. Not surprisingly, P2P applications were found in 90% of enterprises – in several cases, as many as seven different P2P application variants. In several cases, imaginative employees had brought their home PCs into work, installing them on the corporate network to run P2P on the high speed network. As a result of this analysis, some organizations have created appropriate computing resource usage policies to eliminate the use of home PCs on the network.

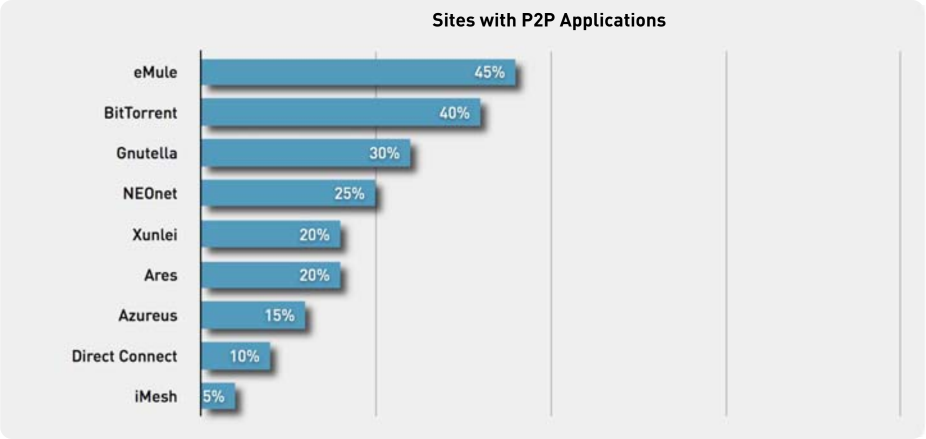

Figure 4: Breakdown of most common P2P applications discovered across all 20 sites.

Web-based file transfer and storage: harmless utility or data sinkhole?

These applications are utility-oriented, designed under the guise of helping users share large files. Users upload their files and are given a password-protected URL, which can then be sent to whomever they want. For home use these applications may be very helpful as a means to bypass ISP-enforced email attachment limitations, but in a corporate environment, outside of the visibility of IT, their value is questionable and may not outweigh the data loss and compliance risks. While these applications were found in 30% of environments in the sample, the frequency of occurrence of these types of applications has risen sharply recently as users have latched onto them as a way to get around IT-enforced email attachment limitations, or worse, content-focused rules.

Media applications: consuming bandwidth at an extraordinary rate.

Streaming audio and video are known to consume large amounts of bandwidth, but this report shows that it has risen to an alarming level within corporate environments. In several cases, media applications (video and audio applications of all types) were consuming upwards of 30% of the organization’s bandwidth. Putting the bandwidth issues and associated costs aside, there is also an employee productivity issue to consider with most media applications. Media applications found across the 20 sites can be broken down into several different categories.

- Browser-based video applications: The most common example is HTTP-Video which was found in 100% of the customer environments. Not surprisingly in 25% of the accounts, commercially available media applications that leverage the browser such as YouTube, VeohTV, SocialTV, and MetaCafe were found to be on the customer networks. This statistic is expected to increase as more streaming video applications such as Hulu Networks become popular.

- Video applications using peer-to-peer: in a perfect example of technology trying to turn over a new leaf, P2P is now being used in commercial video streaming solutions such as Skinkers, BitTorrent DNS, UUSee, TvAnts, SopCast, PPStream and PPLive. While not nearly as prevalent as HTTP-Video, but more likely to consume massive amounts of bandwidth, due to their ability to stream movies, sports events and prime time TV, these applications were found on 25% of enterprises in our sample.
- Streaming audio applications: Perhaps less of a productivity concern than video-related applications (but still a bandwidth consumer), streaming audio over HTTP was found in 100% of the accounts while non-HTTP audio (client/server) applications were found in 35% of the enterprises.

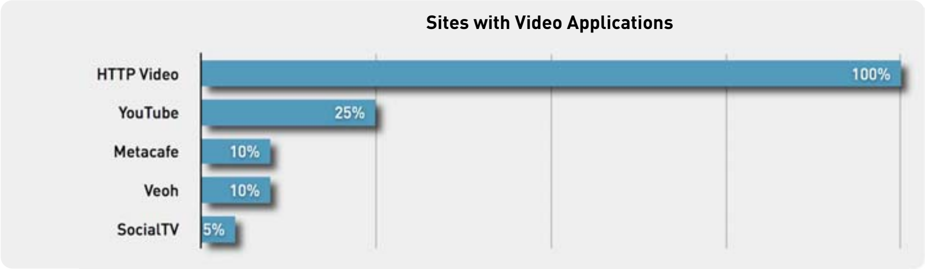

Figure 5: Breakdown of video applications discovered across all 20 sites.

Social networking: collaboration, recruitment tool, security threat or a waste of time?

If we listen to the news, social networking applications are the current “killer app” and they are unlikely to go away anytime soon. Employees, particularly those who are entering the work force now, have become accustomed to using social networking applications and expect to do so at work. When used in a structured manner within corporate environments, the value of social networking can be enhanced communication and collaboration resulting in more rapid time to market, often with a better, more thoroughly researched product or service.

This is where enterprises face a dilemma – do they block it and force users to go around it? Do they allow it but in a controlled manner (e.g., based on schedule)? Or do they embrace it internally, using it to recruit new employees, and hopefully fostering collaboration. The answers will vary, but 75% of the organizations participating in the AVR report service had social networking on their network. These applications are possibly the best example of why it is important to make an informed security policy decision. By knowing which application it is, the related security risks and who may be using, organizations can make an informed security decision.

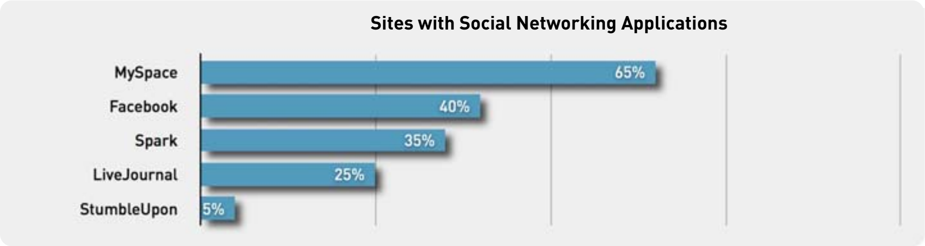

Figure 6: Most commonly found social networking applications across all 20 sites.

Google applications: powerful tools that challenge IT to control them.

Many may not be aware of the wide range of applications that Google has made available to end-users. Gmail is an obvious example, but Google Docs, Desktop, and Calendar are just a few of the powerful applications that Google has made available, for free, over HTTP(S). These applications were found in 60% of the customer engagements and we expect the numbers to increase. This is not to say that organizations have actually endorsed these applications. On the contrary - many do not want them on the network. But many end users are using these applications and Google has added fuel to the fire by challenging end-users to openly ignore/circumvent IT attempts to exert control over the use of these applications. There are several reasons why enterprises do not want these applications on their network. Support is one obvious reason, but less obvious is the fact that Google learns from their end-user traffic and this is something most enterprises want to avoid. For example, Google Desktop, if improperly configured, can index the files of the user's machine into the massive Google repository.

Tunneling Applications Mask User Activities

Tunneling applications are very powerful applications that, in some cases, are used by IT to bolster their security infrastructure and support end users. In other cases, their evasive characteristics can be used to mask the user's intentions. Web surfing proxies can be used to hide IP addresses or they can be used to bypass a firewall. Remote desktop applications can streamline help desk operations or they can allow a user to again, sneak past the firewall. Finally, most of the encrypted tunneling applications are designed solely to bypass detection.

Non-IT proxies: dedicated to bypassing the security controls.

Several types of these applications were detected in corporate environments during the traffic assessments. The case behind most of these applications is relatively clear cut – they are designed to tunnel one application inside another, in some cases using encryption such as SSL or a proprietary algorithm. Examples of these types of applications include non-IT supported HTTP-Proxies like KProxy, CGIProxy and PHproxy. When deployed on an end-user machine, outside of the realm of IT support, the sole purpose of these types of applications is to evade detection. The decision on how to treat some of these applications is fairly clear cut, assuming that they can be detected on the network. Non-IT supported proxies were found in 80% of the customer environments.

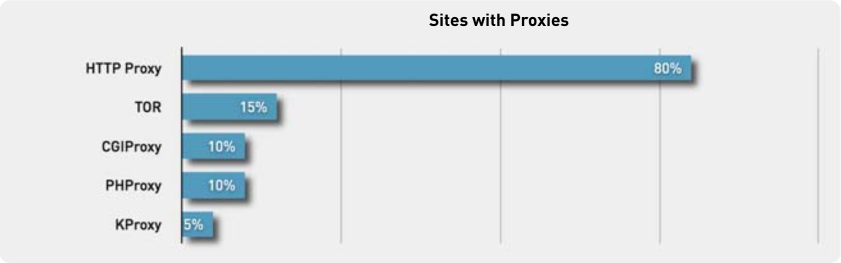

Figure 7: Most commonly found proxy and tunneling applications discovered across all 20 sites.

Encrypted tunneling applications: no legitimate business use case on corporate network.

Applications such as TOR (The Onion Router), Hamachi and Hopster were found in 15% of the customer environments. Looking specifically at TOR as an example, the official web site (http://www.torproject.org/) description reads as follows:

> *"Tor is a software project that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."*

There are very few, if any, reasons an employee should have this type of application residing on their work PC, particularly if it is outside of the realm of IT support.

Encrypted Applications – Protection or Masking Mechanism?

These applications typically use encryption, often times proprietary, to bypass detection. Application examples include Skype, Joost and Bittorent (uTorrent) as well as those that may use SSL.

Skype.and Joost: Encryption for security or to bypass detection?

Skype and Joost are two examples of applications that use encryption as a default or an option to "protect transmission" but in reality, the use is to bypass security controls. While these applications were found in only 50% of the engagements, they raise concerns among IT organizations because the applications, with their proprietary encryption, can lead to clandestine transmission of malware, as well as corporate data—all while obscured/protected by encryption.

SSL: the black hole on enterprise networks.

Not surprisingly, SSL was present in 100% of the customer engagements, although quite a few customers were surprised at the quantity of SSL in use. Encrypted SSL traffic will require a very delicate balancing act for enterprises in terms of what they should and should not decrypt. Healthcare, 401K and stock plan access will likely be left alone in most organizations, while access to other non-work-related and many collaborative business applications may be fair targets for decryption and inspection.

Enterprise Applications Used by Consumers

Of the 161 applications detected (Appendix 2) across the 20 different accounts in this sample, approximately 25% were traditional networking protocols, VoIP, database applications, as well as collaboration and email applications. Within the applications that may be considered enterprise-oriented, the analysis found there are some cases where these applications are being used for end-user (consumer-oriented) purposes.

Remote login control applications: powerful utilities that bring new risks.

These applications allow the PC administrator to login to a remote machine, establishing a tunnel providing the user with full, remote control of that PC. Originally designed for help desk environments, these applications are allowing end-users to login their home PCs where end-user applications can be accessed without interruption (or detection). Applications such as LogMeIn, VNC and MS-RDP were found in 75% of the customer engagements. Several customers had specific policies for these applications that allowed their use, but only over a specific port. For those customers, the findings confirmed that the policy was being violated – employees were logging into their home machines from work and were using non-work related applications.

Some of the more sophisticated users were using SSH to establish a secure tunnel to their home PC, leaving it open so that they could go home and then use the SSH tunnel as an unmonitored access point to the corporate network.

VoIP: a powerful tool with high potential for abuse.

Traditionally, VoIP was an enterprise application, but it has become a very accessible end-user application. Skype, MSN-Voice and Yahoo-Voice were found in 75% of the customer engagements (SIP and H.323 were also detected). Seemingly harmless in their goal of enabling inexpensive phone calls, the issue with these applications is that many fall outside the realm of IT support. Additional risks are introduced because some of them have had known vulnerabilities while others are capable of file transfer, bringing data loss issues.

Summary

The findings in this report demonstrate that it is no longer a simple task to flatly declare applications good or bad. An accurate assessment means viewing details on the applications themselves as well as the individual application risk characteristics, and balancing that risk against the business value of the application. This level of detail is becoming increasingly critical as more enterprises look to embrace those applications that, in the past, have been banned and/or blocked. The Palo Alto Networks PA-4000 Series and the Application Visibility and Risk Report assessment service is helping customers regain visibility into and control over the applications traversing their network.

The powerful combination of identifying and controlling, via security policy, more than 560 applications is bringing granular levels of application visibility and control back to the IT department where it belongs. The summary of the Palo Alto Networks Application Visibility and Risk reports performed in 20 enterprise customers is a proof point that enterprises want to know which applications are traversing the network and how to control them.

Appendix 1: Methodology

The Palo Alto Networks Application Visibility and Risk assessment involves deploying a Palo Alto Networks PA-4000 Series firewall within the customer 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 one to seven days, an Application Visibility and Risk Report is generated that presents the findings along with the associated business risks and a more accurate picture of how the network is being used.

Instead of relying solely on port and protocol as the means of identifying traffic, Palo Alto Networks uses a patent-pending technology called App-ID. Designed to address security evasion tactics commonly used in many of today's new applications, App-ID and the PA-4000 Series firewall helps IT regain application visibility and control. The identity of the application generated by App-ID provides IT with exactly which applications are traversing the network, displayed in their common names, as opposed to the port and protocol. This information can be used to create and enforce application usage policies that may enable the secure use of previously banned applications or may more accurately block those applications that have no business on a corporate network.

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

To facilitate the decision making process on how to treat an application, Palo Alto Networks provides additional background for more than 560 applications including a detailed description, alternative sources of information and which port(s) are commonly used. To help keep administrators more informed, eight different application characteristics are provided including:

• File transfer capabilities	• Known vulnerabilities
• Ability to evade detection	• Propensity to consume bandwidth
• Used for malware transmission/propagation	• How pervasively it is used
• Whether it tunnels other applications	• Is it prone to misuse

Rounding out the application knowledge accessible by an administrator is what underlying technology the application uses (browser, client-server, P2P or network protocol). Used as a research tool or as a policy creation tool, Palo Alto Networks is bringing visibility and corresponding control back to the IT department. To view the applications and their respective characteristics, please visit the Palo Alto Networks Application Research Center at www.paloaltonetworks.com/arc. The remainder of this document highlights the findings generated from the 20 Application Visibility and Risk Report service.

Appendix 2: Most Common Applications Found

Listed below are all of the applications found across all 20 accounts, ranked in terms of frequency. Note that there is a mix of consumer or end-user oriented applications along with a wide range of business and networking applications. To view details on all 560+ applications, including their characteristics and the underlying technology in use, please visit www.paloaltonetworks.com/arc.

1. SSL
2. HTTP-Video
3. Flash
4. FTP
5. HTTP-Audio
6. RSS
7. SMTP
8. Webdav
9. MSN
10. HTTP-Proxy
11. AOL-Mail
12. DNS
13. MS-Update
14. Myspace
15. MS-RDP
16. SNMP
17. ICMP
18. Atom
19. Outlook-Web
20. Gmail
21. Google-Desktop
22. MS-Exchange
23. Yahoo-IM
24. AIM-Express
25. Netbios-NS
26. POP3
27. AIM
28. MSRPC
29. NTP
30. Yahoo-Mail
31. Hotmail
32. MS-DS-SMB
33. Google-Safebrowsing
34. eMule
35. Yahoo-Voice
36. Skype
37. Facebook
38. Web-Crawler
39. Soap
40. BitTorrent
41. LDAP
42. Spark
43. SIP
44. Google-Calendar
45. MSN-File-Transfer
46. Gnutella
47. MS-Netlogon
48. MSN-Voice
49. Google-Picasa
50. Google-Earth
51. YouTube
52. LiveJournal
53. Syslog
54. qq
55. NEOnet
56. Megaupload
57. IMAP
58. Active-Directory
59. Live365
60. Skype-Probe
61. X11
62. Google-Toolbar
63. Live-Meeting
64. Google-Talk
65. MySpace-IM
66. Yahoo-Webmessenger
67. SharePoint
68. Xunlei
69. Ares
70. TFTP
71. Comcast-Webmail
72. Kerberos
73. iTunes
74. SopCast
75. RTMP
76. RTSP
77. RTP
78. Move-Networks
79. Google-Docs
80. Yahoo-Toolbar
81. eBuddy
82. Netbios-SS
83. Netbios-DG
84. DHCP
85. Azureus
86. TOR
87. Pandora
88. H.323
89. UUSee
90. TvAnts
91. PPLive
92. VeohTV
93. Metacafe
94. Flexnet-Installanywhere
95. LogMeIn
96. PHProxy
97. CGIProxy
98. SNMP-Trap
99. Norton-AV-Broadcast
100. NCP
101. IRC
102. SLP
103. Subspace
104. DirectConnect
105. SSH
106. IPsec-ESP-UDP
107. Lotus-Notes
108. MySpace-Mail
109. Oracle
110. MSSQL-DB
111. Radius
112. Cooltalk
113. PPStream
114. MMS
115. SocialTV
116. Dotmac
117. Apple-Update
118. TrendMicro
119. StumbleUpon
120. GRE
121. VNC
122. R-Services
123. R-Exec
124. Rlogin
125. Radmin
126. KProxy
127. MS-Groove
128. CPQ-Wbem
129. SAP
130. Echo
131. IPP
132. Yum
133. Symantec-Syst-Center
134. Sophos-Update
135. EtherIP
136. Google-Analytics
137. Blog-Posting
138. Elluminate
139. Adobe-Connect
140. Jabber
141. Lotus-Sametime
142. ICQ
143. Meebo
144. Portmapper
145. RPC
146. SharePoint-Admin
147. Corba
148. Yahoo-File-Transfer
149. IMesh
150. Gtalk-File-Transfer
151. RapidShare
152. YouSendIt
153. Backweb
154. IPsec-ESP
155. IKE
156. Lotus-Notes-Admin
157. Groupwise
158. Squirrelmail
159. Optimum-Webmail
160. Sybase
161. MySQL