Controlling Peer-to-Peer Applications

April, 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

Palo Alto Networks provides enterprises with visibility into and control over applications traversing the network irrespective of port, protocol, SSL encryption or evasive tactic used. With the knowledge of the application identity in hand, administrators can then use that data to implement granular security policies.

As highlighted in this paper, P2P applications are just one example of the type of applications that are identified and can be controlled by Palo Alto Networks. The visibility and control outlined in this paper can be applied to more than 500 applications across 14 categories including email, web mail, business applications, networking and more. Visit the Application Research Center at www.paloaltonetworks.com/arc for a complete breakdown of the categories and their respective applications.

Introduction

Peer-to-Peer (P2P) technology is not new, in fact, some of the earliest cases of P2P use were in Usenet and news server systems with the use case being the distribution of news articles. P2P applications are designed to leverage shared resources, CPU cycles and bandwidth, across an ad hoc network. The advantage of a P2P network is that it distributes the load across a network and decentralizes command and control, rather than focusing it on a small number of centralized servers. For many years, P2P was used quietly in the technical community and in fact can be a very useful tool for an IT department or anyone who needs to deal with moving large files around.

The Internet boom and the release of Napster brought P2P squarely into the music sharing application business and more recently it has expanded into video sharing and distribution. While Napster has been shut down, many more P2P offspring have risen, garnering an extremely bad reputation brought on not by it's distribution efficiency but by what was being distributed - copyrighted music files and other materials.

The Dark Side of P2P

More recently, P2P technology has been at the heart of some inadvertent sharing of employee records in several large, well known organizations where employees inadvertently exposed the personal data of employees and customers via P2P applications on their computers. Whether these data exposure examples were purposeful or not is unknown – what is known is that many of the readily available P2P applications are confusing and can be improperly configured, resulting in the unintentional sharing of folders as highlighted in a report assembled by the US Patent and Trademark Office. The report looks at five leading P2P applications and shows how, in the hands of an inexperienced user, P2P can be a dangerous tool, exposing personal and corporate information with ease.

- Pfizer Breach Illustrates Risks of Sharing Files
  http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=296490&intsrc=news_ts_head
- P2P Leads to Major Leak at Citigroup Unit
  http://www.darkreading.com/document.asp?doc_id=134544
- Filesharing Programs and Technological Features Induce Users to Share
  http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf

Not to be left out in the cold, malware creators and thieves have joined the fray. Knowing that P2P can easily evade today's firewalls and that it is pervasively deployed by inexperienced users, hackers have begun using P2P as a means of BOT distribution and file collections. In one recent discovery, a Trojan deployed by P2P technology laughs at you while it deletes your files. And in a more worrisome trend, many popular P2P search terms are no longer names of a

favorite song or movie but are now terms used to steal identity or personal information. So the question arises, which is to blame, the application or the application owner?

P2P Applications For Commercial Use?

What is important to point out is that P2P was not developed to be used maliciously – it can be a valuable tool in the hands of an experienced user. And as the trend towards web-based media continues, P2P technology can be used to deliver a service or improve productivity. Recent examples include:

- Microsoft Secure Content Downloader (MSCD), Peer-Assisted Download Manager To Deliver Software Updates
  http://www.microsoft.com/downloads/details.aspx?familyid=9a927cf6-16e4-4e21-9608-77f06d2156bb&displaylang=en
- Skinkers teams With Microsoft For New Live Streaming TV Offering
  http://arstechnica.com/journals/microsoft.ars/2007/07/05/livestation-to-offer-live-streaming-television-over-the-internet
- Bittorrent Jumps Into Enterprise Market With Content Delivery Service
  http://www.news.com/8301-10784_3-9793357-7.html?tag=nefd.only

Undoubtedly there are many other cases where P2P is used in a beneficial manner, and given the fact that the Internet is an established piece of most corporate networks, it is predicted that P2P will continue to be rolled into commercial software solutions. As a result, corporate IT departments will be doubly challenged in their efforts to control P2P applications--blocking the "bad" P2P applications (and their owners) while allowing the "good" ones. Best practices need to be implemented—both in terms of policies and technology—to control the use of P2P and its associated risks.

Controlling P2P Applications

As a tool that leverages distributed resources, P2P applications need to be connected to a network of other users. This enables them to evade detection through various means. They will port hop, continually searching for a port that the firewall allows traffic over to get connected. They are known to emulate or use HTTP as another means of passing through the firewall as if it is web browsing traffic, undetected. And some P2P applications are known to use encryption, yet another means of evading detection.

While P2P applications do indeed offer potential benefits to enterprises, they also bring certain risks. In order to mitigate those risks, it is recommended that a multi-faceted approach to controlling them be implemented.

If application controls are going to be implemented and enforced, they should be part of the overarching corporate security policy, whether it is P2P or otherwise. And as part of the process of implementing an application control policy, IT should make a concerted effort to learn about the P2P applications. Proactively installing them in a lab environment to see how they act can be very educational. Another form of education is peer discussions, asking other IT professionals for their input is an invaluable source of information. Yet a third source of information would be the P2P focused web sites, message boards and blogs. Ignoring the issue or acknowledging it exists but doing nothing about it until "something happens" can be a career limiting tact.

Employee Controls

Most companies have some type of application usage policy, outlining which applications are allowed, and which are prohibited. It is assumed that every employee understands the contents of this policy and the ramifications of not complying with it. While employee policies are a key piece to the P2P control puzzle but in many cases, they represent a number of challenges.

- Given the increasing number of “bad” applications, how will an employee know which applications are allowed and which are banned?
- How is the list of unapproved applications updated, and who ensures employees know the list has changed?
- What constitutes a policy violation?
- What are the ramifications of policy violations – firing or a reprimand?

Documented employee policies are a key piece to the P2P control puzzle but will remain largely ineffective as a stand alone control mechanism.

Desktop Controls

Desktop controls present IT departments with significant challenges. Careful consideration should be applied to the granularity of the desktop controls and the impact on employee productivity. As with employee policies, desktop controls are a key piece to the gaining the upper hand on the growth of P2P applications in the enterprise and if used alone, will be ineffective for several reasons.

The drastic step of desktop lock down to keep users from installing their own applications is a task that is easier said than done.

- Laptops connecting remotely, Internet downloads, USB drives and email are all means of installing applications that may or may not be approved.
- Removing administrative rights completely has proven to be difficult to implement and, in some cases, limits end-user capabilities.
- USB drives are now capable of running an application so in effect, the P2P application could be accessed after the network admission was granted.

Desktop controls can complement the documented employee policies as a means to gain the upper hand on P2P applications.

Network Controls

At the network level, what is needed is a means to identify the P2P applications and block or control them. By implementing network level controls, IT is able to minimize the possibility that internal files are shared and network congestion associated with large file transfers is alleviated. Several possible control mechanisms can be used at the network level, each of which carry certain drawbacks that reduce their effectiveness.

- Stateful firewalls can be used as a first line of defense, providing coarse filtering of traffic and segmenting the network into different, password protected zones. One drawback to Stateful firewalls is that they use protocol and port to identify and control what gets in and out of the network. This port-centric design is relatively ineffective when faced with applications such as P2P that hop from port to port until they find an open connection to the network.
- Adding IPS to a firewall deployment enhances the network threat prevention capability by looking at a subset of traffic and blocking known threats or bad applications. IPS offerings lack the breadth of applications and the performance required to look at all traffic across all ports and as such, cannot be considered a full solution.
- IPS technologies are typically designed to look only at a partial set of traffic to avoid impeding performance, and as such, would be unable to cover the breadth of applications needed by today’s enterprises. And finally, managing a FW+IPS combination is usually a cumbersome task, requiring different management interfaces pointed at separate policy

tables. Simply put, the current bolt-on solutions do not have the accuracy, policy, or performance to solve today's application visibility and control requirements.

- Proxy solutions are another means of traffic control but here too, they look at a limited set of applications or protocols and as such only see a partial set of the traffic that needs to be monitored. So a P2P application will merely see a port blocked by a proxy and hop over to the next one that is open. By design, proxies need to mimic the application they are trying to control so they struggle with updates to existing applications as well as development of proxies for new applications. A final issue that plagues proxy solutions is throughput performance brought on by how the proxy terminates the application, and then forwards it on to its destination.

The challenge with any of these network controls is that they do not have the ability to identify P2P applications; look only at a portion of the traffic and suffer from performance issues.

Using the Palo Alto Networks Firewalls to Control P2P

Palo Alto Networks avoids many of the issues that existing network control solutions suffer from by delivering a high performance firewall that takes an application-centric approach to traffic classification, accurately identifying all applications traversing the network, irrespective of port, protocol, SSL encryption or evasive tactic employed. By addressing security evasion tactics commonly used in many of today's new applications with a new traffic classification technology called App-ID™, Palo Alto Networks can help IT regain control over P2P applications at the network level, complementing any existing desktop and employee control mechanisms.

App-ID™ accurately identifies more than 500 applications, including more than 30 P2P applications, flowing in and out of the network. All traffic flowing through the Palo Alto Networks firewalls is processed by App-ID™ and the identity of the application, P2P or otherwise, is displayed in the management interface using their common application names. The application identity is then used as the basis of all firewall security policies including access control, user permissions, threat prevention and more.

Identifying P2P Applications

Palo Alto Networks' App-ID uses multiple traffic classification mechanisms, operating in concert, to determine exactly what applications are traversing the network. App-ID looks at traffic flowing across all ports, not just a subset of known used ports, thereby increasing the odds of detecting the application. By taking an application-centric approach to traffic classification, Palo Alto Networks addresses security evasion tactics used by P2P applications, such as the use of non-standard ports, dynamically changing ports and protocols, emulating other applications, and tunneling to bypass existing firewalls. As a result, App-ID identifies more than 30 different P2P applications, which translates to more than 100 P2P clients. By identifying the P2P network, as opposed to the clients, broader coverage is achieved in the effort to control P2P usage.

As traffic flows across the network, App-ID establishes the application session and maintains session state, while additional application identification mechanisms more accurately classify, and therefore control, the traffic. App-ID has four traffic classification mechanisms but the two that are used to identify P2P are Application Decoders and Application Signatures.

- **Application Decoders:** Application decoding in App-ID serves two purposes. First, it identifies the more complex and/or evasive applications such as P2P or Skype. It not only contains the ability to apply application signatures, but it is also able to perform more complex pattern matching operations on the traffic. Second, it is used for continuous application decoding to perform threat detection throughout the session, and can look for anomalies and changes in applications during this process.

- **Application Signatures:** Context-based signatures focus on identifying the specific applications looking for the unique application properties and related information exchange to correctly identify the traffic. The application signatures are capable of identifying a wide range of applications even when they are tunneling over non-standard ports or emulating carrier applications such as HTTP.

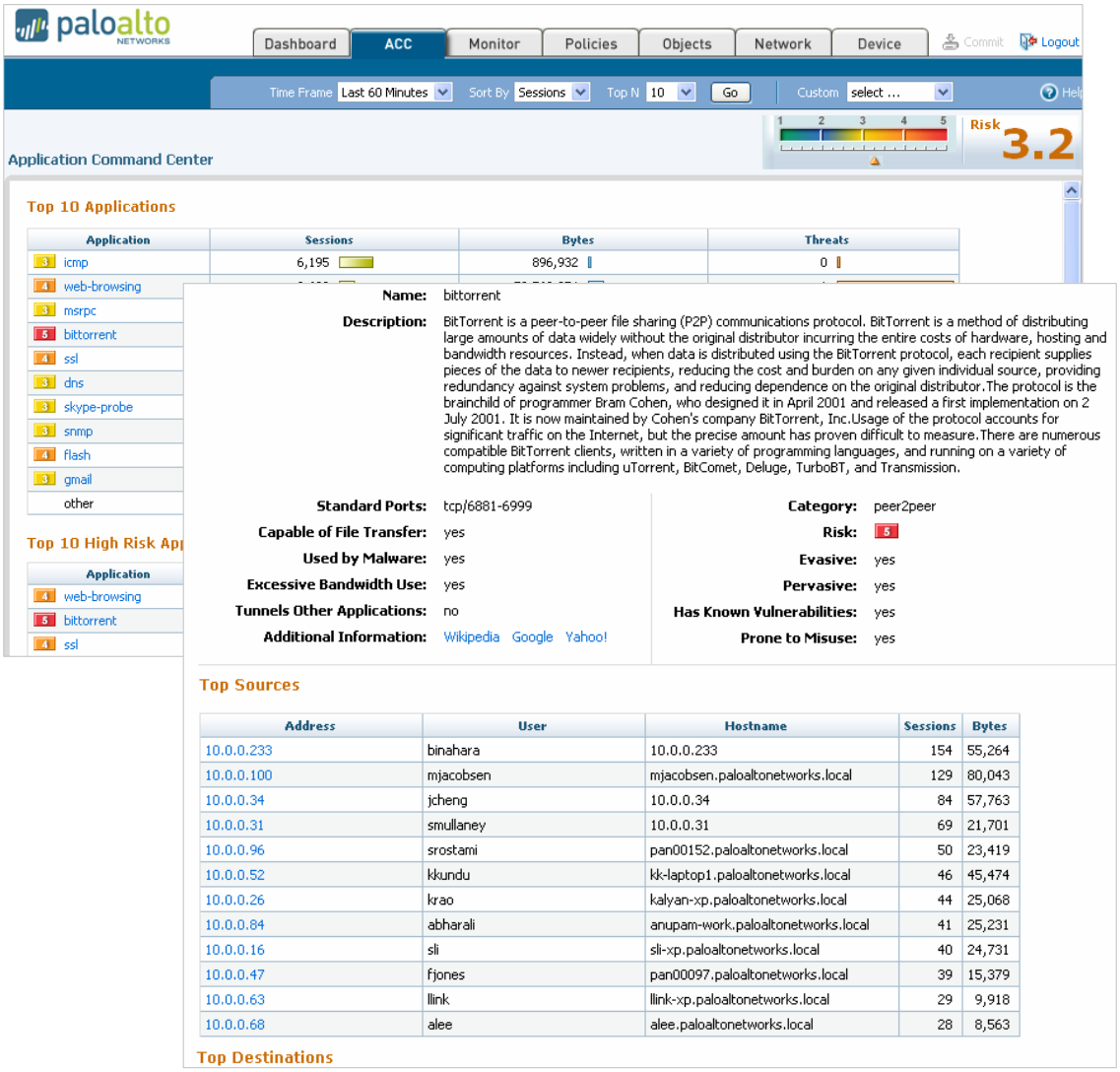

Figure 1: *Application Command Center (background screen) provides a current view of application activity with drill down into specific applications such as BitTorrent for additional details (foreground screen).*

When App-ID identifies a P2P application, the administrator can quickly see exactly which of the P2P applications are running on the network using the application names along with micro- and macro-level data, categorized by sessions, bytes, threats, source/destination IP addresses, and time. Clicking on the P2P application BitTorrent, an administrator can drill down into details on the application itself, the threats it poses, who is using it, and how much bandwidth it is consuming.

Administrators are also able to see who is using the application, based on the IP address or the specific user and group, based upon their Active Directory profile. Also included are the top 10 source and destination countries, allowing administrators to see where the traffic is flowing. Armed with the visibility into which P2P applications are traversing the network, administrators can implement security policies from the policy editor similar to traditional firewalls.

Applying Positive Control (Firewall) Policies to P2P Applications

Once the P2P application(s) have been identified, an administrator can use the rule-based editor to create a P2P application usage control policy for BitTorrent. Or, to be safer and implement a wider net, the policy can be established against the Peer-to-Peer group, thereby covering all P2P application currently identified. The advantages of selecting the Peer-to-Peer Group in the policy editor is that it catches all current as well as those that are added in the future. As new P2P applications are added by the Palo Alto Networks development team, they are automatically covered through the Palo Alto Networks dynamic update service.

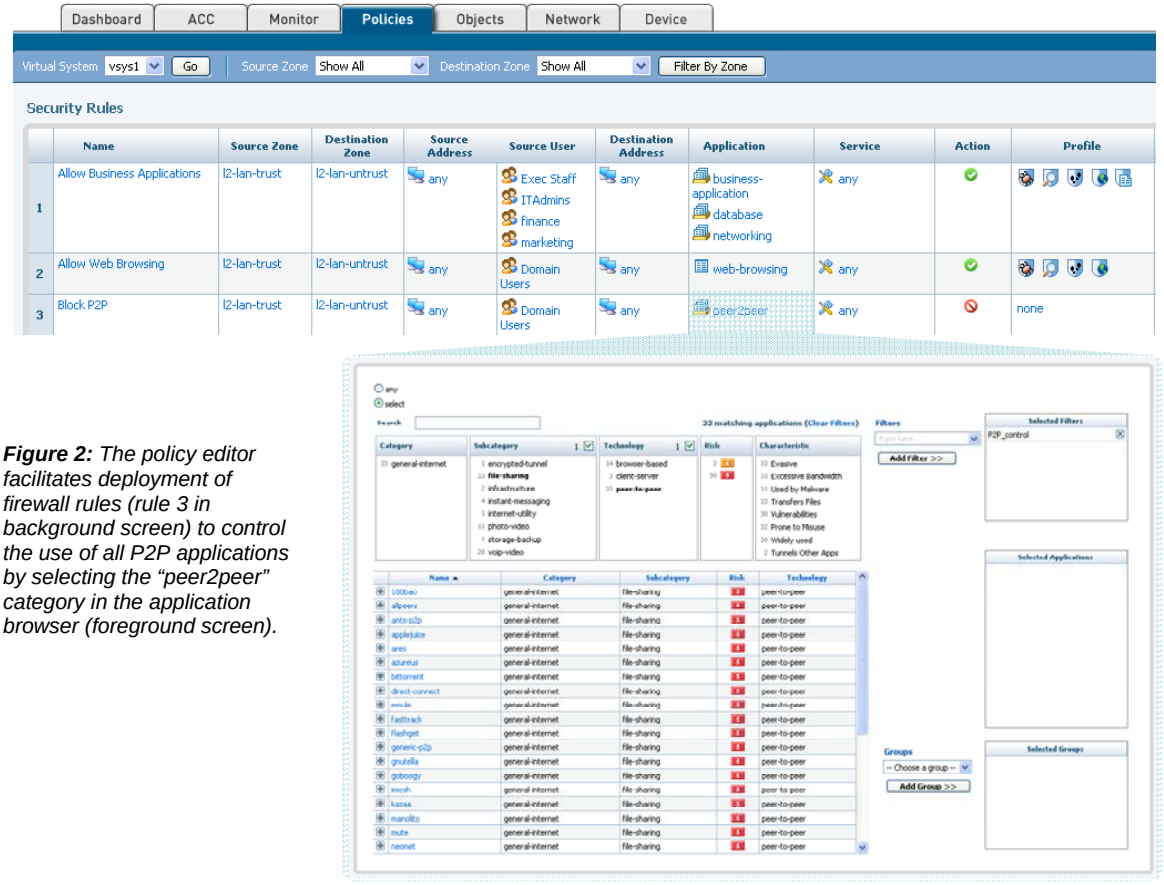

Figure 2: *The policy editor facilitates deployment of firewall rules (rule 3 in background screen) to control the use of all P2P applications by selecting the "peer2peer" category in the application browser (foreground screen).*

In some cases, administrators will want to block all P2P applications, while in others, such as when a company uses BitTorrent to distribute software, they may wish to enforce specific rules to allow it - but only for key individuals. In this scenario, an application such as BitTorrent can be selected, and then the specific users allowed to use BitTorrent are selected based on their Active Directory information – in the example below, IT and admins, mjaobsen and mkeil are allowed to use it.

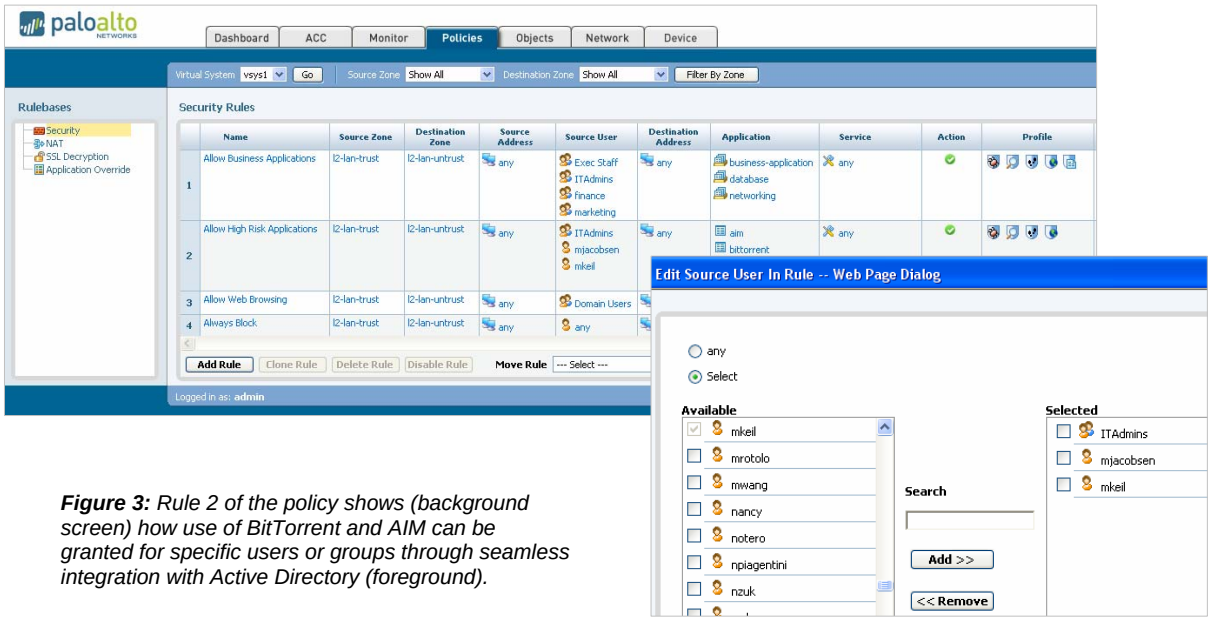

Figure 3: *Rule 2 of the policy shows (background screen) how use of BitTorrent and AIM can be granted for specific users or groups through seamless integration with Active Directory (foreground).*

Deployment Flexibility

Palo Alto Networks believes that the most appropriate place to control P2P applications is at a strategic point in the network through which all traffic flows -- the firewall. A robust networking foundation that includes Virtual Wire mode (completely transparent to surrounding devices), layer 2, or layer 3 modes brings deployment flexibility, allowing the installation in any one of 3 modes:

- **Tap Mode:** By connecting the PA-4000 Series to the network via a span port, IT can monitor traffic in real-time, providing the IT department with exactly which applications are traversing the network without disrupting the existing infrastructure.
- **Inline Transparent Mode:** Using Virtual Wire mode, the PA-4000 Series is deployed inline, complementing, yet completely transparent to the existing security infrastructure, allowing IT to begin controlling applications as needed.
- **Primary Firewall:** With full support for traditional firewall applications, protocols and access control capabilities, the PA-4000 Series can perform all of the same allow/deny functionality that existing firewalls can, allowing the PA-4000 Series to become the primary firewall solution.

Conclusion

By discarding the traditional traffic classification mechanisms of port and protocol, and taking an application centric approach, the Palo Alto Networks PA-4000 Series next-generation firewall is able to bring unparalleled application visibility and control back to the IT department. Whether the need is to control one of the application categories such as P2P or a more general application visibility and control requirement, the PA-4000 Series allows administrators to define traditional firewall policies to control their application traffic.