



To Block or Not. Is that the Question?

December 2009

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

Contents

Executive Summary.....	3
Enterprise 2.0 Applications	3
The Three Characters In The Enterprise 2.0 Play	6
The Role Of IT: Safe Enablement Through Smart Policies	8
The Tools Required To Safely Enable Enterprise 2.0.....	9
Employee Controls	9
Desktop Controls.....	10
Network Controls	10
Using the Palo Alto Networks Next-Generation Firewall.....	11
Identifying Enterprise 2.0 Applications	11
Applying Positive Control (Firewall) Policies to Enterprise 2.0 Applications	13
Deployment Flexibility.....	14
Conclusion	14
About Palo Alto Networks	15

Copyright © 2009, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, "the Network Security Company," PAN-OS, FlashMatch, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. in the United States. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

EXECUTIVE SUMMARY

There is a serious problem with today's enterprise networks—the users are in control.

IT workers—who ironically are equally at the root of this very problem—believe it is because the users are out of control. Users dare use new web-based applications and hence open up the network to unknown threats and force it to perform tasks it wasn't designed to support. Clearly those users are wrong and so the answer to this traffic problem becomes easy. *Just block it!*

Users believe it is because the IT workers didn't design the network to allow them to just get their job done. They want to use the very applications they use as consumers outside the walls of their company because they're easy. It's their collaborative, "always-on" nature that makes them sticky and relevant. It's in fact everything that the classic enterprise applications are not known for ... open, easy to use, and always connected to the rest of the world. Clearly IT is wrong and so the answer to this problem becomes easy. *Just don't block it!*

When faced with choice, the human mind tends to bias to the extremes. Why go for grey if you can turn something into a black-or-white choice? But as always, it turns out that the answer to today's problems in enterprise networks isn't a simple choice between whether to block or not. The real answer lies in the ability to see exactly what is going on, apply a shade of grey, and come up with the right answer.

This White Paper is a practical guide to how to properly deal with Enterprise 2.0 applications (and what they are to begin with)—from getting visibility to how to create and enforce policies that allow for safe enablement. The data used in this paper is based on application and network traffic in over 200 organizations worldwide collected during a 6-months period in 2009¹.

ENTERPRISE 2.0 APPLICATIONS

Only a few years ago, the world was still considered round. Borders existed around countries, cities, even companies. Some were imaginary borders enforced by policies of law, others were physical borders enforced by machines. The firewall became the "borderline" to enterprise networks. Nothing without a "passport" could come in or go out. Known traffic—of which there was little—was allowed in and all other traffic was denied access. The world was simple.

Today, we recognize the world is flat—as in a total lack of borders. We may think or hope they still exist, but in reality almost every border has been compromised. In the context of enterprise networks, the traditional firewall has long ceased to be relevant. New generations of applications, technologies, and techniques have emerged that have compromised the traditional borders, despite the veritable sprawl of technology that has been thrown at solving the problem. In other words, developers have found ways to avoid the borders by inventing evasive tactics, tunnels, and other ways to "jump the fence." In addition, the user community has found ways too. When they see URL's being blocked or applications being denied to communicate into or out of the corporate network, they find a way around it from sites such www.proxy.org. More and more so, this happens under the banner of the 4th and 5th Amendment of the [US Bill of Rights](#) or the 12th Article of the UN's [Universal](#)

¹ [Application Usage and Risk Report](#), Fall 2009 Edition by Palo Alto Networks.

[Declaration of Human Rights](#). Hence, this is no longer just a topic of IT policies but rather one of fundamental consumer rights.

Enterprise 2.0 applications have become the poster children of the flat world. Defined as "*a system of web-based technologies that provide rapid and agile collaboration, information sharing, emergence and integration capabilities in the extended enterprise*"², these applications have taken the world by storm. What started out as applications that were mostly focused on searching, linking, and tagging rapidly shifted to ones enabling authoring, networking, and sharing.

Examples of first-generation Enterprise 2.0 applications are:

- Wiki's such as Socialtext
- Blogging tools such as Blogger
- RSS tools such as NewsGator
- Enterprise bookmarking and tagging tools such as Cogenz
- Messaging tools such as AOL Instant Messenger (AIM)

Examples of second-generation Enterprise 2.0 applications are:

- Content management tools such as SharePoint
- Browser-based file sharing tools such as MegaUpload.com
- Complex social networks such as Facebook
- Publishing tools such as YouTube
- Unified messaging tools such as Skype
- Posting tools such as Twitter

While there are many efforts to build directories for Enterprise 2.0 applications that are active in the enterprise, it remains a challenge to come up with a complete list. One such effort is Appopedia³ which is published by the{app}gap.

Two efforts by Palo Alto Networks have produced both a good inventory of available applications as well as research into their enterprise adoption.

1. The semi-annual [Application Usage and Risk Report](#) that contains aggregated application adoption and usage data from hundreds of organizations worldwide;
2. The [Applipedia](#) that contains detailed information of the over 900 applications Palo Alto Networks can control, including over 200 Enterprise 2.0 applications.

² Wikipedia "[Enterprise Social Software](#)"

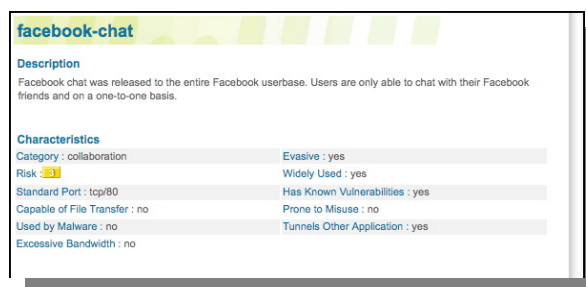
³ [Appopedia](#) by the{app}gap



Category	Subcategory	Technology	Risk	Characteristic
167 business-systems	27 audio-streaming	322 browser-based	249 1	360 Evasive
246 collaboration	10 auth-service	310 client-server	151 2	272 Excessive Bandwidth
112 general-internet	16 database	177 network-protocol	226 3	217 Prone to Misuse
123 media	47 email	98 peer-to-peer	181 4	455 Transfers Files
259 networking	22 encrypted-tunnel		100 5	196 Tunnels Other Apps
	15 erp-crm			199 Used by Malware
	84 file-sharing			487 Vulnerabilities
	26 gaming			580 Widely Used

Figure 1: Applipedia, the online application encyclopedia from Palo Alto Networks

Applications such as Facebook are in fact compound. When Facebook was introduced on February 4, 2004, it was a highly restricted application that served a single purpose. But over the years its adoption and use have exploded and today it is in use by over 300 million people worldwide—more than the entire population of the United States. During that period, Facebook introduced new applications such as Facebook photo, and in April 2008, Facebook chat. What was a simple application had now become a network of applications. But it didn't stop there. Facebook turned itself into an [application platform](#) and today [tens of thousands](#) of applications have been developed that are part of the Facebook universe. In parallel, Facebook became prone to many hacks, exploits, and vulnerabilities.



facebook-chat	
Description	
Facebook chat was released to the entire Facebook userbase. Users are only able to chat with their Facebook friends and on a one-to-one basis.	
Characteristics	
Category : collaboration	Evasive : yes
Risk : 3	Widely Used : yes
Standard Port : tcp/80	Has Known Vulnerabilities : yes
Capable of File Transfer : no	Prone to Misuse : no
Used by Malware : no	Tunnels Other Application : yes
Excessive Bandwidth : no	

Figure 2: Intelligence about Facebook chat from Applipedia

What's more concerning is how Enterprise 2.0 applications have "infiltrated" the network. For the first time ever, two major trends came together that made it possible for these applications to get adopted without IT involvement.

The first trend goes back to the early 90's, when technologies such as Visual Basic emerged that made it possible for anyone to develop simple applications without IT assistance. Servers were placed under desks to run them and users were genuinely happy because they were able to get the job done. Traditional IT consumers had now become producers. While the vast majority of these applications didn't pose a security risk to the organization, they did however become an IT nightmare from an information management and compliance perspective alone.

The second trend started when in early 2000's simple collaborative web-based applications emerged. The situation started to become very different because these applications, by their very nature, crossed the enterprise network boundaries entirely. And whereas in the nineties the usage of web-based applications was mostly for e-commerce and e-mail, these ones that were now switched on and accessible everywhere were turning information consumers into producers—first in the consumer world but rapidly in the business world as well. What's even more surprising and

worrisome to many IT professionals is how fast the innovation and adoption cycles have accelerated. For example:

- In less than 18 months since its inception in April 2008, Facebook chat has overtaken Yahoo! IM and AIM inside enterprises.
- Between March 2009 and September 2009, the enterprise penetration of Google Docs has increased from 33% to 82%.
- In that same time period, Twitter use in enterprise jumped 252% in terms of sessions and 775% in terms of bandwidth.

As stated before, Enterprise 2.0 applications are multi-faceted and multi-functional. Some of those features are quite obvious, but many are available “behind the scenes.” For example, 70% of them are capable of transferring files. That means that while the obvious use could be Voice-over-IP (VoIP) or instant-messaging, the same application can be used to transfer files. Examples of this capability include Skype and IBM/Lotus Sametime. Another complexity arises when applications can be used to share multiple artifacts. An example would be WebEx, an application that can share out desktop content to multiple viewers. In many cases, sharing a PowerPoint presentation is probably quite innocent, but sharing ones desktop through the WebEx Desktop Sharing feature introduces severe security and compliance issues.

Many Enterprise 2.0 applications also are not very good in terms of quality—sometimes because they were built that way, but more often because they haven’t been built to enterprise-class quality and security requirements. That’s why 28% of them can propagate malware and a whopping 64% have known vulnerabilities. It’s those properties that make them feared by IT and lead to a very binary attitude when it comes to allowing them on the network. But what many IT professionals have found out is that trying to block them it is not as straightforward as switching off a server or blocking a URL or port. Conventional wisdom and techniques no longer work.

Many Enterprise 2.0 applications are cloud-based and accessed through the browser. But applications such as SharePoint, which has seen an equally rapid adoption, are most often deployed on-premise and yet carry risks too. Analysts such as Gartner believe that SharePoint is very much like Visual Basic in the nineties; a third of the implementations are rogue in their conservative estimates⁴. In essence, the vast majority of Enterprise 2.0 applications make it into the enterprise without the involvement of IT. Thought leaders in this space such as Andrew McAfee and Dion Hinchcliffe actively propagate informal, user-led rollouts and strong functional management support, but don’t elaborate on the role of IT other than as an enabler of technology. It’s that lack of rigid structure and oversight that has motivated so many users in the enterprise to adopt these new applications and convinced them that it’s their right to use them to get their jobs done.

THE THREE CHARACTERS IN THE ENTERPRISE 2.0 PLAY

First, let’s focus on the developers and their role. Clearly, it would be wrong to think that most developers are of malicious intent when they develop Enterprise 2.0 applications. But the reality is somewhere in the middle. Knowing that most traditional security infrastructures would block their applications, developers have looked for ways to get through. That meant that they make the applications hop from port to port until they find a way through, or tunnel their applications through condoned traffic. Often times the motivation wasn’t to infect or pollute, but rather to reach and enable. But in doing so, the lines between bona fide and malicious intent blurred fast. The same is

⁴ [Article](#) by Gartner analyst Neil MacDonald on March 24, 2009.

true for encryption; most of the time the developers are genuinely protecting the users and their data, but more and more they use it to obfuscate and confuse.

A common issue that got introduced by the developers is the “share everything” approach. In other words, if you want to benefit from sharing, you also allow others to benefit from sharing with you. This mentality is often times directly reflected in the software where on installation the default settings—often times buried deep down in the software itself—share the files of the user out onto the network. File sharing, once again, is a good example of that. What started as Nullsoft, Napster, and KaZaA has now evolved into a vast collection of peer-to-peer (P2P) applications, protocols and technologies that live both in the open (such as LimeWire) and in the dark. But regardless of their status or legality, they all apply the same principles to sharing and cause major issues because of the ignorance of the users.

Let’s face it, regardless of the developers’ intent, it is clear that there are obvious issues related to security and compliance associated with Enterprise 2.0 applications. As Steve Hamm, a tech reporter at BusinessWeek⁵ said: “...[it] is like leaving the back door open on a restaurant. A lot of bugs are coming in.”

Many articles and even books⁶ have been written about what motivates people to use collaborative applications in the enterprise. It really all comes down to a rather simple explanation; people want to get their job done so they can go home early. While that sounds very mundane, researchers around the world have consistently found that the productivity argument not only was the motivation, but also could be proven by analyzing the actual impact. McKinsey recently conducted what is perhaps the most elaborate global study⁷ on this topic. It found that 69 percent of respondents report that their companies have gained measurable business benefits, including more innovative products and services, more effective marketing, better access to knowledge, lower cost of doing business, and higher revenues. Companies that made greater use of the technologies, the results show, report even greater benefits. Successful companies not only tightly integrate Enterprise 2.0 technologies with the workflows of their employees but also create a “networked company,” linking themselves with customers and suppliers through the use of these applications.

The above findings fly straight in the face of the anti-productivity argument often associated with the use of Enterprise 2.0 applications. While it is clear that the use of Enterprise 2.0 applications brings with it substantial security, privacy, compliance, and reputational risks, it’s also becoming very clear that the risk of people wasting their employers’ time and resources is not that great.

It’s hard to argue with the overwhelming evidence that Enterprise 2.0 applications are changing the way people work and at the same time become more productive while spending less money and time. That’s why it should come as no surprise that in a recent study⁸ by the Association for Information and Image Management (AIIM) over half of organizations are now considering Enterprise 2.0 to be “important” or “very important” to their business goals and success. However, it’s also clear that risks remain and safe enablement is paramount.

⁵ [Article](#) by BusinessWeek reporter Steve Hamm on November 24, 2009.

⁶ Examples are [Enterprise 2.0](#) by Andrew McAfee and [The Facebook Era](#) by Clara Shih

⁷ [Global survey](#) by McKinsey, September 2009

⁸ [AIIM Industry Watch Collaboration and Enterprise 2.0](#), June 2009

This then brings us to IT. Many would argue that IT's impact on and involvement with Enterprise 2.0 today is minimal, or for that matter should be minimal. Others would argue that IT as a whole is rather irrelevant in a user-driven movement such as Enterprise 2.0, and yet others argue that IT should have a stronger role. What often remains is a lot of opinions and little reason.

Most of the time, IT workers have participated just as much in Enterprise 2.0 as any other employee. After all, they're just as motivated to getting the job done as anyone else. In addition, IT workers have been asked to help users proactively or reactively with their issues related to Enterprise 2.0 applications. It is quite common for IT to be asked to enable certain applications that require a server-based installation, such as SharePoint, although there are countless examples of rogue servers "under desks" with non-sanctioned applications.

But more often than not, IT becomes aware of Enterprise 2.0-related issues once the adoption has happened. Calls into the IT helpdesk range from the benign ("I lost my Facebook password") to the extreme cases of major network and security issues such as a full-on contamination with an exploit like Koobface⁹ that infected close to 1 million computers in 2009.

THE ROLE OF IT: SAFE ENABLEMENT THROUGH SMART POLICIES

It is time for IT to become relevant in the Enterprise 2.0 discussion and movement. Going back to the very fundamentals of the role of IT, it's all about 3 things; enablement, governance, and management.

Enablement is about first and foremost about education. In the case of Enterprise 2.0 applications, the users have long decided on the benefits, although there continue to be opportunities for education on the choice of the best application for the job. IT's role is that of an advisor and mentor; showing the users what applications are best at solving the requirements, and how to best use them once selected. But enablement is also about raising the awareness of the risks associated with applications. For that, IT workers need to become true super-users themselves, albeit in a different sense of that term than usual. An Enterprise 2.0 super-user is someone who "lives" inside the application and relies on it for a major set of tasks. For IT to be relevant, it needs to adopt Enterprise 2.0 wholeheartedly and without prejudice. Once that's achieved, IT can successfully educate the users on all the risks associated with the use of Enterprise 2.0 applications—even those that pertain to the social and reputational implications of their use.

For governance to be effective, IT needs to take a major role in the definition of smart policies. But it is critical for IT not to be the sole owner of these policies as their effectiveness and relevance are inversely proportional to the amount of classic IT thinking. This may sound highly controversial, but Enterprise 2.0 applications have a tendency to become the "forbidden fruit" and butchering the "sacred cow" that are their policies has become the ingredient for the "best burgers¹⁰." And while most Enterprise 2.0 adoption starts in a bottoms-up way, it won't go very far without executive sponsorship and support. This implies that while IT may try to stop their use, once Enterprise 2.0 applications have been successfully adopted it can no longer count on executive support to do that.

Often times the governance discussion is illustrated with examples of mistakes that users made while using certain types of Enterprise 2.0 applications such as social media. It's an easy argument for IT to do so, but it's ultimately a losing one for the simple reason that "mistakes in social media

⁹ Wikipedia: [Koobface](#) worm

¹⁰ Freely borrowed from Kriegel's famous 1997 [book](#)

are inevitable – after all, you’re building relationships and what relationship is perfect?¹¹ Nor is it a smart idea for IT to pursue a compliance-based argument for the simple reason that no legislation exists per se that governs the use of Enterprise 2.0 applications. However, it comes down to using the right tool for the job and to be smart about it. For example, in a heavily regulated environment such as stock trading, the use of instant-messaging may be prone to retention and auditability rules. IT’s role is to educate the traders on the implications of each of the tools, participate in the definition of the use policy, and subsequently monitor and enforce its use. In this example, that policy could prevent the traders from using Facebook chat for instant-messaging, but enable MSN for that use.

Governance and its management counterpart work best if they’re based on a set of smart corporate policies that are developed by the 4 major stakeholders in the Enterprise 2.0 landscape; IT, HR, executive management, and the users. Clearly IT has a role to play, but it can’t be the binary role that it so often times plays nor can it be lax about its role as the enabler and governor.

THE TOOLS REQUIRED TO SAFELY ENABLE ENTERPRISE 2.0

Application controls are going to be implemented and enforced and therefore should be part of the overarching corporate security policy. As part of the process of implementing an application control policy, IT should make a concerted effort to learn about the Enterprise 2.0 applications. This includes embracing them for all their intended purposes and if needed proactively installing them or enabling them in a lab environment to see how they act. What also works well is engaging in peer discussions and asking other IT professionals for their input. Obviously that input needs to be based on facts rather than opinion (of which we know there is much!) A third good source of information is the Enterprise 2.0-focused web sites, message boards, blogs, and developer communities.

Ignoring the issue or acknowledging it exists but doing nothing about it until “something happens” can be a career limiting tact.

EMPLOYEE CONTROLS

The development of policy guidelines for the use of Enterprise 2.0 applications is often challenging as many examples are available but the high tension between risk and reward has polarized the opinions. At the core of the issue is that the two organizations that typically get involved—IT and HR—have in fact been sidelined during the adoption. To build a policy for safe use after the adoption has happened is nothing short of a monumental task.

Examples of policies are plenty, ranging from the extremely simple to the highly convoluted. On the simple side, Microsoft’s “Be Smart” is probably unbeatable. More complete policies can be found “in the wild” from companies such as IBM¹² and Intel¹³. In most cases, the Enterprise 2.0 guidelines are part of an overall code of conduct and privacy policy.

No matter what policy you develop, a few key elements need to be represented:

- Given the increasing number of “bad” applications, how will an employee know which applications are allowed and which are banned?

¹¹ [Charlene Li](#), Founder of Altimeter Group and Enterprise 2.0 expert

¹² [IBM Social Computing Guidelines](#)

¹³ [Intel Social Media Guidelines](#)

- 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?

Given that a large number of Enterprise 2.0 applications not only manifest themselves on the enterprise network or devices where they could be controlled, but also on the employees' mobile devices, documented employee policies need to be a key piece to the Enterprise 2.0 control puzzle. However, employee controls will remain largely ineffective as a stand-alone control mechanism for safe enablement of Enterprise 2.0 applications.

DESKTOP CONTROLS

Desktop controls traditionally present IT departments with significant challenges. Careful consideration is applied to the granularity of the desktop controls and the impact on employee productivity. As with employee policies, desktop controls are a piece to the safe enablement of Enterprise 2.0 applications in the enterprise. However, since 72% of Enterprise 2.0 applications are browser-based, the effectiveness of desktop controls is limited.

Even for the 28% of applications that run on the desktop, 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, an Enterprise 2.0 application could be accessed after the network admission was granted.

Desktop controls can complement the documented employee policies as a rather limited means to safely enable Enterprise 2.0 applications.

NETWORK CONTROLS

At the network level, what is needed is a means to identify Enterprise 2.0 applications and block or control them. By implementing network level controls, IT is able to minimize the possibility of threats and disruptions stemming from the use of Enterprise 2.0 applications. Several possible control mechanisms can be used at the network level, each of which carries 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 Enterprise 2.0 applications 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 understanding 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 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 an Enterprise 2.0 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 Enterprise 2.0 applications, look only at a portion of the traffic, and suffer from performance issues.

USING THE PALO ALTO NETWORKS NEXT-GENERATION FIREWALL

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 Enterprise 2.0 applications at the network level, complementing any existing desktop and employee control mechanisms.

App-ID™ accurately identifies more than 900 applications, including more than 200 Enterprise 2.0 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, Enterprise 2.0 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 ENTERPRISE 2.0 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 Enterprise 2.0 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 200 different Enterprise 2.0 applications.

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 Enterprise 2.0 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 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.

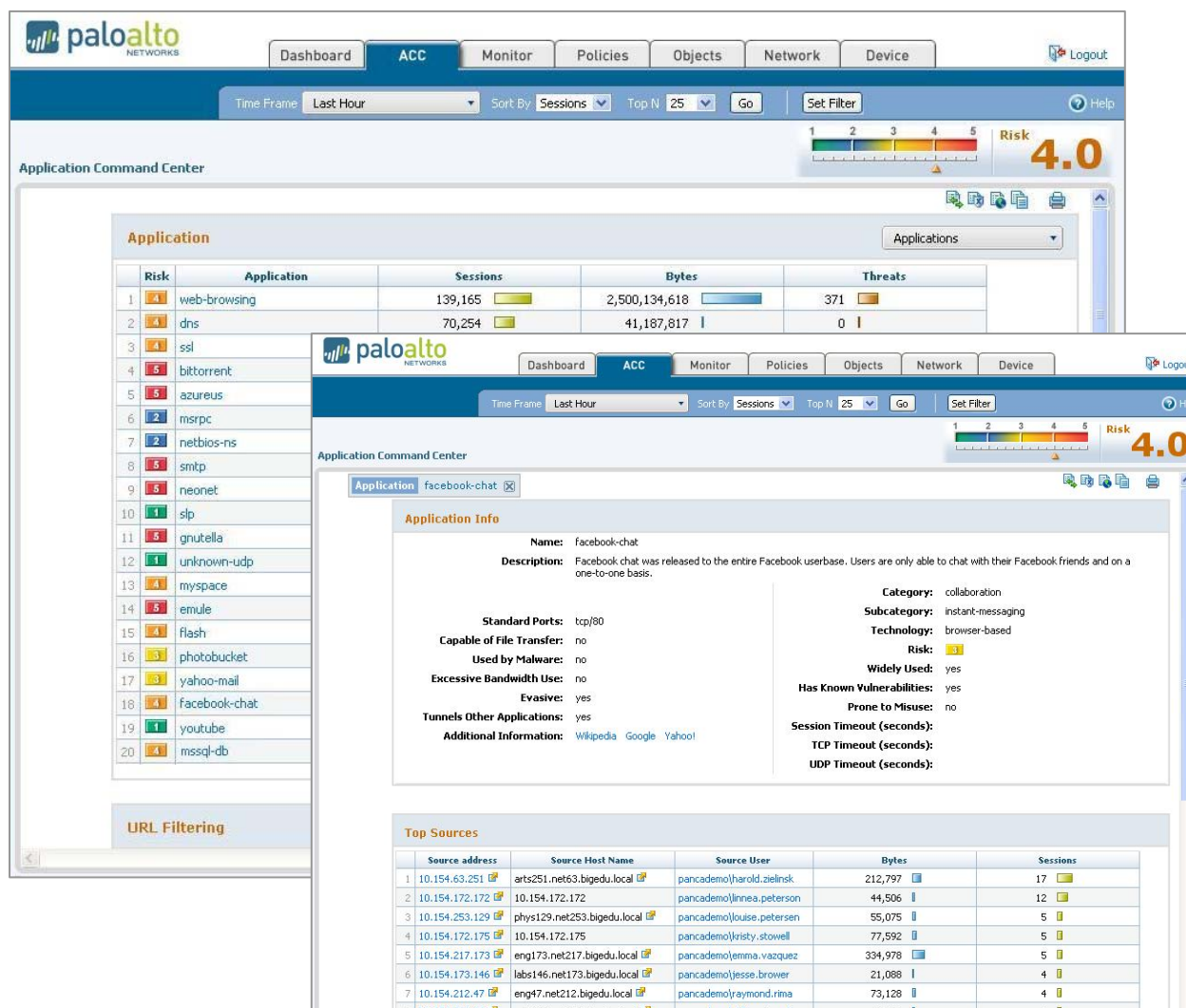


Figure 3: Application Command Center (background screen) provides a current view of application activity with drill down into specific applications such as Facebook Chat for additional details (foreground screen).

When App-ID™ identifies an Enterprise 2.0 application, the administrator can quickly see exactly which of those 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 Enterprise 2.0 application Facebook Chat, 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 Enterprise 2.0 applications are traversing the network, administrators can implement security policies from the policy editor similar to traditional firewalls.

APPLYING POSITIVE CONTROL (FIREWALL) POLICIES TO ENTERPRISE 2.0 APPLICATIONS

Once the Enterprise 2.0 application(s) have been identified, an administrator can use the rule-based editor to create an application usage control policy for applications like Facebook Chat. Or, to be safer and implement a wider net, the policy can be established against the Instant-Messaging group, thereby covering all instant-messaging applications currently identified. The advantage of selecting the Instant-Messaging group in the policy editor is that it catches all current as well as those that are added in the future. As the Palo Alto Networks development team adds new applications, they are automatically covered through the Palo Alto Networks dynamic update service.

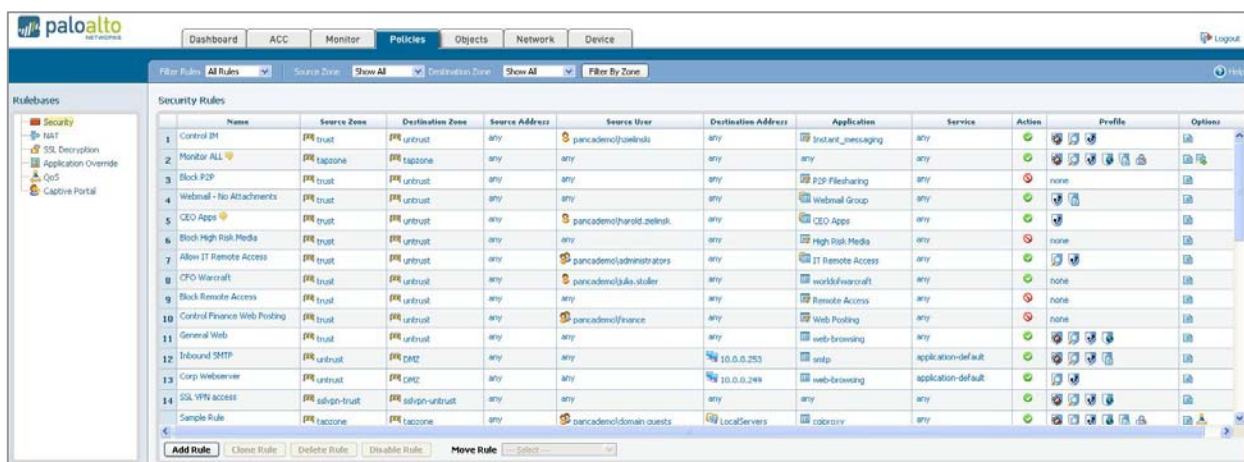
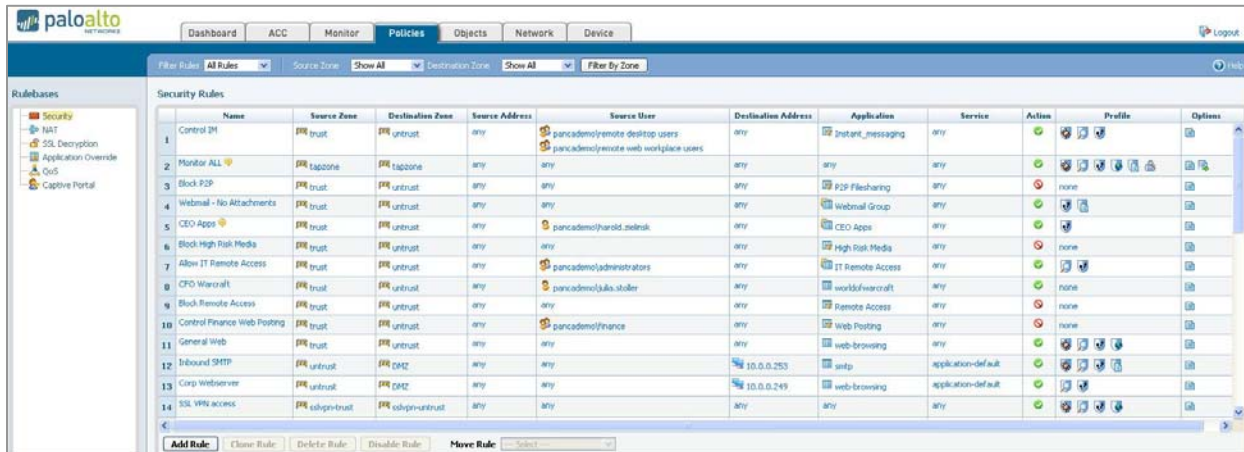


Figure 4: An individual's policy for instant messaging applications

In some cases, administrators will want to block all instant-messaging applications, while in others, such as when a company uses Facebook Chat to communicate with customers, they may wish to enforce specific rules to allow it - but only for key individuals. In that scenario, an application such as Facebook Chat can be selected, and then the specific users allowed to use it are selected based on their Active Directory information.



Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1 Control IM	trust	untrust	any	pancademo/remote desktop users; pancademo/remote web workplace users	any	instant_messaging	any	allow	none	Log, Alert, Deny, Allow
2 Monitor ALL	trust	trust	any	any	any	any	any	deny	none	Log, Alert, Deny, Allow
3 Block PDF	trust	untrust	any	any	any	PDF Filesharing	any	deny	none	Log, Alert, Deny, Allow
4 Webmail - No Attachments	trust	untrust	any	any	any	Webmail Group	any	deny	none	Log, Alert, Deny, Allow
5 CEO Apps	trust	untrust	any	pancademo/hardid_melink	any	CEO Apps	any	allow	none	Log, Alert, Deny, Allow
6 Block High Risk Media	trust	untrust	any	any	any	High Risk Media	any	deny	none	Log, Alert, Deny, Allow
7 Allow IT Remote Access	trust	untrust	any	pancademo/administrators	any	IT Remote Access	any	allow	none	Log, Alert, Deny, Allow
8 CFO Warcraft	trust	untrust	any	pancademo/julia.stoler	any	worldofwarcraft	any	deny	none	Log, Alert, Deny, Allow
9 Block Remote Access	trust	untrust	any	any	any	Remote Access	any	deny	none	Log, Alert, Deny, Allow
10 Control Finance Web Posting	trust	untrust	any	pancademo/finance	any	Web Posting	any	deny	none	Log, Alert, Deny, Allow
11 General Web	trust	untrust	any	any	any	web-browsing	any	allow	none	Log, Alert, Deny, Allow
12 Inbound SMTP	trust	DMZ	any	any	10.0.0.253	smtp	application-default	allow	none	Log, Alert, Deny, Allow
13 Corp Webserver	trust	DMZ	any	any	10.0.0.249	web-browsing	application-default	allow	none	Log, Alert, Deny, Allow
14 SSL VPN access	subvpn-trust	subvpn-untrust	any	any	any	any	any	allow	none	Log, Alert, Deny, Allow

Figure 5: A group policy for instant messaging applications

DEPLOYMENT FLEXIBILITY

Palo Alto Networks believes that the most appropriate place to control Enterprise 2.0 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 Palo Alto Networks Next-Generation Firewall to the network via a span port, IT can monitor traffic in real-time, providing the IT department with data that accurately describes which applications are traversing the network without disrupting the existing infrastructure.
- **Inline Transparent Mode:** Using Virtual Wire mode, the Palo Alto Networks Next-Generation Firewall 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 Palo Alto Networks Next-Generation Firewall can perform all of the same allow/deny functionality that existing firewalls can, allowing it to become the primary firewall solution.

CONCLUSION

Palo Alto Networks believes that the most appropriate place to control Enterprise 2.0 applications is at a strategic point in the network through which all traffic flows—the firewall. The question is not whether to block or not. Rather, the question is how companies define and enforce policies that allow for smart and safe enablement as there is ample evidence of the productivity and cost benefits of Enterprise 2.0 adoption around the world.

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, please visit <http://www.paloaltonetworks.com>.