

Application Visibility and Risk Report

Prepared for Federal Entity

Prepared by Matt Keil

Thursday, August 13, 2009

Palo Alto Networks
232 E. Java Street
Sunnyvale, CA 94089
Sales 866.207.0077
www.paloaltonetworks.com

Why Palo Alto Networks?

Federal Entity is evaluating the Palo Alto Networks next-generation firewalls as a means of enhancing their security posture through increased application visibility and control. Before delving into the results of the evaluation, it is important to review the key Palo Alto Networks differentiators that Federal Entity should consider as the evaluation process continues.

The Palo Alto Networks next generation firewall brings visibility and control over applications, users and content back to the IT department using three unique technologies: App-ID, User-ID and Content-ID. Delivered as a purpose-built platform, Palo Alto Networks next generation firewalls differentiate themselves from other security solutions in the following ways:

Application visibility and control with App-ID

The only firewall to use App-ID™, a patent-pending classification technology that uses four different mechanisms (application protocol detection and decryption, application decoding, application signatures, and heuristic analysis) to identify more than 800 applications irrespective of port, protocol, SSL encryption or evasive tactic employed. The identity of the application is then used as the basis of all firewall policy decisions as well as any applicable logging and reporting output.

It is important to note that existing firewalls use port and protocol as the only means of traffic classification which means that evasive applications can easily live up to their namesake, dynamically selecting an open port and passing quietly through the firewall, circumventing all manner of inspection. Or the application can emulate another application or use SSL and tunnel through the firewall unencumbered by security.

User visibility and control with User-ID

The only firewall to enable policy control over applications and content based on user and group information from within Microsoft's Active Directory (AD). User activity can be viewed across the entire feature set including Application Command Center (ACC), App-Scope, traffic logs, reporting as well as the policy editor.

Content inspection with Content-ID

Palo Alto Networks is the only firewall that melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing. Content-ID is hardware accelerated, obviating the need for typical performance vs. security trade-offs.

Powerful Visualization Tools and Unified Policy Control

A powerful set of visualization tools displays current application activity, activity over time and incident forensics is coupled with an easy-to-use policy interface that facilitates the creation and enforcement of granular appropriate usage policies. Rather than using cobbled together, hard-to-use management interfaces to set policies for disparate technologies, Palo Alto Networks uses a single policy to assemble all security rules including the matching criteria for the access control, threat prevention, URL filtering, logging, QoS and more. Building an application usage policy is as easy as building a music play list in iTunes – the application browser enables administrators to build a dynamic policy based on a wide range of application criteria including category, subcategory, underlying technology and behavioral characteristics. Most all of the competitive offerings will need multiple management interfaces to manage the disparate technologies that create basic security rules.

We believe that the Palo Alto Networks next-generation firewall will provide unmatched levels of visibility and control over the applications and threats traversing the network. The remainder of the document will focus on the findings of the recent analysis.

Summary and Key Findings

Palo Alto Networks conducted an application visibility and risk analysis for Federal Entity using the Palo Alto Networks next-generation firewall. Powered by three unique technologies App-ID, User-ID and Content-ID, the Palo Alto Networks next-generation firewall provides visibility into, and control over the applications, users and content traversing the network. This report summarizes the analysis beginning with key findings and an overall business risk assessment. Beyond that, the report analyzes Federal Entity traffic based on specific applications, the technical risks and threats, and provides a high level picture of how the network is being used. The report closes with a summary and recommended actions.

Key findings that should be addressed by Federal Entity:

Installation and use of personal applications is occurring. There are quite a few instances of end-user oriented, non-work related applications being used, elevating business risks.

Applications that can be used to conceal activity. Proxy and remote access were detected on the network. IT savvy employees are using these applications with increasing frequency to conceal activity. Visibility into who is using these applications and for what purpose should be investigated.

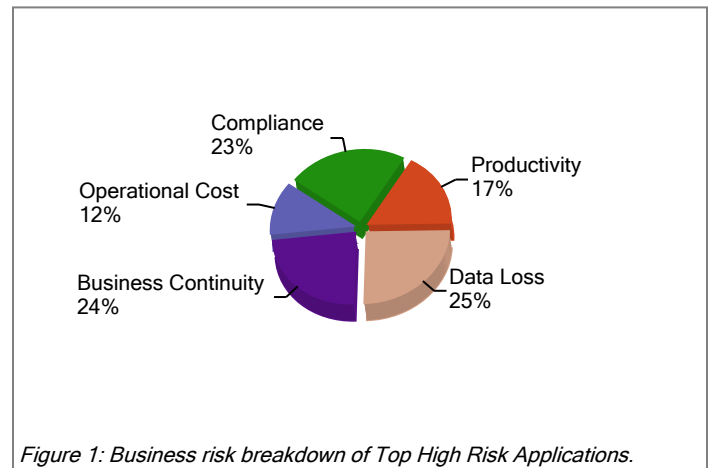
Applications that can lead to data loss. P2P and online file transfer applications are in use, exposing Federal Entity to significant security, data loss and possible copyright infringement risks.

Applications used for personal communications. Instant messaging applications, web mail applications, and VoIP applications were detected on the network. These types of applications expose Federal Entity to possible productivity loss, compliance and business continuity risks.

Bandwidth hogging, time consuming applications. Media and Social networking applications were detected on the network. Media and social networking applications are notorious consumers of corporate bandwidth and employee time.

Business Risks Introduced by High Risk Application Traffic

The potential business risks that can be introduced by the applications traversing the company network are determined by looking at the behavioral characteristics of the high risk applications (those that carry a risk rating of 4 or 5 on a scale of 1-5). Each of the behavioral characteristics equates to a business risk: application file transfer can lead to data leakage, ability to evade detection or tunnel other applications can lead to compliance risks, high bandwidth consumption equate to increased operational costs and whether it can be easily misused and is prone to malware or vulnerabilities introduce business continuity risks. A summary of business risk calculation is shown in figure 1 and a complete description of the risks can be found in Appendix A. Identifying the risks an application poses to company is the first step towards effectively managing the related business risks.



High Risk Applications in Use

The high risk applications (risk rating of 4 or 5) sorted by category, then by subcategory and by underlying technology are shown below. The ability to view the application along with its respective category, subcategory and technology can help determine the business value of the application and the risks they represent.

Key Findings on High Risk Applications:

Activity Concealment: proxy (2) and remote access (5) applications were found. IT savvy employees are using these applications with increasing frequency to conceal activity and in so doing, can expose Federal Entity to compliance and data loss risks.

File transfer/data loss/copyright infringement: P2P (5) applications and online file transfer (5) applications were found. These applications expose Federal Entity to data loss, possible copyright infringement and act as a threat vector.

Personal Communications: a combination of instant messaging, web mail and VoIP applications (20) were found. These types of applications expose Federal Entity to possible productivity loss, compliance and business continuity risks.

Bandwidth hogging: media applications, including photo/video (7), audio streaming (2) and social networking (3) applications were found. Media and social networking applications represent an employee productivity drain and can consume an inordinate amount of bandwidth.

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	concur	business-systems	general-business	browser-based	116,673	4
4	google-docs	business-systems	office-programs	browser-based	7,935,120	371
4	ms-groove	business-systems	office-programs	peer-to-peer	21,031	6
4	adobe-update	business-systems	software-update	client-server	355,699,610	555
4	ms-update	business-systems	software-update	client-server	1,452,291,623	23,921
4	mobile-me	business-systems	storage-backup	browser-based	5,715,885	44
4	outlook-web	collaboration	email	browser-based	431,338	3
4	secureserver-mail	collaboration	email	browser-based	4,503,825	153
4	yandex-mail	collaboration	email	browser-based	42,477	5
4	squirrelmail	collaboration	email	browser-based	6,922,610	271
4	gmail	collaboration	email	browser-based	741,323,000	44,931
4	hotmail	collaboration	email	browser-based	290,356,788	8,893
4	aim-mail	collaboration	email	browser-based	333,781,723	14,820
4	noteworthy	collaboration	email	browser-based	14,631	2
4	pop3	collaboration	email	client-server	73,210,576	41,693
4	ms-exchange	collaboration	email	client-server	51,361,600,601	1,377,793
5	smtp	collaboration	email	client-server	16,988,212,103	158,999
5	ebuddy	collaboration	instant-messaging	browser-based	10,003	1
4	aim-express	collaboration	instant-messaging	browser-based	43,802,347	3,342
5	jabber	collaboration	instant-messaging	client-server	114,906	2
4	yahoo-im	collaboration	instant-messaging	client-server	3,448,304	218
4	aim	collaboration	instant-messaging	client-server	736,948	97
4	gadu-gadu	collaboration	instant-messaging	client-server	6,821	4
4	icq	collaboration	instant-messaging	client-server	410,523	155
5	yahoo-file-transfer	collaboration	instant-messaging	peer-to-peer	11,569	1
5	msn-file-transfer	collaboration	instant-messaging	peer-to-peer	274,379	15
4	adobe-connect	collaboration	internet-conferencing	browser-based	2,235,907	228
4	facebook	collaboration	social-networking	browser-based	857,656,471	33,160
4	myspace	collaboration	social-networking	browser-based	94,601,591	1,508

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	spark	collaboration	social-networking	browser-based	10,355	5
4	yahoo-voice	collaboration	voip-video	peer-to-peer	2,851,301	98
5	skype	collaboration	voip-video	peer-to-peer	16,199,331	445
4	msn-voice	collaboration	voip-video	peer-to-peer	61,380	12
4	sip	collaboration	voip-video	peer-to-peer	2,385,722	5,843
4	yousendit	general-internet	file-sharing	browser-based	46,783,198	15
4	xdrive	general-internet	file-sharing	browser-based	63,715	2
4	docstoc	general-internet	file-sharing	browser-based	618,621	12
4	mediafire	general-internet	file-sharing	browser-based	2,378	2
5	webdav	general-internet	file-sharing	browser-based	6,191,373	2,405
5	ftp	general-internet	file-sharing	client-server	3,036,369,890	49,015
4	tftp	general-internet	file-sharing	client-server	263,826	2,424
5	emule	general-internet	file-sharing	peer-to-peer	2,494,905	560
5	soribada	general-internet	file-sharing	peer-to-peer	697,371	20
5	ares	general-internet	file-sharing	peer-to-peer	7,663	35
5	gnutella	general-internet	file-sharing	peer-to-peer	17,889,730	2,832
5	bittorrent	general-internet	file-sharing	peer-to-peer	73,777,431	206,613
4	flash	general-internet	internet-utility	browser-based	21,430,369,945	74,371
4	web-browsing	general-internet	internet-utility	browser-based	217,179,784,248	3,160,333
4	google-desktop	general-internet	internet-utility	client-server	57,811,872	10,524
4	atom	general-internet	internet-utility	client-server	20,838,909	285
5	rss	general-internet	internet-utility	client-server	378,851,329	16,476
5	http-audio	media	audio-streaming	browser-based	5,271,081,417	1,928
4	itunes	media	audio-streaming	client-server	1,184,210,324	604
4	zango	media	gaming	browser-based	997,772	40
4	limelight	media	photo-video	browser-based	9,453,489,993	7,769
5	youtube	media	photo-video	browser-based	11,763,698,737	7,212
5	http-video	media	photo-video	browser-based	1,551,966,211	4,700
4	rtmpt	media	photo-video	browser-based	79,111,726	1,586
5	asf-streaming	media	photo-video	browser-based	5,027,756,865	1,579
4	dailymotion	media	photo-video	browser-based	69,144,179	118
4	rtmp	media	photo-video	client-server	14,785,895,188	4,205
4	ssl	networking	encrypted-tunnel	browser-based	11,608,739,880	534,588
4	ssh	networking	encrypted-tunnel	client-server	3,696,336,678	2,625
4	dns	networking	infrastructure	network-protocol	8,745,605,084	15,591,453
4	icmp	networking	ip-protocol	network-protocol	484,197,796	2,111,693
5	http-proxy	networking	proxy	browser-based	26,638	16
5	cgiproxy	networking	proxy	browser-based	93,996	3
5	x11	networking	remote-access	client-server	15,650,647,237	46,846
4	ms-rdp	networking	remote-access	client-server	827,657,126	595
4	rsh	networking	remote-access	client-server	7,559	9
5	vnc	networking	remote-access	client-server	14,105,261	2
4	pptp	networking	remote-access	network-protocol	2,524,348	178

Figure 2: High risk applications sorted by category, subcategory and technology.

Application Characteristics That Determine Risk

The Palo Alto Networks research team uses the application behavioral characteristics to determine a risk rating of 1 through 5. The characteristics are an integral piece of the application visibility that administrators can use to learn more about a new application that they may find on the network and in turn, make a more informed decision about how to treat the application. Note that many applications carry multiple behavioral characteristics.

Application Behavioral Characteristics

Prone to misuse: used for nefarious purposes or is easily configured to expose more than intended. Examples include SOCKS, as well as newer applications such as DropBoks, AppleJuice and NEOnet.

Tunnels other applications: able to transport other applications. Examples include SSH and SSL as well as Hopster, TOR and RTSP, RTMPT.

Has known vulnerabilities: application has had known vulnerabilities.

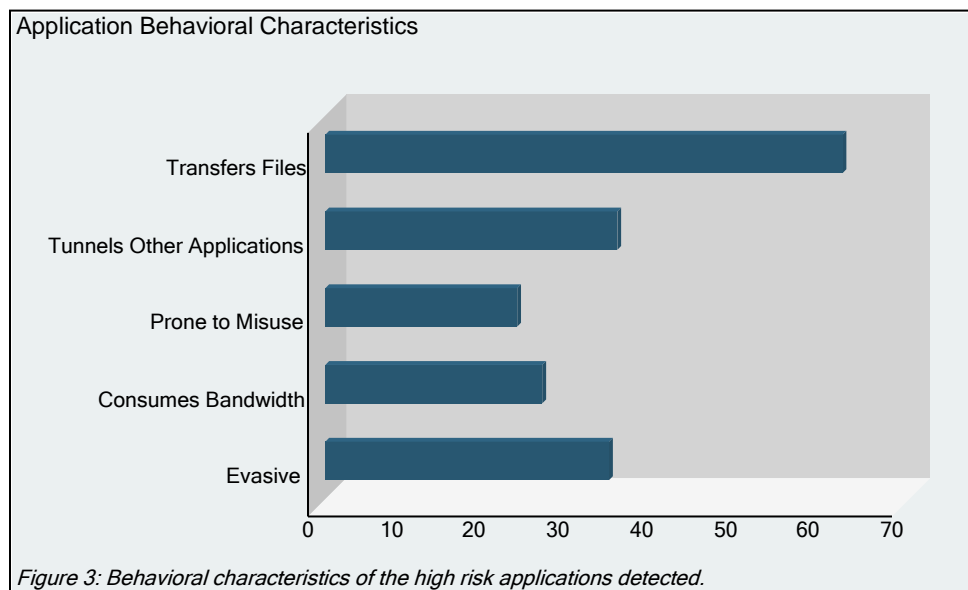
Transfers files: able to transfer files from one network to another. Examples include FTP and TFTP as well as webmail, online filesharing applications like Megaupload and YouSendIt.

Used by malware: has been used to propagate malware, initiate an attack or steal data. Applications that are used by malware include collaboration (email, IM, etc) and general Internet categories (file sharing, Internet utilities).

Consumes bandwidth: application consumes 1 Mbps or more regularly through normal use. Examples include P2P applications such as BitTorrent, Xunlei and DirectConnect as well as media applications, software updates and other business applications.

Evasive: uses a port or protocol for something other than its intended purpose with intent to ease deployment or hide from existing security infrastructure.

With the knowledge of which applications are traversing the network, their individual characteristics and which employees are using them, Federal Entity is enabled to more effectively decide how to treat the applications traffic through associated security policies.



Top Applications Traversing the Network

The top applications overall in terms of bandwidth consumed then sorted by category, subcategory and technology provide a high level view of the types of applications that are being used most commonly. The ability to view the application category, subcategory and technology is complemented by the behavioral characteristics (previous page), resulting in a more complete picture of the business benefit an application may provide.

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
2	ms-netlogon	business-systems	auth-service	client-server	31,453,218,831	328,515
2	ldap	business-systems	auth-service	client-server	4,739,582,471	944,995
2	kerberos	business-systems	auth-service	client-server	1,536,880,154	551,885
2	active-directory	business-systems	auth-service	client-server	1,144,635,530	155,502
2	mssql-db	business-systems	database	client-server	5,118,699,843	62,620
3	hp-jetdirect	business-systems	management	client-server	25,951,632,835	15,531
3	snmp	business-systems	management	client-server	3,100,960,768	10,342,856
3	ms-sms	business-systems	management	client-server	1,212,067,940	10,703
4	ms-update	business-systems	software-update	client-server	1,452,291,623	23,921
3	ms-ds-smb	business-systems	storage-backup	client-server	32,004,204,268	779,994
3	rsync	business-systems	storage-backup	client-server	11,461,679,515	42
4	ms-exchange	collaboration	email	client-server	51,361,600,601	1,377,793
5	smtp	collaboration	email	client-server	16,988,212,103	158,999
5	ftp	general-internet	file-sharing	client-server	3,036,369,890	49,015
4	web-browsing	general-internet	internet-utility	browser-based	217,179,784,248	3,160,333
4	flash	general-internet	internet-utility	browser-based	21,430,369,945	74,371
3	pandora	media	audio-streaming	browser-based	20,762,344,443	8,928
5	http-audio	media	audio-streaming	browser-based	5,271,081,417	1,928
4	itunes	media	audio-streaming	client-server	1,184,210,324	604
5	youtube	media	photo-video	browser-based	11,763,698,737	7,212
4	limelight	media	photo-video	browser-based	9,453,489,993	7,769
5	asf-streaming	media	photo-video	browser-based	5,027,756,865	1,579
5	http-video	media	photo-video	browser-based	1,551,966,211	4,700
3	photobucket	media	photo-video	browser-based	1,436,452,510	13,059
4	rtmp	media	photo-video	client-server	14,785,895,188	4,205
3	rtsp	media	photo-video	client-server	6,256,173,494	545
1	move-networks	media	photo-video	client-server	1,684,630,980	443
4	ssl	networking	encrypted-tunnel	browser-based	11,608,739,880	534,588
4	ssh	networking	encrypted-tunnel	client-server	3,696,336,678	2,625
2	msrpc	networking	infrastructure	network-protocol	34,005,496,011	3,527,231
1	lwapp	networking	infrastructure	network-protocol	15,372,151,829	10,967
4	dns	networking	infrastructure	network-protocol	8,745,605,084	15,591,453
2	netbios-ns	networking	infrastructure	network-protocol	5,025,217,528	4,887,431
5	x11	networking	remote-access	client-server	15,650,647,237	46,846
2	gre	networking	routing	network-protocol	23,129,369,119	106

Figure 4: Top applications that are consuming the most bandwidth, sorted by category, subcategory and technology.

Key observations on top 35 (out of 192) applications in use:

There is a wide range of business and non-business oriented applications in the top 35 applications overall. The most common types of applications are photo-video, auth-service and infrastructure.

Applications That Use HTTP

The HTTP applications report shows the applications found on the network that use HTTP in some way, shape or form. Many business applications use HTTP as a means to speed deployment and simplify access while non-business applications use it to bypass security. In cases where more granular controls are present, intrepid employees are using external proxies and circumventors to bypass controls. Knowing exactly which applications that use HTTP is a critical piece of a strong overall security posture.

Risk	HTTP Application	Bytes	Sessions
4	web-browsing	217,179,784,248	3,160,333
4	flash	21,430,369,945	74,371
5	youtube	11,763,698,737	7,212
4	limelight	9,453,489,993	7,769
3	rtsp	6,256,173,494	545
5	http-audio	5,271,081,417	1,928
1	move-networks	1,684,630,980	443
5	http-video	1,551,966,211	4,700
4	ms-update	1,452,291,623	23,921
3	photobucket	1,436,452,510	13,059
3	ms-sms	1,212,067,940	10,703
4	itunes	1,184,210,324	604
1	shoutcast	1,098,644,297	90
2	hulu	917,021,639	974
4	facebook	857,656,471	33,160
4	gmail	741,323,000	44,931
1	myspace-video	396,648,465	1,236
2	soap	382,390,479	110,170
5	rss	378,851,329	16,476
3	yahoo-mail	361,146,154	16,714
4	aim-mail	333,781,723	14,820
4	hotmail	290,356,788	8,893
2	google-safebrowsing	229,831,865	8,221
3	gmail-chat	200,100,502	5,501
3	imeem	130,182,101	466
2	xm-radio	107,763,640	23
4	myspace	94,601,591	1,508
3	zimbra	81,962,183	1,143
4	rtmpt	79,111,726	1,586
5	bittorrent	73,777,431	206,613

Figure 5: Top HTTP applications identified ranked in terms of bytes consumed.

Key observations on top 30 (out of 110) HTTP applications in use:

The report shows that the number of business applications such as MS-Update and SOAP are far outnumbered by the wide range of non-business applications which include photo-video, email, audio-streaming, internet-utility, social-networking, instant-messaging and file-sharing applications.

Top Threats Traversing the Network

The increased visibility into the traffic flowing across the network helps improve threat prevention by determining exactly which application may be transmitting the threat, not just the port and protocol. This increased visibility into the actual identity of the application means that the threat prevention engine can quickly narrow the number of potential threats down thereby accelerating performance. To further accelerate performance and improve accuracy, a uniform signature format is used to detect and block viruses, spyware, botnets, and vulnerability exploits in a single pass.

Threat Name	Type	Count
Samba NMBD_Packets.C NetBIOS Replies Stack-Based Buffer Overflow Vulnerability	vulnerability	17,266
Samba send_mailslot() Buffer Overflow Vulnerability	vulnerability	9,351
SMTP long RCPT to anomaly	vulnerability	1,018
MiniBug retrieve weather information	spyware phone home	670
RelevantKnowledge	spyware phone home	622
ISC BIND DNS Resolver Buffer Overflow Vulnerability	vulnerability	427
Hotbar_10_0_368 Get image Request	spyware phone home	312
SMTP long AUTH anomaly	vulnerability	275
ShopperReports Track/Upgrade/Report activities	spyware phone home	256
MiniBug check ads	spyware phone home	159
Microsoft Windows Print Spooler Buffer Overflow Vulnerability	vulnerability	137
Microsoft IIS 5.0 WebDAV Remote Buffer Overflow Vulnerability	vulnerability	81
MyWay_Speed_Bar Track activity 2	spyware phone home	46
ShopperReports Services requests	spyware phone home	29
Microsoft SQL Server INSERT Statement Buffer Overflow Vulnerability	vulnerability	14
BIND iquery buffer overflow Vulnerability	vulnerability	13
DNS Possible Nymex/Blackworm Activity	vulnerability	13
EarthLink_Toolbar Click toolbar News button links	spyware phone home	13
Apache Tomcat Directory Listing Information Disclosure	vulnerability	12
MyWay_Speed_Bar Ads	spyware phone home	10
MyWebSearch_Toolbar startup configuration	spyware phone home	7
MyWebSearch_Toolbar mysaconfg request	spyware phone home	5
NetBIOS Windows 2000 ADMIN Connect	vulnerability	5
Microsoft SQL Server TDS Packet Fragment Handling Vulnerability	vulnerability	3
HTTP: User Authentication Brute-force Attempt	recon attack	2
Double Content-Length HTTP Header Anomaly	vulnerability	2
Apple QuickTime Player H.264 Parsing Buffer Overflow Vulnerability	vulnerability	2
Hidden Iframe For Drive-By Download Web Exploitation	vulnerability	2
Samba LSA RPC LsarAddPrivilegesmCrafted Request Handling Heap Overflow	vulnerability	2
MSSQL xp_cmdshell execution	vulnerability	2

Figure 7: Top threats identified, sorted by count.

Key observations on the 30 most commonly detected threats (out of 34):

The Palo Alto Networks next-generation firewall is providing visibility into a wide range of spyware and application vulnerabilities traversing the network.

Application Usage by Category

As part of the traffic classification process, the Palo Alto Networks next-generation firewall identifies and categorizes the applications and technology traversing the network in terms of sessions and bandwidth. This data complements the granular application and threat data and provides a more complete summary of the types of applications and technology in use.

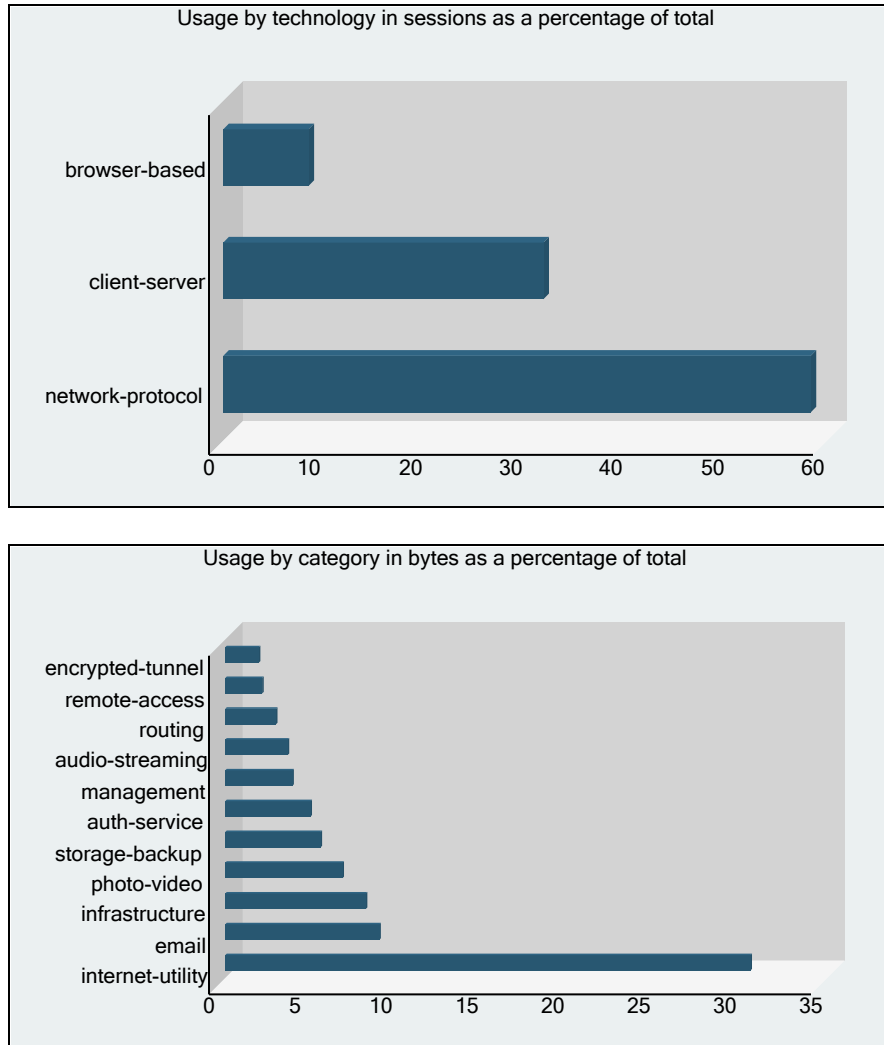


Figure 8: Application usage by category and by technology.

Key observations on application usage by category and technology:

During the evaluation phase, network-protocol consumed 58% of the sessions, indicating fairly heavy usage.

In terms of application usage by category, internet-utility applications consumed 31% of the overall bandwidth.

Findings:

During the planning phase for the Palo Alto Networks analysis the Federal Entity team explained that their environment is relatively open but the inability to see which applications were traversing the network was a clear concern due primarily to the limited visibility provided with the current infrastructure. The analysis uncovered the following items.

Proxies and remote access applications were found. Proxy and remote access applications were found on the network. These tools, commonly used by IT, are now being used by intrepid users to conceal their activity and bypass security.

P2P and online file transfer application usage. P2P and online file transfer/sharing applications were found, exposing Federal Entity to security, data loss and copyright infringement risks.

Media and social networking applications. There are a significant number of media and social networking applications running on the network. These applications represent significant challenges to IT – how to balance morale, recruitment and end-user satisfaction with productivity, threat exposure, compliance and data loss risks.

Use of Webmail, IM and VoIP. Many examples of these applications were found on the network and most of these applications can easily bypass firewalls and act as threat vectors as well as being an avenue for data leakage.

Recommendations:

Implement appropriate application usage and web surfing policies.

Like most organizations, Federal Entity lacks fine-grained policy governing application use - because it hasn't historically been necessary or enforceable. With the growth in user-controlled applications, their tendency to carry evasive characteristics, and the threats that take advantage of them, we recommend adjusting the appropriate use policies (AUP) to govern use on a per application or application category basis, now that such governance is both necessary and enforceable.

Address high risk areas such as P2P and online file transfer/sharing.

The risks associated with these applications may present problems for Federal Entity as employees use these applications to bypass existing traditional controls. Without understanding, categorizing, and mitigating risk in these areas, Federal Entity exposes itself possible unauthorized data transfer as well as the associated application level threats.

Implement policies dictating use of proxies and remote access applications.

These applications are sometimes used by employees who want to access their home machines and the applications on them. This represents possible threat vector as well as a productivity drain. Federal Entity should implement policies dictating the use of these applications. Possible options are to dictate which groups can use a specific proxy or remote access application and then block all others.

Regain control over media applications.

Federal Entity should look at applying policies to rein in the use of these applications without offending the user community. Possible options would be a time-based schedule, or QoS marking to limit consumption.

Seek Application Visibility and Control.

The only way to mitigate the application-level risk is first to have visibility of application traffic, then to understand it, and finally to be able to create and enforce policy governing it. There are a few technologies that offer some of the visibility required for certain types of applications, but only next-generation firewalls enable organizations to have visibility across all application traffic and offer the understanding, control, and scalability to suit enterprises. Accordingly, our recommendation involves deploying a Palo Alto Networks firewall in Federal Entity network and creating the appropriate application-granular policies to ensure visibility into application traffic and that the network is being used according to the organization's priorities.

Appendix A: Business Risk Definitions

When developing the risk analysis above, we looked at the potential impact the application could have on the enterprise and the processes within. Risks to the business break down into the following five categories.

Productivity:

Risk to productivity stems from misuse. This can take two forms:

- employees are using non-work-related applications instead of doing their job (e.g. Myspace, Facebook, personal email, blogging)
- non-work applications consume so much bandwidth that legitimate applications function poorly (e.g., YouTube, streaming/HTTP audio)

Compliance:

Most organizations must comply with an array of government and business regulations – in the US, this includes GLBA, HIPAA, FD, SOX, FISMA, and PCI. Most of these focus on safeguarding an organization's operational, financial, customer, or employee data. Certain applications represent significant threats to that information – either themselves or with the threats that target them (e.g., BitTorrent and MySpace, respectively). Any application that can transfer files (webmail, Skype, IM) can represent significant compliance issues.

Operational Costs:

Risks to operational costs come in two flavors – one, having applications and infrastructure that is used inappropriately to such an extent that more must be bought (e.g., WAN circuits upgraded due to streaming video) to ensure that business processes work, and two, incidents and exploits resulting in IT expense (e.g., rebuilding servers or networks following a security incident involving an exploit or virus).

Business Continuity:

Business continuity risks refer to applications (or the threats they carry) that can bring down or otherwise make unavailable critical components of certain business processes. Examples include email, transaction processing applications, or public facing applications harmed by threats or effectively denied service via excessive consumption of resources by non-business applications.

Data Loss:

The risk of data loss is the traditional information security set of risks – those associated with the theft, leakage, or destruction of data. Examples include many public thefts of customer data, theft or inadvertent leak of intellectual property, or destruction of data due to a security threat/breach. A variety of threats play a role, including exploits borne by applications (e.g., Facebook, Kazaa, IM, webmail), and non-business-related applications running on enterprise resources (e.g., BitTorrent, IM).

Appendix B: About Palo Alto Networks

Palo Alto Networks™ enables visibility and policy control of applications running on enterprise networks. Based on App-ID™, a patent pending traffic classification technology, the Palo Alto Networks next-generation firewalls accurately identify applications – regardless of port, protocol, SSL encryption or evasive tactic employed. Enterprises can now set and enforce application usage policies to meet compliance requirements, improve threat mitigation and lower operational costs. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks Next-Generation Firewalls

Palo Alto Networks' family of next-generation firewalls enables more effective risk management on enterprise networks by employing business-relevant elements such as applications, users, and content as the basis for policy control. With its next generation firewalls, Palo Alto Networks addresses key shortcomings that plague traditional Stateful Inspection-based firewalls--a reliance on port/protocol to identify the applications and the assumption that IP address equates to a users identity.

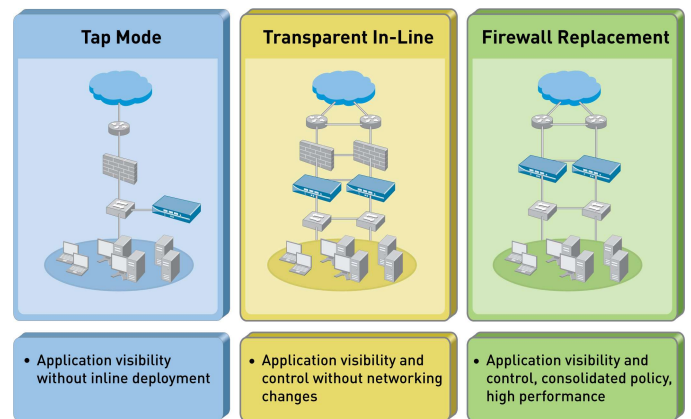
Palo Alto Networks uses App-ID to accurately identify the application, and maps the application to the user identity while inspecting the traffic for content policy violations. By focusing on business-relevant elements such as applications, users and content for policy controls, the security team can achieve the following business benefits:

- Manage risk through policy-based application usage control and threat prevention.
- Enable growth by embracing new, web-based applications in a controlled and secure manner.
- Facilitate operational efficiency by controlling application usage based on users and groups, not IP addresses.

With a rich networking foundation and a familiar policy management editor, the Palo Alto Networks firewalls can be deployed as a complement to, or as replacement for, an existing firewall implementation.

Key features:

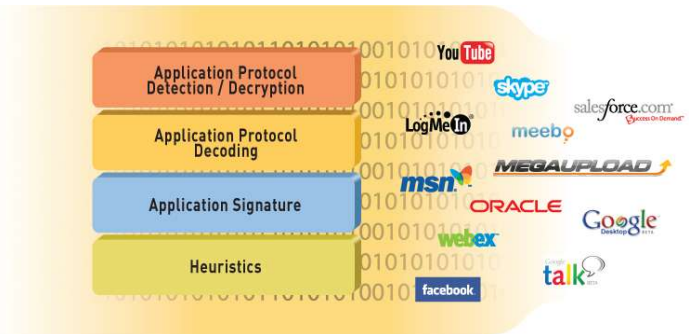
- **Application visibility and control:** Accurate identification of the applications traversing the network enables policy-based control over application usage.
- **SSL inspection:** Identifies and decrypts applications that use SSL, enabling policy-based control over the ever increasing amounts of SSL traffic.
- **Visualization tools:** Graphical visibility tools, customizable reporting and logging enables administrators to make a more informed decision on how to treat the applications traversing the network.
- **Policy-based application control:** The policy-editor takes full advantage of existing firewall knowledge to streamline creation and deployment of application usage control policies.
- **Legacy firewall support:** Support for traditional inbound and outbound port-based firewall rules mixed with application-based rules smoothes the transition to a Palo Alto Networks next generation firewall.
- **Application browser:** Helps administrators quickly research what the application is, its' behavioral characteristics and underlying technology resulting in a more informed decision making process on how to treat the application.
- **User-based visibility and control:** Seamless integration with Microsoft Active Directory (AD) facilitates application visibility and policy creation based on user and group information in AD, not just IP address.
- **Real-time threat prevention:** Detects and blocks viruses, spyware, worms and application vulnerabilities in real-time, dramatically improving performance and accuracy.
- **High performance:** Purpose-built platform with function-specific processing for networking, security, threat prevention and management delivers the performance required to protect today's high speed networks and eliminate security bottlenecks commonly associated with computationally intensive security applications.
- **Networking architecture:** Support for dynamic routing, site-to-site IPsec VPN, virtual wire mode and layer 2/layer 3 modes facilitates deployment in nearly any networking environment.



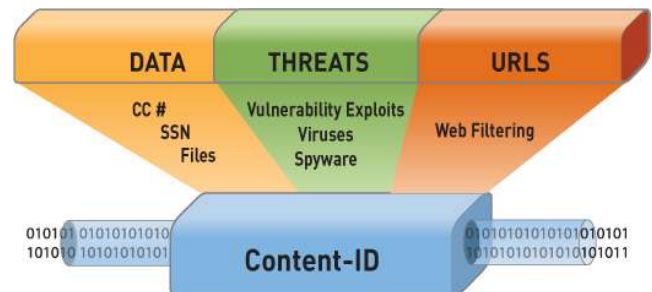
Key Palo Alto Networks Technologies

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

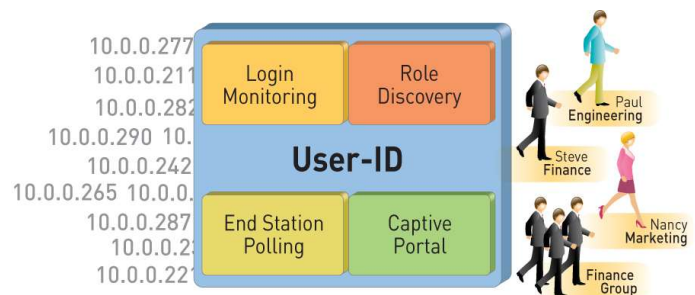
App-ID: Using as many as four different traffic classification mechanisms, App-ID™ accurately identifies exactly which applications are running on their network-irrespective of port, protocol, SSL encryption or evasive tactic employed. App-ID gives administrators increased visibility into the actual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



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



User-ID: Seamless integration with Microsoft Active Directory links the IP address to specific user and group information enabling IT organizations to monitor applications and content based on the employee information stored within Active Directory. User-ID allows administrators to leverage user and group data for application visibility, policy creation, logging and reporting.



Single Pass Parallel Processing Architecture: Manages multi-Gbps traffic flows using a single pass software engine that is tightly integrated with a parallel processing hardware platform containing function specific processing for networking, security, threat prevention and management. A 10 Gbps data plane smoothes traffic flow between processors and eliminates potential bottlenecks while the physical separation of control and dataplane ensures that management access is always available, irrespective of traffic load.

