Application Visibility and Risk Report

Prepared for: Sample Customer

Prepared by: Palo Alto Networks

August 10, 2010

Palo Alto Networks
232 E. Java Dr
Sunnyvale, Ca
94089

Why Palo Alto Networks?

Sample Customer 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 capabilities that Sample Customer 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 the applications traversing the network, 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 enterprise directory services (Active Directory, eDirectory, LDAP). 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 are 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 editor to assemble all security rules, including the matching criteria for 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 dynamically filter the application database using 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 Sample Customer 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 Sample Customer 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 Sample Customer:

Personal applications are being installed and used on the network.
End-users are installing and using a variety of non-work related applications that can elevate business and security risks.

Applications that can be used to conceal activity were found.
IT savvy employees are using applications that can conceal their activity. Examples of these types of applications include external proxies, remote desktop access and non-VPN related encrypted tunnel. Visibility into who is using these applications, and for what purpose should be investigated.

Applications that can lead to data loss were detected.
File transfer applications (peer-to-peer and/or browser-based) are in use, exposing Sample Customer to significant security, data loss, compliance and possible copyright infringement risks.

Applications used for personal communications were found.
Employees are using a variety of applications that enable personal communications. Examples include instant messaging, webmail, and VoIP/video conferencing. These types of applications can introduce productivity loss, compliance and business continuity risks.

Bandwidth hogging, time consuming applications are in use.
Media and social networking applications were found. Both of these types of applications are known to consume 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 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 can introduce business risks. Application file transfer can lead to data leakage; ability to evade detection or tunnel other applications can lead to compliance risks; high bandwidth consumption equates to increased operational costs and applications that are prone to malware or vulnerabilities can introduce business continuity risks. Identifying the risks an application poses to is the first step towards effectively managing the related business risks.

A summary of the business risk calculation is shown in figure 1. Appendix A has a complete description of the business risks.
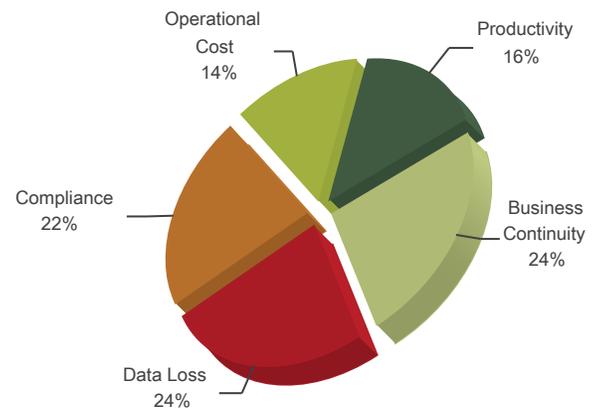

Figure 1: Business risk breakdown of Top High Risk Applications

Top High Risk Applications in Use

The high risk applications (risk rating of 4 or 5) sorted by category, subcategory and bytes consumed are shown below. The ability to view the application along with its respective category, subcategory and technology can be useful when discussing the business value and the potential risks that the applications pose with the respective users or groups of users.

Key observations on the 44 high risk applications:

Activity Concealment:
Proxy (1) and remote access (1) applications were found. IT savvy employees are using these applications with increasing frequency to conceal activity and in so doing, can expose Sample Customer to compliance and data loss risks.

File transfer/data loss/copyright infringement:
P2P applications (11) and browser-based file sharing applications (21) were found. These applications expose Sample Customer to data loss, possible copyright infringement, compliance risks and can act as a threat vector.

Personal communications:
A variety of applications that are commonly used for personal communications were found including instant messaging (1), webmail (7), and VoIP/video (3) conferencing. These types of applications expose Sample Customer to possible productivity loss, compliance and business continuity risks.

Bandwidth hogging:
Applications that are known to consume excessive bandwidth including photo/video (3), audio (2) and social networking (1) were detected. These types of applications represent an employee productivity drain and can consume excessive amounts of bandwidth and can act as potential threat vectors.

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	ms-update	business-systems	software-update	client-server	18,782,971	80
5	smtp	collaboration	email	client-server	433,023,390	50,088
4	hotmail	collaboration	email	browser-based	57,137,438	9,603
4	pop3	collaboration	email	client-server	8,397,015	3,757
4	imap	collaboration	email	client-server	7,076,029	975
4	outlook-web	collaboration	email	browser-based	1,496,961	259
4	mail.ru	collaboration	email	browser-based	668,214	328
4	mail.com	collaboration	email	browser-based	379,209	113
4	aim-mail	collaboration	email	browser-based	281,338	19
4	squirrelmail	collaboration	email	browser-based	146,058	52
4	netease-mail	collaboration	email	browser-based	9,284	4
4	qq	collaboration	instant-messaging	client-server	2,652	1
4	plaxo	collaboration	social-networking	browser-based	87,519	114
4	yahoo-voice	collaboration	voip-video	peer-to-peer	191,086	187
4	msn-voice	collaboration	voip-video	peer-to-peer	2,294	4
5	skype	collaboration	voip-video	peer-to-peer	600	5
5	bittorrent	general-internet	file-sharing	peer-to-peer	653,958,615	39,490
5	gnutella	general-internet	file-sharing	peer-to-peer	63,525,411	195,463
5	emule	general-internet	file-sharing	peer-to-peer	58,486,566	337,272
4	megaupload	general-internet	file-sharing	browser-based	44,527,276	2,883
5	azureus	general-internet	file-sharing	peer-to-peer	33,509,645	163,912
5	ftp	general-internet	file-sharing	client-server	8,730,742	4,932
5	ares	general-internet	file-sharing	peer-to-peer	3,895,002	796
5	xunlei	general-internet	file-sharing	peer-to-peer	920,580	9
5	webdav	general-internet	file-sharing	browser-based	245,285	101
5	neonet	general-internet	file-sharing	peer-to-peer	88,008	881
4	sendspace	general-internet	file-sharing	browser-based	58,923	8
5	kazaa	general-internet	file-sharing	peer-to-peer	5,440	10
4	web-browsing	general-internet	internet-utility	browser-based	2,310,667,405	659,246
4	web-crawler	general-internet	internet-utility	browser-based	53,123,691	9,227
4	google-desktop	general-internet	internet-utility	client-server	548,439	366
4	flash	general-internet	internet-utility	browser-based	16,610	1
5	http-audio	media	audio-streaming	browser-based	29,016,462	184
4	itunes	media	audio-streaming	client-server	190,326	120
4	zango	media	gaming	browser-based	1,294	1
5	asf-streaming	media	photo-video	browser-based	65,430,274	606
4	metacafe	media	photo-video	browser-based	443,159	119
4	rtmp	media	photo-video	browser-based	48,152	11
4	ssl	networking	encrypted-tunnel	browser-based	1,256,990,820	341,179
4	ssh	networking	encrypted-tunnel	client-server	9,409	1
4	dns	networking	infrastructure	network-protocol	459,674,387	997,988
4	icmp	networking	ip-protocol	network-protocol	23,352,636	145,830
5	http-proxy	networking	proxy	browser-based	7,651,209	425
4	pptp	networking	remote-access	network-protocol	39,734	7

Figure 2: High risk applications (rating of 4 or 5) that are traversing the network.

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.

Application Behavioral Characteristic Definitions

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 BitTorrent and AppleJuice.

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 – and typically, exploits.

Transfers files: Able to transfer files from one network to another. Examples include FTP and P2P 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 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, Sample Customer is enabled to more effectively decide how to treat the applications traffic through associated security policies. Note that many applications carry multiple behavioral characteristics.
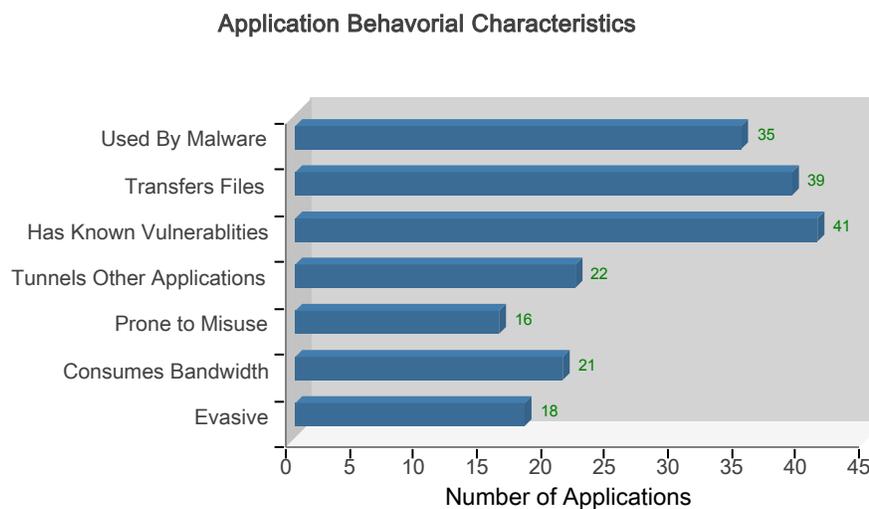
Application Behavorial Characteristics

Characteristic	Number of Applications
Used By Malware	35
Transfers Files	39
Has Known Vulnerablities	41
Tunnels Other Applications	22
Prone to Misuse	16
Consumes Bandwidth	21
Evasive	18

Figure 3: Behavioral characteristics of the high risk applications detected

Top Applications Traversing the Network

The top 35 applications (based on bandwidth consumption), sorted by category and subcategory are shown below. 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	ldap	business-systems	auth-service	client-server	4,119,884	233
2	oracle	business-systems	database	client-server	100,937,010	263
2	ntp	business-systems	general-business	network-protocol	9,155,660	41,559
1	mcafee	business-systems	software-update	client-server	30,483,048	2,538
4	ms-update	business-systems	software-update	client-server	18,782,971	80
5	smtp	collaboration	email	client-server	433,023,390	50,088
3	yahoo-mail	collaboration	email	browser-based	237,586,873	14,115
4	hotmail	collaboration	email	browser-based	57,137,438	9,603
4	pop3	collaboration	email	client-server	8,397,015	3,757
4	imap	collaboration	email	client-server	7,076,029	975
3	comcast-webmail	collaboration	email	browser-based	4,988,629	1,086
3	gmail-chat	collaboration	instant-messaging	browser-based	5,465,603	337
3	livejournal	collaboration	social-networking	browser-based	4,808,459	594
5	bittorrent	general-internet	file-sharing	peer-to-peer	653,958,615	39,490
5	gnutella	general-internet	file-sharing	peer-to-peer	63,525,411	195,463
5	emule	general-internet	file-sharing	peer-to-peer	58,486,566	337,272
4	megaupload	general-internet	file-sharing	browser-based	44,527,276	2,883
5	azureus	general-internet	file-sharing	peer-to-peer	33,509,645	163,912
5	ftp	general-internet	file-sharing	client-server	8,730,742	4,932
4	web-browsing	general-internet	internet-utility	browser-based	2,310,667,405	659,246
4	web-crawler	general-internet	internet-utility	browser-based	53,123,691	9,227
2	google-safebrowsing	general-internet	internet-utility	browser-based	21,042,714	163
2	ping	general-internet	internet-utility	network-protocol	20,939,438	110,078
5	http-audio	media	audio-streaming	browser-based	29,016,462	184
3	pandora	media	audio-streaming	browser-based	9,039,456	95
5	asf-streaming	media	photo-video	browser-based	65,430,274	606
3	photobucket	media	photo-video	browser-based	52,849,132	13,623
3	rtsp	media	photo-video	client-server	40,532,962	465
4	ssl	networking	encrypted-tunnel	browser-based	1,256,990,820	341,179
4	dns	networking	infrastructure	network-protocol	459,674,387	997,988
2	msrpc	networking	infrastructure	network-protocol	201,683,796	404,532
2	netbios-ns	networking	infrastructure	network-protocol	54,190,592	463,919
1	slp	networking	infrastructure	network-protocol	50,411,272	15,347
4	icmp	networking	ip-protocol	network-protocol	23,352,636	145,830
5	http-proxy	networking	proxy	browser-based	7,651,209	425

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

Key observations on top 35 (out of 123) applications in use:

The most common types of applications are email and file-sharing.

Application Subcategories

The subcategory breakdown of all the applications found, sorted by bandwidth consumption provides an excellent summary of where the application usage is heaviest. These data points can help IT organizations more effectively prioritize their application enablement efforts.

Sub-Category	Number of Applications	Bytes Consumed	Sessions Consumed
internet-utility	11	2,408,961,154	779,359
encrypted-tunnel	2	1,257,000,229	341,180
file-sharing	12	867,951,493	745,757
infrastructure	8	770,456,381	1,885,065
email	12	751,190,438	80,399
photo-video	12	160,436,138	15,131
database	1	100,937,010	263
software-update	5	50,662,410	3,022
audio-streaming	8	38,694,131	521
ip-protocol	3	23,420,862	146,628
social-networking	7	10,976,541	1,382
general-business	2	9,800,272	41,648
proxy	1	7,651,209	425
auth-service	3	7,246,732	16,984
instant-messaging	4	5,597,775	358
management	5	2,303,288	2,270
voip-video	4	1,690,012	5,672
remote-access	2	1,047,197	70
gaming	4	878,468	502
storage-backup	2	476,050	16
office-programs	1	262,624	38
web-posting	1	259,340	19
routing	1	79,740	69
erp-crm	1	14,150	10
Grand Total	**112**	**6,477,993,644**	**4,066,788**

Figure 5: Subcategory breakdown of all the applications found, sorted by bytes consumed.

Key observations on application subcategories:

The application subcategories that are consuming the highest amount of bandwidth are: internet-utility, encrypted-tunnel, file-sharing.

Applications That Use HTTP

The top 25 applications (based on bandwidth consumed) that use HTTP in some way, shape or form are shown below. Many business applications use HTTP as a means to speed deployment and simplify access while non-business applications may use it to bypass security. Knowing exactly which applications that use HTTP is a critical datapoint when assembling an application enablement policy.

Risk	HTTP Application	Technology	Bytes	Sessions
4	web-browsing	browser-based	2,310,667,405	659,246
5	bittorrent	peer-to-peer	653,958,615	39,490
3	yahoo-mail	browser-based	237,586,873	14,115
2	msrpc	network-protocol	201,683,796	404,532
5	asf-streaming	browser-based	65,430,274	606
5	gnutella	peer-to-peer	63,525,411	195,463
5	emule	peer-to-peer	58,486,566	337,272
4	hotmail	browser-based	57,137,438	9,603
4	web-crawler	browser-based	53,123,691	9,227
3	photobucket	browser-based	52,849,132	13,623
4	megaupload	browser-based	44,527,276	2,883
3	rtsp	client-server	40,532,962	465
5	azureus	peer-to-peer	33,509,645	163,912
1	mcafee	client-server	30,483,048	2,538
5	http-audio	browser-based	29,016,462	184
2	google-safebrowsing	browser-based	21,042,714	163
4	ms-update	client-server	18,782,971	80
3	pandora	browser-based	9,039,456	95
5	http-proxy	browser-based	7,651,209	425
3	gmail-chat	browser-based	5,465,603	337
3	comcast-webmail	browser-based	4,988,629	1,086
3	livejournal	browser-based	4,808,459	594
2	classmates	browser-based	3,909,540	5
5	ares	peer-to-peer	3,895,002	796
3	friendster	browser-based	1,902,603	556

Figure 6: Top HTTP applications identified ranked in terms of bytes consumed.

Key observations on top 25 (out of 82) HTTP applications in use:

There is a mix of both work and non-work related applications traversing the network that can use HTTP in some way or another.

Top URL Categories in Use

Another aspect to consider regarding visibility into application traffic is the identification and subsequent control of the websites users are visiting. URL filtering controls, combined with application control and threat prevention can dramatically improve network security.

URL Category	Count
adult-and-pornography	71,431
spyware-and-adware	26,739
online-gambling	1,010
questionable	1,000
weapons	100
social-networking	55
web-advertisements	30
unknown	18
shareware-and-freeware	6
block-list	3

Figure 7: Top URL categories visited

Key observations on the top 25 most frequently visited URLs:

The URL category report shows a mix of work and non-work related web activity.

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.

Threat Name	Type	Severity	Count
MiniBug check ads	spyware phone home	medium	73
Hotbar_10_0_368 disp .dll requests	spyware phone home		49
FTP evasion attack	vulnerability	critical	19
Lop Collect informtation request 1	spyware phone home	low	18
Bot: Swizzor phone home activity	spyware phone home	critical	18
Novell ZENworks Remote Management Buffer Overflow	vulnerability	critical	16
WebFerret 2 updating from website	spyware phone home	medium	10
WebFerret 1 searching keyword	spyware phone home	medium	10
WeatherStudio runtime detection	spyware phone home	medium	8
HTTP Basic Authentication String Over Long	vulnerability	high	6
WhenU_FanzoneToolbar Search Request 2	spyware phone home	low	4
Girafa_Toolbar search hijack search hijack	spyware phone home	medium	4
Excite_Search_bar	spyware phone home		3
MyWay_Speed_Bar Switch engines	spyware phone home	low	3
MyWay_Speed_Bar Track activity 2	spyware phone home	low	3
CA BrightStor ARCServe Backup Agent For MSSQL Server Buffer Overflow	vulnerability	high	3
MyWay_Speed_Bar Track activity 1	spyware phone home	low	3
Starware_Toolbar Update	spyware phone home	medium	2
Comet_Systems log report	spyware phone home	medium	2
Email-Worm/Win32.Klez.a	virus	medium	2
Comet_Systems Update requests Track activity	spyware phone home	medium	2
ShopperReports Track/Upgrade/Report activities	spyware phone home	medium	1
Win_Anti_Virus_Pro_2007	spyware phone home		1
MyWebSearch_Toolbar startup configuration	spyware phone home	medium	1
MyWay_Speed_Bar Ads	spyware phone home	low	1

Figure 8: Top threats identified, sorted by count.

**Key observations on the 25 most commonly detected (out of 30) threats:**

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

Of the 30 individual threats found, 10% are critical, 10% are high and 33% are medium severity. The remainder are low severity or informational.

Application Usage by Underlying Technology and Category

The resource consumption (sessions and bytes) of the applications based on underlying technology and subcategory are shown in the charts below. This data complements the granular application and threat data to provide a more complete summary of the types of applications, based on sub-category and underlying technology in use.

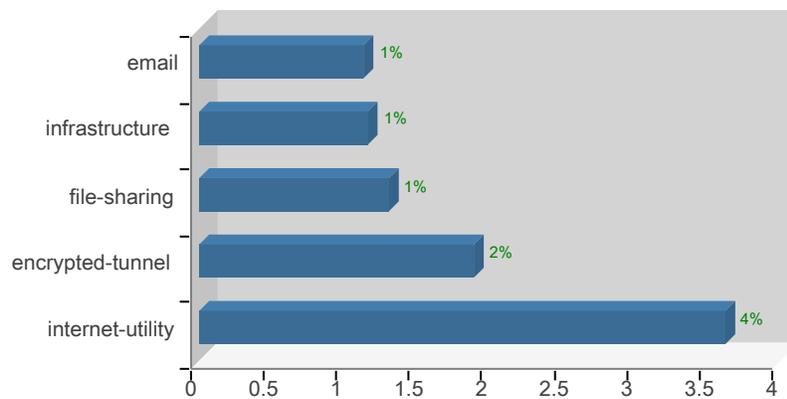Usage by technology in sessions as a percentage of total
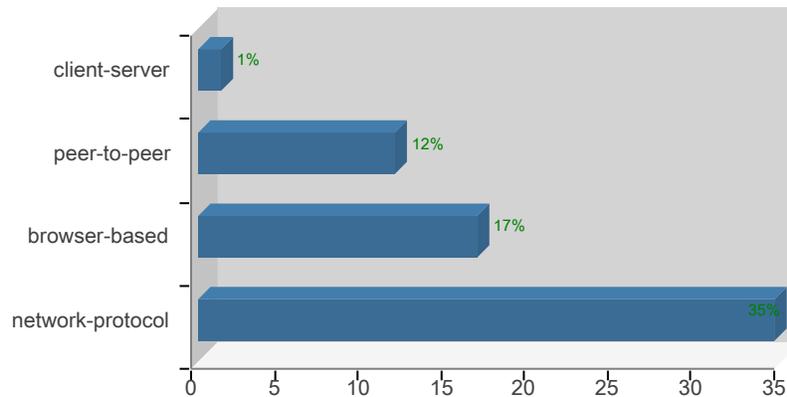
Usage by category in bytes as a percentage of total

Figure 9: Application usage by category and by technology.

Key observations on application usage by category and technology:

During the evaluation, network-protocol applications consumed 35% of the sessions.

In terms of application usage by category, internet-utility applications consumed 4% of the overall bandwidth.

Findings:

During the planning phase for the Palo Alto Networks analysis, the Sample Customer team explained that their environment is relatively open but the inability to see which applications were traversing the network introduces a wide range of business and security risks. The analysis uncovered the following items.

Activity concealment applications were found. Activity concealment applications were found on the network. IT savvy users are now using these applications to conceal their activity and bypass security.

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

Media and social networking application usage. Applications that are used for entertainment and socializing (media, audio, social networking) were found on the network. These applications represent significant challenges to IT – how to balance morale, recruitment/retention and end-user satisfaction with productivity, threat exposure, compliance, and data loss risks.

Use of Webmail, IM and VoIP. Examples of these applications were found on the network. Many 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, Sample Customer 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 Sample Customer as employees use these applications to bypass existing traditional controls. Without understanding, categorizing, and mitigating risk in these areas, Sample Customer exposes itself to 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 a possible threat vector as well as a productivity drain. Sample Customer 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
Sample Customer 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 Sample Customer 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™ is the network security company. Its next-generation firewalls provide visibility and policy control over applications, users and content. Enterprises can use a Palo Alto Networks next-generation firewall to implement appropriate application usage policies to meet compliance requirements, improve threat mitigation and lower operational costs.

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.

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.

Palo Alto Networks next-generation firewalls can be deployed as a complement to, or as replacement for, an existing firewall implementation.
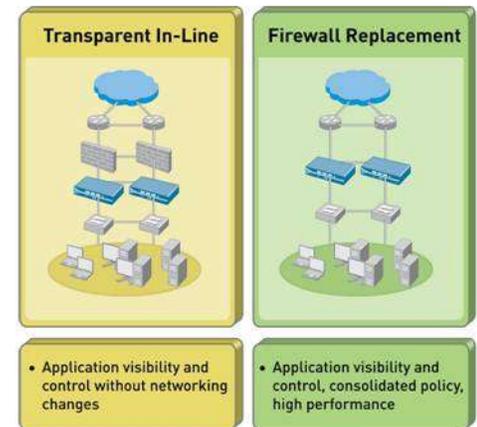
Key features:

- **Application visibility and control:** Accurate identification of the applications traversing the network enables policy-based control over application usage at the firewall, the strategic center of the security infrastructure.
- **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.
- **User-based visibility and control:** Seamless integration with enterprise directory services facilitates application visibility and policy creation based on user and group information, not just IP address.
- **Real-time threat prevention:** Detects and blocks application vulnerabilities, viruses, spyware, and worms; controls web activity; all in real-time, dramatically improving performance and accuracy.
- **File and data filtering:** Administrators can implement several different types of policies that reduce the risk associated with unauthorized file and data transfer.
- **Networking architecture:** Support for dynamic routing (OSPF, RIP, BGP), virtual wire mode and layer 2/layer 3 modes facilitates deployment in nearly any networking environment.
- **Policy-based forwarding:** Forward traffic based on policy defined by application, source zone/interface, source/destination address, source user/group, and service.
- **Virtual systems:** Create multiple virtual "firewalls" within a single device as a means of supporting specific departments or customers. Each virtual system can include dedicated administrative accounts, interfaces, networking configuration, security zones, and policies for the associated network traffic.
- **VPN connectivity:** Secure site-to-site connectivity is enabled through standards-based IPSec VPN support while remote user access is delivered via SSL VPN connectivity.
- **Quality of Service (QoS):** Deploy traffic shaping policies (guaranteed, maximum and priority) to enable positive policy controls over bandwidth intensive, non-work related applications such as streaming media while preserving the performance of business applications.
- **Real-time bandwidth monitor:** View real-time bandwidth and session consumption for applications and users within a selected QoS class.

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.
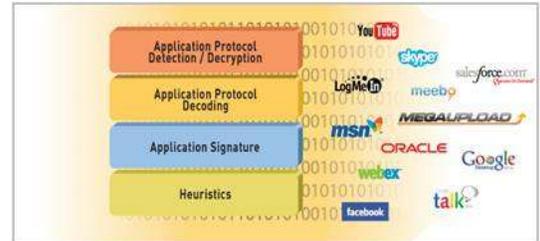

User-ID: Seamless integration with enterprise directory services such as Active Directory, eDirectory, LDAP, and Citrix enables administrators to view and control application usage based on individual users and groups of users, as opposed to just IP addresses. User information is pervasive across all features including application and threat visibility, policy creation, forensic investigation, and reporting.
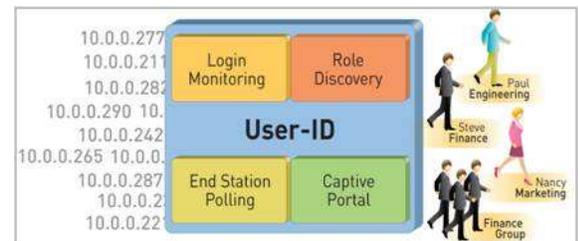
Content-ID: A stream-based scanning engine that uses a uniform threat signature format detects and blocks a wide range of threats and limits unauthorized transfer of files and sensitive data (CC# and SSN) while a comprehensive URL database controls non-work related web surfing. The application visibility 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.
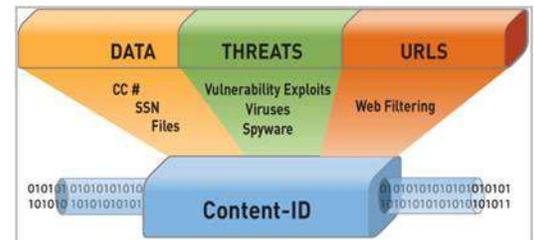
Single Pass Parallel Processing Architecture: Manages multi-Gbps traffic flows using a single pass software engine that is tightly integrated with a parallel processing hardware platform containing function specific processing for networking, security, threat prevention and management. A 10 Gbps data 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.
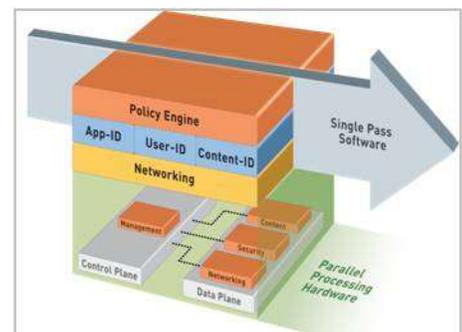
Appendix C: Additional Information

This page can be used to insert added information about the partner, the customer environment, the sales team, possible next steps, deployment plans or other important data points.