

Application Visibility and Risk Report

A tool for closing more business!



What is an AVR Report?

- Helps close more business
 - Builds a powerful business case for Palo Alto Networks with C-level audiences
 - Makes our solution a must have, not a nice to have
 - Use it early to gain commitment for a C-level meeting / economic buyer - PRIOR to installing the evaluation



Application Visibility and Risk Report

Prepared for Company X

Prepared by Palo Alto Networks

Friday, March 20, 2009

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

Key Elements in an AVR Report

- Summary of the findings
 - Key facts on what was found
- Details of the findings
 - Details on applications, threats, bandwidth, URLs
- Recommended actions
 - Compares the existing policies with what was found

Summarizes what was found...

- Tells the budget holder what we are going to review
- Presents findings in clear, business oriented manner
- Introduces business risks associated with the application traffic



Summary and Key Findings

Palo Alto Networks conducted an application visibility and risk analysis for Company X 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 Company X 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 Company X:

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, remote access and encrypted tunneling (eg TOR, Hamachi) 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.

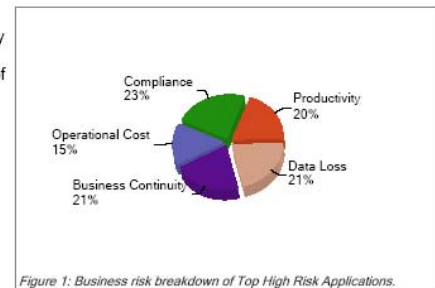
Applications that can lead to data loss. P2P and online file transfer applications are in use, exposing Company X to significant security, data loss and possible copyright infringement risks.

Applications used for personal communications. Instant messaging applications, web mail applications, and VoIP applications were detected on the network. These types of applications expose Company X 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.



Details on the findings...

- Delivers details on what was found
- Top applications
- Top high risk applications
- URLs, Threats, bandwidth consumption

High Risk Applications in Use

The high risk applications (risk rating of 4 or 5 shown below). The ability to view the applications determine the business value of the applications.

Key Findings on High Risk Applications

Activity Concealment: proxy was also found. IT savvy employees doing, can expose Company X

File transfer/data loss/copy: found. These applications expose

Personal Communications: These types of applications expose

Bandwidth hogging: media applications were found. Media consume an inordinate amount

Risk	Application
4	editgrid
4	google-docs
4	evernote
4	ms-groove
4	ms-update
4	adobe-update
4	mobile-me
4	sosbackup
5	horde
4	outlook-web
4	roundcube
4	gmail
4	netease-mail
4	fastmail
4	aim-mail
4	outblaze-mail
4	squirrelmail
4	mail.com
4	qq-mail
4	mail.ru
4	hotmail
4	yandex-mail
4	secureserver-mail
4	imap
5	smtp
4	pop3
4	ms-exchange
4	twig
4	aim-express
5	ebuddy

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
MiniBuo retrieves weather information	software.phone.home	4,576

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
1	syslog	business-systems	management	client-server	8,355,346,064	24,231
4	ms-update	business-systems	software-update	client-server	59,429,984,410	118,079
3	apple-update	business-systems	software-update	client-server	16,366,244,120	32,134
4	adobe-update	business-systems	software-update	client-server	7,772,801,909	13,136
4	squirrelmail	collaboration	email	browser-based	6,475,270,847	514,043
5	smtp	collaboration	email	client-server	21,301,863,500	2,037,421
3	facebook-chat	collaboration	instant-messaging	browser-based	11,427,976,877	545,344
1	blackboard	collaboration	internet-utility	browser-based	26,214,653,556	788,724
4	facebook	collaboration	social-networking	browser-based	102,708,763,192	4,711,624
5	bittorrent	general-internet	file-sharing	peer-to-peer	846,225,518,513	26,730,296
5	gnutella	general-internet	file-sharing	peer-to-peer	87,248,635,137	8,035,564
5	emule	general-internet	file-sharing	peer-to-peer	63,490,724,759	12,077,408
5	xunlei	general-internet	file-sharing	peer-to-peer	14,282,488,274	14,195
4	flash	general-internet	internet-utility	browser-based	709,730,098,914	1,143,571
4	web-browsing	general-internet	internet-utility	browser-based	594,189,573,268	24,029,882
5	http-audio	media	audio-streaming	browser-based	64,581,162,955	41,329
3	pandora	media	audio-streaming	browser-based	37,292,967,128	30,211
4	ruckus	media	audio-streaming	browser-based	6,452,213,457	7,584
4	itunes	media	audio-streaming	client-server	29,352,390,994	227,723
3	xbox-live	media	gaming	client-server	39,932,682,099	540,520
3	worldofwarcraft	media	gaming	client-server	17,061,352,634	14,318
5	youtube	media	photo-video	browser-based	218,222,089,400	176,533
5	http-video	media	photo-video	browser-based	181,474,876,989	53,013
2	hulu	media	photo-video	browser-based	72,661,516,902	61,906
4	limelight	media	photo-video	browser-based	63,571,739,997	81,849
1	myspace-video	media	photo-video	browser-based	22,310,108,410	90,615
5	asf-streaming	media	photo-video	browser-based	20,888,906,065	5,653
3	photobucket	media	photo-video	browser-based	10,526,523,690	159,020
1	move-networks	media	photo-video	client-server	126,395,030,505	29,408
4	rtmp	media	photo-video	client-server	86,616,709,167	28,270
3	rtsp	media	photo-video	client-server	32,792,791,451	3,189
4	ppstream	media	photo-video	peer-to-peer	22,135,922,125	352,826
4	ssl	networking	encrypted-tunnel	browser-based	83,304,563,902	1,871,085
4	gpass	networking	encrypted-tunnel	client-server	24,081,789,782	7,773
5	http-proxy	networking	proxy	browser-based	6,714,814,130	2,635

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

Key observations on top 35 (out of 308) 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, file-sharing and audio-streaming.

Conclusion: Findings and Recommendations



- Findings should reflect the discrepancies between what the customer security policy was designed to accomplish and what was really happening

- Recommendations are tailored to address key issues uncovered and documented in the earlier pages of the report and summarized in the findings.

Findings:

During the planning phase for the Palo Alto Networks analysis the Company X 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 Company X 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, Company X 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 Company X as employees use these applications to bypass existing traditional controls. Without understanding, categorizing, and mitigating risk in these areas, Company X 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. Company X 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.

Company X 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 Company X 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.

When to Use the AVR Report

- Targeted at accounts where:
 - The champion is willing to set up a meeting with the economic buyer (C-level or other) and said person is receptive to a meeting
 - Tech champion loves the product has no budget authority for it
 - We found and fixed some issues they were unaware of
- Not recommended for accounts where:
 - Reception of Palo Alto Networks is lackluster
 - Did not find anything interesting during the eval
 - Account status is on life support
 - Palo Alto Networks champion is unwilling or unable to help set a C-level meeting



Delivering the AVR Report

- Recommended delivery methodology
 - Face-to-face meeting
 - *Palo Alto Networks Sales/SE, our champion, the C-level/economic buyer, partner*
 - Take the time to print it in color
 - Use Palo Alto Networks folders, combined with a literature, and the corporate backgrounder
 - Set the stage – once we are finished, let's talk about ordering
 - Report delivery should be a team effort – led by sales, supported by SE
 - *Walk through the report, talking about what was found, what it means and recommendations*

Results

- AVR has been instrumental in helping Palo Alto Networks achieve our revenue targets
 - Helps partners make more money
 - Close more deals
 - Charge as a service
- Some statistics
 - Produced more than 160 AVR Reports
 - AVR helped generate more than 60% of our revenue to date
- No other vendor provides a business tool like this
 - Use it as a differentiator

Assembling the AVR Report

- C-level meeting commitment
 - Export statistics from evaluation box (CLI command)
 - *tftp export stats-dump to [ip address]*
 - *scp export stats-dump to [ip address]*
 - Data is exported in a tar.gz file – do not unzip it or alter it!
 - Best results are after it has been tuned a bit and has run for at least 24 hours
 - Information on their application usage policy –
 - *This allows you to show that what they have is not working!*
- Print report in color – make copies for all attendees
- Close the deal!

Thanks!