



The Case for a Policy-Based Web-Use Management Approach

Wavecrest Computing
2006 Vernon Place
Melbourne, FL 32901
Toll-free: 877-442-9346
Voice: 321-953-5351
Fax: 321-953-5350

www.wavecrest.net

Abstract

Prompted by the explosion of employee Web usage in enterprises of all types, this paper reviews policy-based Web-use management approaches. It first reviews their need and then describes how they can be implemented in a way that benefits all concerned.

By way of definition, a "policy-based Web-use management" approach integrates specific *policy* provisions ("do's and don'ts") with (a) a semi-automated monitoring and auditing *process* and (b) follow-on management processes and actions. And the terms "use" and "usage" refer to constructive, productive use of the Web as well as undesirable or unacceptable use.

The paper points out that enterprises of all kinds—business, education, government, etc.—are rapidly increasing their use of the Internet. This increase goes far beyond "sales" and "research." It now extends to many core-business or mission-related functions. As more and more dollars and manpower are invested in this effort, and as the dependency on network resources increases, these enterprises need to strengthen and improve the way in which they manage the use of this increasingly vital resource.

In this regard, the paper urges enterprise managers to become considerably more involved in planning and controlling Internet usage. It goes on to point out that the best way to do this is through use of *policy-based* Web-use management approaches. A logical sequence of actions for them to follow is this: First, they need to establish *policies* that encourage positive Web-use while simultaneously discouraging negative (personal) use. Secondly, they need to put in place *policy-based software* to help ensure compliance with the policy. (Policy-based software can automatically monitor, analyze and document Web usage, providing management with usable, reliable information that helps identify problem areas and determine trends.) Thirdly, management must invest the time and effort to *use this information* to (a) adjust priorities, strategies, schedules and tactics and (b) to guide any necessary workforce-related actions, e.g., assignments, training, or disciplinary action.

The paper concludes by pointing out that the integration of these three elements (i.e., establishing a comprehensive policy, installing policy-based software for reporting, and using the information in the reports to make strategic and tactical adjustments) constitutes an effective policy-based Web-use management approach.

Background

It's no secret that thousands of enterprises are increasing their use of the Internet at a phenomenal rate. Furthermore, they're using it for much more than simple on-line shopping and e-mail. Increasingly, they are using it for *core functions* of the enterprise, e.g., "front office", logistic, administrative, financial, marketing, purchasing, shipping, order tracking, advertising, technical, training, project-collaboration and "just-in-time-manufacturing" activities. While this is all very exciting, many enterprises are discovering that it's a two-edged sword. On the one hand, Internet-based approaches *benefit* the enterprise in many ways, i.e., they typically result in improved communications, increased flexibility and agility, reduced turnaround times, increased profit potential, etc. On the other hand, such approaches result in an increasing level of *dependence* on Internet resources and usage. Now "Net-dependence" is not *inherently* a bad thing. However, without proper management attention, such dependence can lead quickly to ineffective use of the work force. To preclude this from happening, enterprises need to closely manage *all* aspects of Net-related activity.

Managers need to establish policies that encourage positive Web-use while simultaneously discouraging negative (personal) use. Second, they need to put in place policy-based software to help ensure compliance with the policy.

To date, most Internet management efforts, if any, have been aimed solely at preventing or minimizing use of the Net for personal reasons.

Current Management Approaches

To date, most Internet management efforts, if any, have been aimed solely at preventing or minimizing use of the Net for personal reasons. Some enterprises do this by blocking access to "undesirable" sites, e.g., those featuring pornography. This is often referred to as "filtering." Another approach, which some enterprises employ, is the use of a very *simple reporting* system—one that identifies users and lists the sites they have visited. This type of simplistic reporting leaves it up to the individual manager to decide—after the fact—what is abusive and what is not. This is often an onerous burden.

These simplistic approaches, while useful to a point, have several drawbacks. First, they focus solely on the negative aspects of Internet usage and do nothing to prompt or encourage positive, constructive use of network resources. Secondly, they can lead to a false sense of security, i.e., they can never capture more than a modest percentage of "unacceptable" or "undesirable" sites.

Even if these two approaches were effective, mere minimization of abuse is no longer adequate in today's Internet-intensive world. After all, waste and abuse constitute only a small fraction of Internet use, perhaps five percent.

A Better Way

If waste and abuse constitute only five percent of Internet use, *what about the other 95 percent?* This remaining "fraction" consists of extensive human and technological resources that are being devoted to enterprise-related Internet activity every day. As with its other resources, management needs to plan and control Internet usage to ensure optimum results. To do this successfully, enterprise managers need to develop and implement *policy-based* Web-use management *approaches*. At a very fundamental level, a Web-use management *approach* includes:

- a strategy for Internet use
- a policy for governing Internet use
- a *policy-based* mechanism for monitoring and reporting Internet use
- a follow-through process for analyzing Internet usage and taking appropriate action on the basis of that analysis.

As you can see, the first, second and *fourth* bullets represent *human* management functions. These functions involve decision-making responsibilities that cannot be performed by anyone or anything else (sorry, computers can't do it all). On the other hand, the third bullet *can* be handled automatically by well-designed Web-use management products (more on this later). All four bullets are discussed briefly in the following paragraphs.

Strategy for Internet Use

In a way, discussing the need for strategy is "stating the obvious," but then again, maybe not. In today's world, network resources are absolutely crucial to achievement of the enterprise's goals and objectives. In addition, it's no secret that they are extremely expensive. Consequently, to ensure cost-effective mission success, the enterprise should have a carefully crafted, clear strategy for the way these resources are to be used. The strategy should state the enterprise's goals and objectives in a clear, coherent way and should indicate the priorities to be employed, functions that are to be stressed, etc.

Policy for Governing Internet Use

A sound, formal Web-use policy is needed to help implement the enterprise's strategy. In the context of network usage, an effective, thoughtful, and properly administered policy is a dual-purpose document. That is, it 1) encourages and guides all members of the enterprise work force toward positive constructive use of network resources, while 2) simultaneously helping to curb inappropriate or abusive use. To accomplish the first purpose, it should clearly reflect the strategy discussed above as it relates to network usage. In so doing, the policy

A sound Web-use policy is more than just a litany of restrictions and penalties; it is the fundamental promoter and guideline for using network resources in positive ways to benefit the enterprise.

"Policy-based" refers to an application that can be tailored to reflect—and monitor compliance with—the enterprise's own policy.

should clearly state how, when and why network resources should be used and when they should not. To aid the second purpose, it should clearly state what is acceptable use and what is not, and it should clearly indicate the sanctions to be imposed for engaging in unacceptable use. In our judgment, though, the former should be emphasized more than the latter. In sum, a sound Web-use policy is more than just a litany of restrictions and penalties; it is the fundamental promoter and guideline for using network resources in positive ways to benefit the enterprise and all of its members and stakeholders.

Policy-Based Monitoring and Reporting

By definition, Web-use policy *management* strives to ensure that Internet usage conforms to both the positive and restrictive aspects of the enterprise's policy. Successful accomplishment of this objective requires implementation of some type of highly efficient monitoring, documenting and reporting product that can record and display the number, type and origin of Web site visits. This information is needed to determine the degree to which network resource usage conforms to the enterprise's Web-use policy. To produce this information, enterprises can implement some sophisticated but easy-to-use Web-use management *products* that are currently in use in a number of sectors (more on this later).

Follow-Through Process (for Analyzing and Using Reports)

As indicated earlier, an effective policy-based Web-use management approach includes a follow-through process for analyzing Internet usage and taking appropriate action when deviations from policy are noted. Such action may be needed to 1) bring network usage into conformance with policy, or 2) to modify the policy (or related plans) accordingly. When this is the case, management can use the information provided by the reporting system to guide adjustments to priorities, strategies, schedules and tactics, and/or to guide any necessary workforce-related actions, e.g., assignments, training, or disciplinary action. It can also be used to guide the establishment of Web-access blocking regimens if management decides to include filtering in its overall approach.

Web-use Management Products

Having discussed the four elements of policy-based Web-use management briefly, we would now like to follow up on the third one (monitoring/reporting) with a more detailed discussion of Web-use management products. Just what are Web-use management products anyway, and why does anyone need them? Let's take a look.

In the context of this paper, Web-use management products are software applications that analyze Web site visits, list them in subject-matter categories, and determine their acceptability or appropriateness. (Such products may or may not be used in conjunction with filtering.) Through various output reports, these applications provide information to managers for use in identifying relevant trends and making business decisions. Very importantly, these products may or may not be policy-based. ("Policy-based" refers to an application that can be tailored to reflect—and monitor compliance with—the enterprise's own policy.) While both types are useful, a policy-based product is much more advantageous than one that is not. A well-designed, policy-based Web-use management product can monitor and report on Internet usage in a much more useful and efficient way than one which is not policy-based. The reasons for this are discussed next.

Non-Policy-Based Products

If the product is *not* policy-based, it simply reports "raw visit data." It does not analyze results or compare them with any standard. Without extensive manual analysis, such data doesn't answer the most important Web-related question: "Were the visits productive or abusive?"

Policy-Based Products

Conversely, if the product *is* policy-based, it **does** answer the question: "Were the visits productive or abusive?" There are three reasons for this. First, the product can help with policy formulation. Secondly, the product can be used for policy *administration*. Thirdly, it can help with policy dissemination. These three uses of policy-based products are discussed in more detail below:

A well-designed, policy-based product can help enterprise managers define and describe the policy in highly specific language, completely consistent with subsequent audits and reports.

Use of Policy-Based Products for Policy Formulation

A well-designed, policy-based product can help *formulate* as well as *administer* Web-use policy. The parameters of such a product can help enterprise managers define and describe the policy in highly specific language that is completely consistent with subsequent audits and reports. These parameters include the (a) subject-matter categories, (b) acceptability classifications and (c) permissibility thresholds that are built into the product and (if desired) customized by the enterprise. Definitions of these three parameters (product features) can be translated easily into policy language, thus tying the policy directly to the product. These parameters enable enterprise management to assign "acceptability" classifications to the categories and to establish *thresholds* for identification of improper use. These last two concepts are discussed below.

1. Category "Acceptability" Classifications (Ratings). As part of policy definition, each category can be assigned an "acceptability" rating, e.g., "acceptable," "unacceptable" or "neutral." Management makes these assignments on the basis of the enterprise's policy and "business" objectives.

Note: Management can add additional "custom" categories (with enterprise-specific URLs) to the universal, i.e., standard categories built into the product. Custom categories enable management to focus in tightly on areas of particular importance to the enterprise.

2. Intra-Category Thresholds. After assigning an "acceptability" classification to each category, the enterprise can also assign it a quantified "threshold" value. Thresholds, expressed as "number of visits," help differentiate "appropriate" from improper or abusive use, as defined below:
3. Appropriate Use. Appropriate use includes "authorized" visits that benefit the enterprise or user in *positive* ways. Also included is a reasonable but limited number of "personal" visits in selected categories.
4. Improper Use. Improper use is defined three ways:
 - Any number of visits to totally "unacceptable sites."
 - "Excessive visits to Web sites for personal reasons", i.e., a level of visits that is ABOVE the threshold in a nominally authorized category. This is considered "abuse."
 - Excessive visits to sites that may not be "unacceptable," but are simply not productive for the organization's purposes.

As indicated earlier, threshold levels are defined by the enterprise, not the software vendor. And they can relate to the potentially positive as well as negative uses of the Internet.

Policy Dissemination

If the product is well-designed, the category, classification and threshold definitions can be translated easily into policy *language*. The policy can then be widely disseminated, in an understandable form, to all concerned. As part of this process, the various components of a policy-based Web-use management system can be used to "educate" the enterprise's computer users in a *positive* manner. First, management can explain the content of the policy itself, pointing out the reasons—both positive and restrictive—why the policy is necessary. They can then explain how the language of the policy is reflected in the design of the product's categories, classifications and thresholds. Next, they can discuss how these three entities are tailored for the enterprise. Finally, management can describe how the various provisions of the policy will be monitored and audited, how the users will be notified of any deviations, and the kinds of corrective action that may be taken if necessary. As mentioned earlier, such orientation does not need to focus solely on the "negative." It can be used to stress how management *wants* the Web to be used (not just how it should *not* be used), and how proper use can help the enterprise and all of its stakeholders succeed. Done this way, the policy helps preclude misunderstanding or confusion as to what constitutes desirable and undesirable use of the Internet.

To maximize return on their Internet "investment," enterprise managers need to become considerably more involved in planning and controlling Internet usage, and they need to develop and implement policy-based Web-use management approaches.

Use of Policy-Based Products for Policy Administration

A well-designed, policy-based product provides clear, understandable reports which show usage in relation to conformance to the policy ("How many and what kinds of visits are being made? Are they productive or abusive?"). Such a product can help ensure comprehensive, equitable, fair administration of the enterprise's Internet policy. Assuming it is implemented with a thoughtfully designed and tailored set of categories, classifications and thresholds, the product can easily produce a variety of cogent, immediately usable reports. The information in the reports can be as concise or as detailed as desired. The information can be used by itself, or it can be used in conjunction with other enterprise data (functional, financial, etc.) to aid in a wide spectrum of planning and decision making efforts.

Summary

Because of the burgeoning use of the Internet, it behooves enterprises of all kinds to strengthen and improve the way in which they manage the use of this increasingly vital resource. It is no longer enough to simply block access to pornographic sites, or to leave it up to individual supervisors to detect abuse via oversimplified site-visit reports. To maximize return on their Internet "investment," enterprise managers need to become considerably more involved in planning and controlling Internet usage, and they need to develop and implement policy-based Web-use management approaches. To achieve this objective, they first need to establish *policies* that encourage positive—and discourage negative—use of the Internet. Secondly, they need to put in place progressive management systems that *ensure compliance* with the policy. Thirdly, they must support the systems with *policy-based software* that automatically monitors, analyzes, documents (and possibly filters) Web usage. Such software can provide management with usable, reliable information that helps identify problem areas and determine trends. Finally, management must use this information to (a) adjust priorities, strategies, schedules and tactics and (b) to guide any necessary workforce-related actions, e.g., assignments, training, or disciplinary action.