



White Paper

metagroup.com



800-945-META [6382]

January 2004

The Growing Security Threat: Your Employees

*Keeping “Good” Users From Doing
“Bad” Things Over the Internet*

A META Group White Paper

“Establishing a security solution to address the appropriateness of content and its usage within electronic communications has quickly become a legitimate business issue, due in part to productivity, liability, and privacy concerns. A separate solution focused on user and content control, ideally based on an appliance platform and a proxy architecture, will be warranted for most organizations.”



METAGROUP

What Are Users Doing Over the Internet?

Traditional security strategies have focused on “network access” and blocking outside threats from entering the internal network. This has resulted in the erection of multi-tiered demilitarized zones, incorporating controls such as firewalls, authentication services, intrusion detection systems, and antivirus scanners. While these measures remain instrumental to providing security for today’s networked environments, they are no longer sufficient.

Risks and threats to the organization are taking new shape. Now more than ever, they originate from inside the network as well. Today, users in the workplace can effortlessly access the Internet and Internet-based applications. Communicating outside the organization in this fashion introduces the potential for bringing back malicious or offensive content. If left unmonitored and uncontrolled, this could result in significant exposure to the organization, specifically in the form of user productivity losses, legal liability, and degradation of network availability.

A Multifaceted Challenge

Specific challenges begin to become apparent on further examination of the many facets that encompass user-initiated Internet communications beyond the firewall. Of particular interest is the “Web channel,” which supports activities such as employee Internet access, instant messaging, peer-to-peer file sharing, Web-based e-mail, and even collaborative applications (e.g., shared workspace).

Web E-Mail Is a “Back Door” for Viruses

Web e-mail can be a back door for malicious code, such as viruses, or untrusted active content. It allows for offensive/unseemly material, such as pornography or racial disparagement, to be introduced on the corporate network. In addition, it makes possible the unwarranted disclosure of intellectual property.

Instant Messaging (IM) Can Become a “Virtual Water Cooler”

Instant messaging is another example, but is potentially much more troublesome due to its “cloaking capability,” which allows it to evade port-blocking controls (e.g., firewalls). Its network awareness and ability to use virtually any port often creates the misconception among network administrators that the application is blocked, when in fact it is not (e.g., AOL IM will automatically roll over to port 80 if port 5190 is blocked on the firewall). In reality, the unblocked and uncontrolled instant messaging communication serves as a back door for malicious code and viruses via allowed file attachments. It can also create a significant drain on productivity as users engage in “virtual water-cooler” discussions.

Peer-to-Peer File Sharing Hogs Resources and Can Get You Sued

Peer-to-peer (P2P) file sharing is widespread and presents a myriad of challenges to the organization. Uncontrolled P2P file sharing on the corporate network: 1) consumes network bandwidth and degrades network availability; 2) creates a productivity risk as users spend excessive amounts of time downloading content; 3) puts the organization at risk to be sued by various enforcement agencies; and 4) can load spyware (often part of P2P software packages) on corporate systems, which could provide unauthorized access to sensitive information.

How Uncontrolled Users Are Impacting the Business

If organizations take a closer look at the issue, it is clear that they should be concerned with controlling user-initiated Internet communications and associated content for a number of very specific and potentially serious reasons.

Productivity Enhancement

Numerous “Web channel” capabilities have turned corporate networks into virtual playgrounds, where unmonitored users are pushing the limits of acceptable use of company resources. Indeed, misuse of company-provided Internet access for non-business purposes has become rampant. In an ideal world, policies alone would prevent this problem. However, we conservatively estimate inappropriate Web usage to average 2-4 hours per user per week. Web/URL-filtering products can often help with this issue, though they cannot guarantee that users prevented from accessing non-work-related sites will be productive.

Instant messaging is another example where users often get caught up in time-absorbing virtual water-cooler conversations with friends and colleagues. Tools that control and log IM conversations are critical to correcting this situation. Alternatively, leveraging products that provide usage quotas, or that can relax restrictions after normal working hours, will often support establishing such an application as a productive business tool. This creates a happy medium, hopefully to the benefit of all parties.

Resource Conservation

Directly linked to the productivity issue is efficient utilization of computing resources. Unwanted and unproductive activity consumes valuable processor cycles, memory, and disk space from servers, as well as valuable bandwidth from Internet connections and associated networking devices. Appropriate filtering and control can relieve the burden and, at a minimum, stave off the need for expensive system or connection upgrades.

Clearly, bandwidth-hogging applications like P2P file sharing and multimedia streaming must be controlled at some level. P2P file-sharing applications have presented a significant threat to network resources, easily consuming more than 30% of an organization's Internet/WAN bandwidth at times. Additional resources also become tapped during the storage of music and video files after they are downloaded, putting a significant burden on file server capacity.

Liability Protection

One of the most significant benefits of user and content control is the protection it affords against liability. Having related products installed and properly maintained is rapidly becoming the standard of due care among leading global organizations. Doing anything less introduces the potential for damaging lawsuits. For example, litigation could arise from the scenario where one employee is exposed to offensive content downloaded from the Web by another employee. If it is subsequently determined that the company had not taken reasonable measures to prevent this situation, it could be held responsible. In this case, owning, operating, and maintaining a common URL-filtering product configured to prevent access to Web sites known to contain pornographic material would most likely constitute "reasonable measures" and, therefore, should be sufficient to clear the company of related claims of negligence. *(Note: The opinions, descriptions, and recommendations contained in this document may include general or summary information about aspects of various rules, regulations, or standards. The information presented is intended simply as an aid to your understanding of such rules and neither constitutes nor is intended to constitute the provision of legal advice. We urge you to refer to the actual laws, rules, regulations, and/or standards, and to consult with legal counsel concerning your responsibilities, if any, with respect to applicable provisions.)*

A more recent and perhaps more visible liability to organizations is the use of peer-to-peer file sharing on corporate networks. This inappropriate and sometimes illegal use of network resources places a significant risk on the business, opening it up to possible suits by the Recording Industry Association of America (RIAA) or the Motion Picture Association of America (MPAA), both of which continue to hunt down the illegal sharing of copyrighted material.

Privacy Compliance

An increasingly important business consideration is maintaining compliance with various privacy requirements. Legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) in the US and the European Union's Privacy Directive impose various penalties for improper disclosure of personal information that is deemed private or confidential

(e.g., pertaining to patients or customers). In addition to simple monetary fines, privacy breaches can also have dire consequences when it comes to retaining customer trust and maintaining the overall corporate reputation. Certainly, the initial reaction to such requirements is to implement various encryption and authorization controls. However, the sufficiency of these measures is doubtful. Ultimately, a layered approach is appropriate, implying a role for content filters, at least at strategic “privacy boundaries.”

Protection of Intellectual Property

A similar conclusion can be reached for any information that is considered “company confidential.” Clearly, this would include not only trade secrets and other intellectual property, but also financial performance information and details of any strategic initiatives. Two likely communication mediums for this include users’ “posting” to financial message boards and widespread unmonitored IM conversations from inside the corporate network to the outside world. A filtering device capable of keyword searches and conversation logging would be essential to ensuring against an outflux of such material via these electronic means.

How Can Organizations Gain Control?

Hopefully by this point, the need to control the usage of Web channel services has become clear. But what is the best approach?

Firewalls: Not a Good Fit for User and Content Control

A natural tendency for organizations is to use other security devices they have already implemented, in particular firewall systems, to address their user and content control needs. However, we generally recommend against this, primarily on the basis that firewalls typically lack sufficient insight to enable the granular decisions required. Specifically, firewalls, or access control gateways, govern the flow of traffic between two networks based on whether the connection appears to be one that supports a legitimate and allowed business function. The decision is made from information contained solely within packet headers. For that matter, it is mostly network layer details (e.g., source, destination, protocol being used), and the related policies are therefore network-oriented (i.e., the objects used to define rules are items such as IP address ranges and subnetworks).

Even firewalls that incorporate application-layer awareness and control are insufficient when it comes to user control. While these can typically identify specific application-layer protocols (e.g., HTTP) and even commands within those protocols, they still lack the deeper visibility that is often necessary to establish the appropriateness of the material contained within a communication session. What is needed instead is a solution that makes decisions based on the payload portion

of packets — or, more accurately, on entire messages. The point is that the inspections, and therefore the associated policies, must be data-oriented, as well as user-oriented — since appropriateness can often be dependent on the specific users (and their roles) engaged in the communication.

The Criteria That Matter Most

As a result of the differences from traditional access control services, we typically recommend organizations use a separate solution to address their user and content control requirements. In doing so, we emphasize a number of specific guidelines and criteria.

The Benefits of a Proxy Service

A proxy service functions as an intermediary, appearing as the actual destination to the source client and as the actual client to the destination server. In doing so, it fully terminates all communication sessions, unwrapping received packets to an extent, before creating a separate session to convey the rewrapped packets to their eventual destination. This is significant, because the process is inherently well suited to the introduction of additional inspection, and subsequent filtering if necessary, of the messages that are being handled. In fact, different inspection modules that focus on individual “channels” (e.g., Web, e-mail) can all be hosted within the generic proxy capabilities simultaneously. In addition, based simply on how it functions, the proxy service has the added benefits of fixing faulty or deliberately malformed packets, keeping internal addressing structures from being exposed to the Internet, and offering a convenient opportunity to enforce user authentication. For all these reasons, being a proxy is a favorable characteristic for a user and content control solution.

Appliance Platforms Are Preferred

Another platform-oriented characteristic that is favorable is being an appliance. Appliances afford numerous benefits, based primarily on customization of hardware and associated operating systems to better meet the needs of the software running on it — which, when preloaded on the system, yields a self-contained, plug-and-play product. Derivative benefits include significantly enhanced performance and an overall system that has been “hardened” against potential security threats.

Flexibility Is Your Friend

One significant challenge stems from the fact that organizations undoubtedly have different interpretations with regard to what constitutes “appropriate” when it comes to content and the usage of various Web channel services. This suggests that user and content control solutions must be both extensible and highly customizable. They must be able to account for topic matter beyond that which is

common among all organizations and must also be able to account for different policies for different groups of users.

This flexibility must also extend to the options for “filtering,” a term that so far has been used to refer both to the inspection of communication sessions and to the assumed subsequent action of preventing the flow of that which is deemed inappropriate. However, due to the technical difficulties associated with definitively determining that something is “appropriate,” there must be support for multiple types of responses. For example, depending on the circumstances, it may be appropriate to block an entire session, to strip out only the objectionable portions of a message, or to simply monitor “questionable” activity (i.e., log/record its passage and/or flag it for review by an administrator).

Manageability Is a Must

As with just about every security solution, robust management capabilities are essential to successful deployment and ongoing operations. This may even hold more significance for user and content control, given the potential for widely varying policies. The implications here are that not only is a centralized management capability desirable, but also the rules must be definable at the individual user and group level (not just network level). Furthermore, the management construct should be both hierarchical and capable of being delegated. This means that rules can be established that will be “globally” applicable, while local or regional managers can have the flexibility to implement their own policies for the remainder of the subject matter. Finally, robust logging and reporting are absolutely necessary. This is the means not only for recording attempted policy violations (or recording unwanted activity if in “monitor-only” mode), but also for providing the feedback mechanism for making policy adjustments (e.g., based on finding items that are slipping through the filters for whatever reason).

Gain Visibility — Then Control

In terms of implementing a solution, we recommend an ordered progression of measures. Specifically, companies should do the following:

1. **Define acceptable use policies for Web channel services and content (e.g., Web surfing, instant messaging, file sharing):** An example of this would be establishing a policy to log all IM conversations and block all P2P traffic, while making employees aware of these rules via splash pages and e-mails.
2. **Gain visibility into how users are currently accessing the Internet and Internet resources:** Filters and proxies can sit in the flow of traffic and simply monitor user sessions, without impacting other network

resources or limiting usage, ultimately producing detailed reports on user activity.

3. **Begin to enforce acceptable-use policies:** Proxy/filtering appliances can serve a critical role in the security infrastructure to complement the protection afforded by traditional access control measures.

Conclusion

Establishing a security solution to address the appropriateness of content and its usage within electronic communications has quickly become a legitimate business issue, due in part to productivity, liability, and privacy concerns. However, it is a multifaceted problem that is fundamentally different from that addressed by traditional access control gateways, which typically lack the requisite depth of visibility. Therefore, a separate solution focused on user and content control, ideally based on an appliance platform and proxy architecture, will be warranted for most organizations. Complementing traditional controls in this manner can help minimize risks to the organization and keep network users productive.

Mark Bouchard is a senior program director with Security & Risk Strategies, a META Group advisory service. For additional information on this topic or other META Group offerings, contact info@metagroup.com.



About META Group

Return On IntelligenceSM

META Group is a leading provider of information technology research, advisory services, and strategic consulting. Delivering objective and actionable guidance, META Group's experienced analysts and consultants are trusted advisors to IT and business executives around the world. Our unique collaborative models and dedicated customer service help clients be more efficient, effective, and timely in their use of IT to achieve their business goals. Visit metagroup.com for more details on our high-value approach.

