Windows® IT Pro

Filtering the Spectrum of Internet Threats:

Defending Against Inappropriate Content, Spyware, IM, and P2P at the Perimeter

St Bernard Software™

Because of the proliferation of Web-based threats, you can no longer rely on basic firewalls as your sole network protection. Most firewall rules are based on the IP address and network port but they don't inspect the actual network traffic content. For example, consider blended threats that sneak into your company through email and entice employees to click external links that lead to a malicious Web site. Your firewall might recognize only legitimate traffic—in this case, an inbound email inbound and outbound Web request from an internal user.

Attackers continue to evolve clever methods for reaching victims, such as sending crafty Web links through Instant Messaging (IM) clients or email, or by simply linking to other Web sites that your employees might surf. These links can lead to phishing attacks designed to lure victims into divulging personal information. Shutting down access to these Web sites protects your employees and increases the security of your network.

One effective defense to these types of attacks is to deploy a content-aware, perimeter-based network security device that inspects and blocks Web requests based on URL destination. Because the addresses of these threats morph and change regularly, choosing a solution that offers a subscription to an effective list of categorized Web sites lets you permit or deny a category while ensuring that you can effectively block in the background the hundreds of thousands of URLs associated with sites matching that category.

This white paper examines the threats of allowing unwanted or offensive content into your network and describes the technologies and methodologies to combat these types of threats. Specifically, this paper looks at how you can leverage the features of the St. Bernard Software™ iPrism® dedicated Internet filtering appliance to reduce your exposure to these risks and improve the overall security of your network.

Contents

Filtering the Spectrum of Internet Threats:

Defending Against Inappropriate Content, Spyware, IM, and P2P at the Perimeter

Just as security threats and attacks continue to evolve, so must your company's defenses. Unfortunately for many small to medium businesses (SMBs), it's sometimes difficult and costly to commit resources and time to stay protected against the most recent attacks. For example, some of the fastest growing attacks come from phishing email messages that contain links to malicious Web sites. Also, the proliferation of peer-to-peer (P2P) software and IM software has provided attackers with new avenues into your company—avenues that some firewalls might not be able to block. In this white paper, we'll look at solutions such as the St. Bernard Software™ dedicated Internet filtering appliance, which helps address these threats and defend your network with little reconfiguration of your legacy network.

We'll look at how a perimeter network security appliance such as the iPrism® is well suited for SMBs because it lowers total cost of ownership with rapid deployment and ease of configuration, and provides a secure and stable appliance-based solution. Specifically, the iPrism® appliance simplifies the management of specific threats (e.g., blocking and monitoring P2P communications and IM software) without requiring you to know specific, and often changing, protocol information. In essence, the iPrism®

lets you define business rules for your company, then it enforces these rules for you at the technical level. A perimeter device isn't a replacement for your firewall but rather it sits behind your firewall and augments the security of your firewall by providing deeper inspection of the Web, IM, and P2P traffic crossing your network. Perimeter protection against unwanted or offensive content is the tip of the iceberg, yet it's an essential solution that enables organizations to defend against the risks of legal liability and lost employee productivity, and meet compliance guidelines. Incorporating perimeter security features (such as IM and P2P management, and spyware and malware defense) into Internet filtering solutions is essential to provide a first line of defense against these growing and most dangerous threats.

A New Surge of Blended Threats

Traditional viruses and worms exploit vulnerabilities in OSs to install themselves, propagate, and cause damage. The best security against these threats is to use current antivirus software on all your computers, patch all your computers with the latest OS and application security updates, and install a quality firewall between your computers and the Internet that blocks all inbound Internet traffic except that which your company specifically needs (e.g., inbound email or Web traffic to your Web server).

As more and more people adopt these security fundamentals, attackers must look for new attack vectors to infiltrate their victims. One of the oldest and still effective means of attacking a network or user is through social engineering.

Social Engineering and Phishing

Social engineering relies on the victim taking an action that grants the attacker access to their network instead of exploiting a flaw in the technology. An example of social engineering is an attacker who calls a victim purporting to be from the Help desk and asks for the user's network password to test their account. If the victim gives up their password, that person has just granted the attacker complete access to the same resources as the victim.

Phishing attacks are on the rise and use social engineering to scam victims out of their personal information (e.g., social security number, bank passwords, other account information). Typically a phishing attack begins with an email message containing a link to a malicious Web site. The email might be an invitation to get a "Low, Low Mortgage" or it might look like it comes from an actual bank or online service. The sophistication of the attack varies but the end result is often the same—the victim is enticed into clicking a link to a malicious Web site. Phishing attacks most commonly come through email but more recently phishers have turned to using IM because it's new and users haven't yet learned to be wary of messages spoofed from their friends. In the following sections, we'll examine how a perimeter network security device, such as the iPrism®, can block Web requests based on their URL or IM traffic and help protect your network from phishing attacks.

Visiting Fringe Sites

Beyond being lured to nefarious sites through phishing attacks, your users may download and install malicious software (malware) and spyware by visiting Web sites of questionable intent—otherwise known as fringe sites. Your employees might visit these sites because either they mistype a legitimate URL or because they choose to visit an inappropriate or unsafe Web site. For example, many pornography and gambling Web sites often link to or spawn pop-ups to other unknown Web sites linking to even more fringe sites. These fringe sites can host malware or spyware and attempt to trick the user (or exploit a vulnerability) into installing the software. For example, one way to trick a user is to masquerade a fake "close" button in the actual Web page or pop-up window. So when users click that button, they might launch a program instead of closing the window.

Social engineering works well in these scenarios because many SMB users log onto their computers using accounts with privileged system access (such as being a member of the local administrators group). As a result, the Web browser is often running under a privileged account and lets the user download and install software from any Web site. (Or even if the browser is configured under higher security, a privileged user can change this setting—whether on purpose or accidentally or through social engineering.) As you can see from these examples, attackers don't need to hack the OS but rather they merely need to trick the user into clicking a link to download their software and get the user to click the OK button to install the software.

The sophistication of these attacks has steadily increased to a point that discerning legitimate email from spoofed email or confirming the validity of an IM message can be challenging, even for a technically savvy user. What's important to keep in mind is that regardless of the lure—whether it's a phishing email, a link in an IM chat window, or a link to a fringe Web site—the underlying mechanism remains the same in many chases. *The user must click a link to visit a Web site.*

Some perimeter network security appliances use a database of URLs to monitor or block access to certain types of sites. When you review these types of appliances, make sure you select a product that offers a subscription that regularly updates the entries in the database as new sites are discovered or come online.

The iPrism® appliance uses the iGuard database, which you can configure for a daily download to get the latest list of offending URLs. Their subscription-based service lets you filter or monitor Web usage by category and you can choose what level of monitoring is most appropriate for your organization. Each iPrism® appliance requires a subscription to the iGuard database to ensure that the categories of every device are up to date.

Even lenient companies that provide their users with wider use of the Internet probably don't want their employees visiting certain sites known to host nefarious content. For example, to lower the outbreak of spyware in your company, you can configure the iPrism® to block access to the iGuard database *Malware* and *Spyware/Adware* categories. Blocking access to certain URL categories such as *Malware*, *Phishing*, *Spyware/Adware*, *Computer Hacking*, *Copyright Infringement*, or *Other Questionable Activities*, helps dissuade users from visiting sites that might lead to the types of attacks we've discussed.

Peer-to-Peer and Instant Messaging

P2P and IM applications have spread like wildfire. These applications let people all around the world communicate and share files in real time with anyone else on the Internet. Unfortunately, by their very nature, these tools establish connections directly between users and may bypass your firewall or file sharing services (e.g., FTP). Permitting IM and P2P software in your company makes it difficult to control the files entering or leaving your company, who is sending them, or whether those files have been adequately scanned for viruses.

Configuring a traditional firewall to correctly block all IM and P2P software can also be time consuming because each application uses its own proprietary network protocols. Plus, during the past year, P2P software has improved the sophistication of its anti-firewall countermeasures. For example, you can configure your firewall to block specific P2P software based on its documented protocol and network port; however, many P2P applications will try alternative ports that your firewall might already allow (e.g., HTTP, TCP port 80). Even if you disallow incoming connections on any ports, the P2P software might recognize this configuration and instead ask to make an outgoing connection, which your firewall might incorrectly classify as an acceptable Web request. This vulnerability results because many firewalls can't differentiate between a legitimate Web request over port 80 and a P2P request over port 80. Sophisticated firewalls that are application aware can sometimes identify and block P2P software trying to hijack another port. The iPrism® appliance incorporates this logic to let you selectively block IM or P2P traffic.

Inappropriate Web Surfing Can be Costly

In addition to the overt security risks brought by phishing emails, fringe sites, and P2P/IM, don't forget about inappropriate Web surfing, which can also be costly to your business. Each business must assess its culture and tailor its Web surfing policies to suit. Some businesses might have legal or contractual obligations that prohibit their users from accessing certain Web sites. For example, a children's care service might offer Internet access for the youngsters, but contractually assure the parents that access to Web sites containing pornography or drugs is prohibited. Other companies might choose to let employees access certain Web sites for business reasons but restrict access to other leisure sites in hopes of improving employee productivity. Finally, in recent years the press has provided a lot of coverage surrounding the legality of handling digital music. To guard against legal liability, some companies are blocking access to Web sites known to host copyrighted materials such as DVD movies or MP3 music.

In these examples you, can see that every company's needs are different. The iPrism's® iGuard database categorizes millions of Web sites into greater than 60 different categories for which you can create filtering rules. The iGuard subscription updates the iPrism® with the latest categories and URLs as new sites come on line.

Not all categories are disreputable, however. For example, iGuard classifies Web sites as Business, Education, Health, and Internet, as well as the fringe sites like Pornography, Malware, and Other Questionable Activities. The *Internet (Web)* group includes categories for *Web Search*, *Email Host* (e.g., Hotmail), and *Online Chat*, and the *Questionable* group includes categories for *Computer Hacking*, *Copyright Infringement*, *Intolerance/Extremism*, and *Profanity*. The richness of the classification lets you pinpoint and filter only those sites deemed inappropriate to your business. Also, by limiting sites that are inappropriate to your business, you might be able to reduce unwanted network traffic. For example, blocking access to Web sites hosting copyrighted DVD movies dissuades users from downloading huge 4.7GB DVD files using your Internet connection, thereby helping to ensure that your bandwidth is available for legitimate business uses.

So far we've looked at several scenarios describing how filtering Web access to specific URLs, IM, and P2P software can help increase the security of your network. Now let's look at how best to use a firewall to manage some of this traffic and also where a firewall alone can fall short.

Managing These Threats with a Firewall Isn't Enough

Traditional firewalls inspect network traffic based on the IP address and network port information. All firewalls block unwanted incoming traffic, and higher quality firewalls let you block specific outgoing traffic. Access control lists (ACLs) are rules that you program into your firewall to tell it what traffic you want to allow or deny. The complexity of creating these ACLs varies by vendor. For example, if you're using a Cisco Systems PIX Security Appliance and you want to block outgoing Web traffic to a specific malicious Web site, you can create a rule such as

```
access-list inside_out deny ip any host 10.0.0.1
```

In this example we needed to identify a few pieces of technical information. We need to know the source IP address range (in this case, any computer, including computers on our internal network), the destination IP address (in this case, 10.0.0.1), and the protocol that we want to block (e.g., all IP protocols). In this example, this ACL blocks anyone behind the firewall from accessing the computer with the IP address 10.0.0.1 using any protocol.

Although this is a very simple example, it's not necessarily the most intuitive nor effective to implement. As you can see, we need the IP address of the blocked Web site, which can be difficult to obtain, especially if the Web site is distributed or uses a content delivery network whereby many IP addresses are associated with one URL. For this reason, it's most effective to block a Web site by its URL. One approach to blocking Web sites by their URLs is to create false DNS entries to these Web sites. However, this approach also requires a manual process of editing your company's DNS server, which some SMBs might not have easy access to if they use their Internet Service Provider's (ISP's) DNS services.

These technical changes can be costly and time consuming, especially if you don't have a network manager, a firewall manager, or someone else on your staff who can configure your firewall or DNS server as your business needs change or new attacks emerge. Because many SMBs hire consultants to configure their firewalls, they might be reticent to make frequent changes due to cost and convenience. As a result, using just a firewall to reliably and consistently filter access to malicious Web sites often becomes inefficient (or impossible).

A Dedicated Appliance—The St. Bernard Software™ iPrism®

A perimeter network security device such as the iPrism® appliance solves the problems we've discussed in this white paper by managing for you the categories of URLs and blocking access based on point-and-click rules that you create. For additional flexibility, you can create multiple profiles of users and grant each profile access to different categories. You can enable your rules based on profiles of users, and users are identified by their username or IP address. For example, you can permit users within your engineering department to access an entirely different set of Web sites than the users in your customer service department can access.

Operational Modes

St. Bernard Software™ designed the iPrism® to deploy into your legacy network topology without needing to create new subnets or re-IP address your firewall or users' computers. The appliance operates in one of two modes—as a proxy or in "transparent" or bridged mode.

Proxy Mode

If you only want to use the iPrism® to manage and block Web-based traffic, you can install the iPrism® as a Web proxy. In this mode, all Web-based traffic (e.g., traffic allowed through Microsoft Internet Explorer—IE) is first sent to the iPrism® where it's inspected and, if allowed, routed to your firewall on behalf of your clients. This type of installation is less invasive to other traffic on your network but doesn't provide as much security as installing the iPrism® device in transparent mode. Also, you must configure every user's Web browser to use the iPrism® as a proxy and then create a firewall rule to block outbound Web traffic except the traffic that originates from the iPrism®.

Transparent Mode

Installing the iPrism® appliance in transparent mode lets you leverage all the device's features. In transparent mode, you install the device between your users and a firewall. Because the iPrism® bridges the traffic, you don't need to change the IP address any of your computers or change any of their settings (e.g., default gateways). In this mode, all network traffic destined for the Internet passes through the iPrism® before it reaches your firewall. Because the appliance sees all your Internet-bound traffic, not just

Web-based traffic as when you install the device in proxy mode, you can enable the IM and P2P management features. When the device is in transparent mode, you don't have to configure any of your clients' Web browser software to use a proxy server. In essence, you drop the iPrism® between your firewall and users, configure it, and all the users will automatically (and seamlessly) be protected by it. This is one of the strongest advantages of using a perimeter network security device such as the iPrism® and because it's designed to work in this manner, you don't have to install additional software or reconfigure or upgrade your firewall to use it.

Managing the Subscriptions

It's important to update your URL filtering rules on a regular basis as thousands of new Web sites come online every day. Performing this update ensures that you're better protected from any possible new "hot" sites for malware/spyware or other propagating threats. Inevitably your users might need to access a Web site that falls within a restricted category. When they attempt to visit this restricted site, iPrism® redirects them to another Web page stating why the Web site was blocked. The iPrism® appliance additionally presents the user with a link to request access to the site. This link in turn generates a request to an iPrism® administrator who can review the request and open the site, if appropriate. Letting your end users make these requests at the time they're blocked makes them feel like they have options and can help improve acceptance of the system. Nobody likes to feel they are blocked—especially if the site they're visiting is for a legitimate reason. Fortunately, the iPrism® makes the process of requesting exceptions easy for your users.

Making Your Own Rules

Even with a frequently updated subscription, there will be times when you encounter a real-time attack or custom phishing attack that you need to block right away. You can often analyze the contents of the attack to discern its propagation or communication mechanisms. For example, if you view the source code (e.g., in Outlook, you can select View Source) of a suspicious email, you can often discern the "real" link the phisher wants the victim to visit. With this information, you can then create a custom filter that blocks this URL or IP address. This important feature lets you quickly respond to the latest threats attacking your company.

Summary

Managing outbound Web traffic, IM, and P2P software increases the defense of your network. The iPrism® appliance augments your firewall to help protect your network in ways that a traditional firewall can not. It inspects the network traffic passing across your firewall and looks at the URLs and allows or denies the request based on rules that you create. Also, you can allow or block most IM and P2P software connections. The appliance uses a subscription service to populate its URL database, which helps ensure that categorizations don't go stale and that new sites are quickly included. This type of perimeter network security solution can be put into place without affecting your current firewall solution and once installed will help defend your network from phishing attacks, IM/P2P usage, and access to inappropriate Web sites.