Global Information Assurance Certification Paper

Effective Logging & Use of the Kiwi Syslog Utility

By

Brian R. Wilkins
CNE / MCSE / CCNP / CISSP

Abstract

The proliferation of the Internet as well as the growth of internal networks have created an increasing need for centralized logging mechanisms and tools for technical personnel to access information regarding network security, connectivity conditions, and other information concerning their networks. Although its' primary function is to provide simple network logging functionality, or syslog (which will be discussed in depth later), Kiwi's syslog utility provides many other logging, filtering, display, and notification options which can help a network professional troubleshoot problems, monitor specific network activity, and perform a variety of other functions with a minimum amount of effort required.

This paper will familiarize the reader with the basics of syslog as defined by RFC 3164, describe some variations of syslog as implemented by various network hardware vendors, provide an overview specifically of Kiwi's syslog utility and its' functionality, demonstrate basic configuration of the syslog utility, and finally provide examples of some advanced configurations of the syslog utility that will offer specific automated functionality tailored toward specific needs. Screenshots and other information will be presented in order to provide a clearer understanding of how to accomplish these tasks using the utility. After reading this document, a security professional should have a good understanding of how Kiwi's syslog utility could be implemented to provide an effective means of providing network information used for a wide range of tasks.

Introduction to Syslog

What is syslog? Syslog is defined by RFC 1364 in the following way; **"**In its most simplistic terms, the syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors - also known as syslog servers".
See the following URL for the full RFC:
http://www.ietf.org/rfc/rfc3164.txt?number=3164.
"Machines", as referenced in the definition is a very broad term which could represent a P.C. running nearly any operating system, servers running various operating systems, network devices such as switches, routers, firewalls, or other devices. The important thing to note for our purposes here is that the "machine" must have the ability to send syslog messages.

So what is a syslog message? A syslog message is a message that is generated by a machine capable of doing so and transmitted via the IP protocol to another machine (usually a server) that collects the messages (this would be known as the syslog server). The messages themselves may contain any sort of information that the syslog-capable machine is able to generate and send. For example, it is common for a router to be able to generate and send a syslog message when one or more of its' interfaces changes from an "up" state to a "down" state or vise-versa. A router could also be configured to generate syslog messages when access control lists (or ACL's) are violated. These messages are then sent across the network to a syslog server, as configured by the device itself. If, for example, we would like an Ethernet switch to send a syslog message to a syslog server each time an interface changed states, we could configure the specific parameters on the switch to send a syslog message on such an event and we would also provide the switch an IP address of the syslog server somewhere in its' configuration. It is important to note that the device sending the syslog message to the server must be able to establish network connectivity with the syslog server, and both the syslog server and the device sending the message must understand the formatting of the syslog messages.

As often is the case with network device vendors, the actual implementation of certain standards are interpreted differently, and thus the way one vendor implements syslog capabilities on their devices may differ from the way another vendor does it. This is normal and can be handled fairly easily as long as the vendor's implementation of syslog remains somewhat consistent with the "norm" and the syslog server (the server running syslog collection software) is able to interpret and handle the messages appropriately.

Syslog, like any other network communications system, can have certain vulnerabilities associated with it, which must be examined prior to implementation. For example, Unix servers that have a built-in syslog service (which is not what we are referring to here, as Kiwi syslog is a Windows-based product, were recently subjected to several threats related to vulnerabilities in another service, sendmail). For additional information on these vulnerabilities, see the following link:
http://www.cctec.com/maillists/nanog/historical/9510/msg00137.html

Since Kiwi syslog is a Windows-based application, it was not vulnerable to this threat. However, other vulnerabilities do exist that the reader should be aware of, such as specific

vulnerabilities within certain Cisco product operating systems which have caused the operating systems of those devices to hang when a packet on the syslog port was received. For more information on this specific vulnerability, see the following link:
http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

Syslog message delivery between the sending device and the syslog server is not guaranteed. It is a "best-effort" protocol. There are, however, discussions underway to make changes to the protocol which would insure reliable delivery and add security features such as authentication and message replay prevention. This is a brand new initiative, so there isn't a lot of information yet, but what is available can be found on the IETF's website at the following two URLs:
http://www.ietf.org/html.charters/syslog-charter.html

http://www.ietf.org/internet-drafts/draft-ietf-syslog-sign-06.txt

Overview of Kiwi Syslog

There are numerous companies that offer syslog server software. The prices range from free to thousands of dollars, usually depending on the functionality, interoperability with specific vendor's products, and other factors. Kiwi Enterprises is a New Zealand based company which produces several low-cost network management products. Among these is Kiwi's syslog daemon. A "daemon" is simply another word for "service". Kiwi's syslog software is simply a software package that will run on any Windows 95, 98, ME, NT, 2000, or XP based workstation or server. It collects syslog messages that are sent to it and takes whatever action is defined in the configuration. As far as price vs. functionality goes, Kiwi offers (in my opinion) very nice functionality at a very low cost. They offer a freeware version that contains most basic functionality. For full functionality, a license may be purchased for $69.00 (U.S.), with lowered pricing for additional licenses or upgrades (which are free for minor version upgrades). The software can also be downloaded in either an executable format, or in a service format. They both operate essentially the same, except that the service format has the advantage that since it is a system service, it can be started without requiring user login, which is nice if you ever need remotely reboot the server, because no login is required to start the syslog software. Several vendors also either recommend or specifically mention interoperability with Kiwi's syslog software product including the following examples:
Extreme Networks
http://www.extremenetworks.com/support/ewrecommendednetworks.asp

Network-1 Cyberwall Plus
http://www.network-1.com/website/products/centralized/centralized.asp

The installation of Kiwi's syslog server is simply to download the software from their website and run the setup program. Then, depending upon your operating system, a reboot may be required. Once this is complete, the software is ready to use. Since this document is aimed at a fairly technical audience, I will forego all of the details of the

installation except to say that it is very straightforward, simply asks for the installation path, requires you to press "next" a couple of times, and takes about five minutes.

Basic Configuration

The first step in the configuration is to start the syslog server software. This is done through the start menu, just like any other software. The default configuration will be for the software to display all messages received on the screen, and to also log them to a file named "SyslogCatchAll.TXT" which will reside in the installation directory, unless you specify otherwise. Once you maximize the screen, you will have a table (as shown below) listing date, time, priority (used with some syslog generating devices), hostname (which will be replaced with the IP address if it cannot be resolved via DNS), and message. This table shows syslog messages in real-time as they are received. The "hostname" will show you what host the message came from, and the message will be somewhat dependent upon the device that sent the message. For example, messages sent from a firewall will look different than messages sent from an Ethernet switch because they perform different functions and also may be from different vendors. The message portion is generally the important part, or "the meat" of what you are looking for. It is a good idea to initially leave the configuration as-is initially so that you can quickly tell if your devices are sending syslog messages to the server simply by looking at the screen. As you get into more advanced configuration, you will find that generally there are a lot of messages and it may not make sense to continue to display all messages on the screen, but rather to restrict those to simply messages that match some specific criteria.

The next step in configuration is to setup syslog-capable devices to both generate messages and send them to the IP address of the server that you have just installed the syslog software on. The configuration of specific devices is beyond the scope of this document and is dependant upon the device and its' manufacturer, but generally there are various logging "levels" that can be set on the devices that will define how much detail and what types of information to send to the syslog server. For specific information on how to configure your specific device to generate and send syslog messages, you should check with the hardware vendor. Since Cisco products are widely used, I have listed a couple of URLs at the end of this document that explain specifically how to configure various Cisco devices to use syslog.

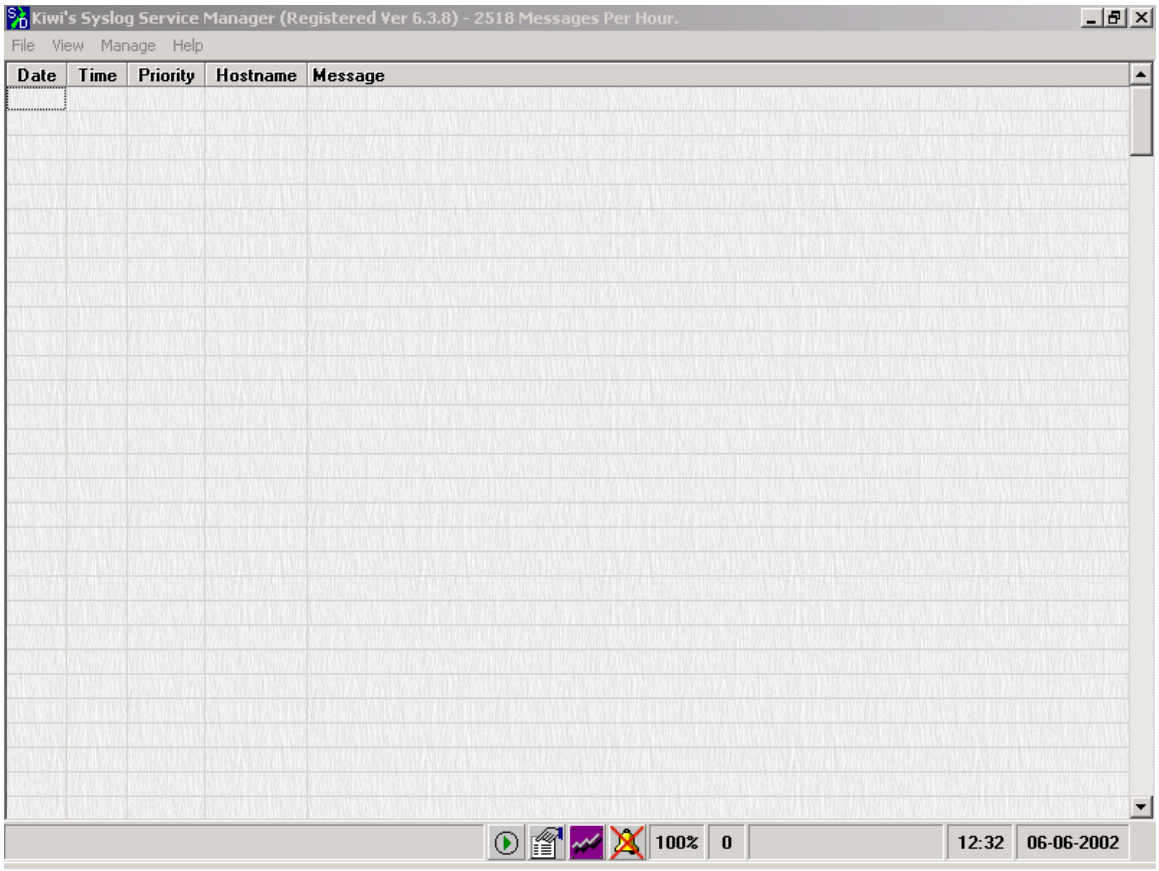
At this point, assuming that the conditions on the devices that you configured are being met to generate syslog messages, you should be seeing the messages on the screen of your syslog server. If your devices do not appear to be sending syslog messages to the server, Kiwi offers a free utility that can be installed on a PC and simply sends test syslog messages so that you can verify your installation. The utility may be downloaded from the same site as the syslog software. This concludes basic configuration.

Advanced Configuration & Sample Uses

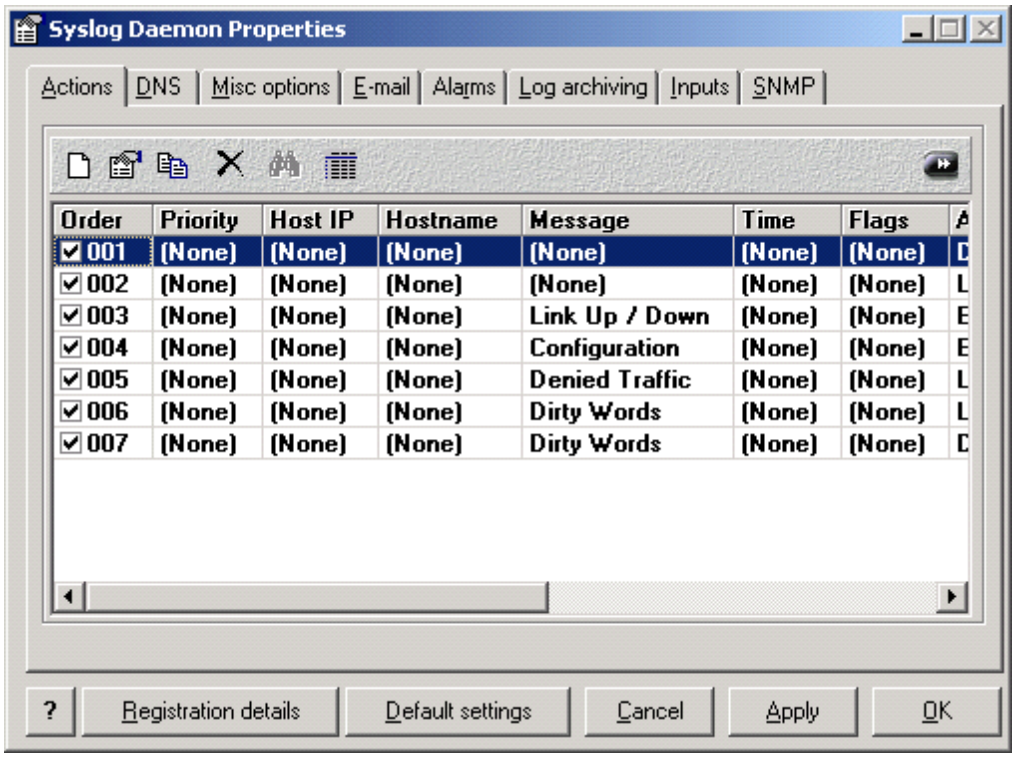
In this section, we will describe some of the more advanced functionality and how to

configure it in Kiwi's syslog server software so that the software becomes a very usable tool and not simply a logging mechanism.

For reference purposes, the following is a screenshot of Kiwi syslog's main screen as described above:

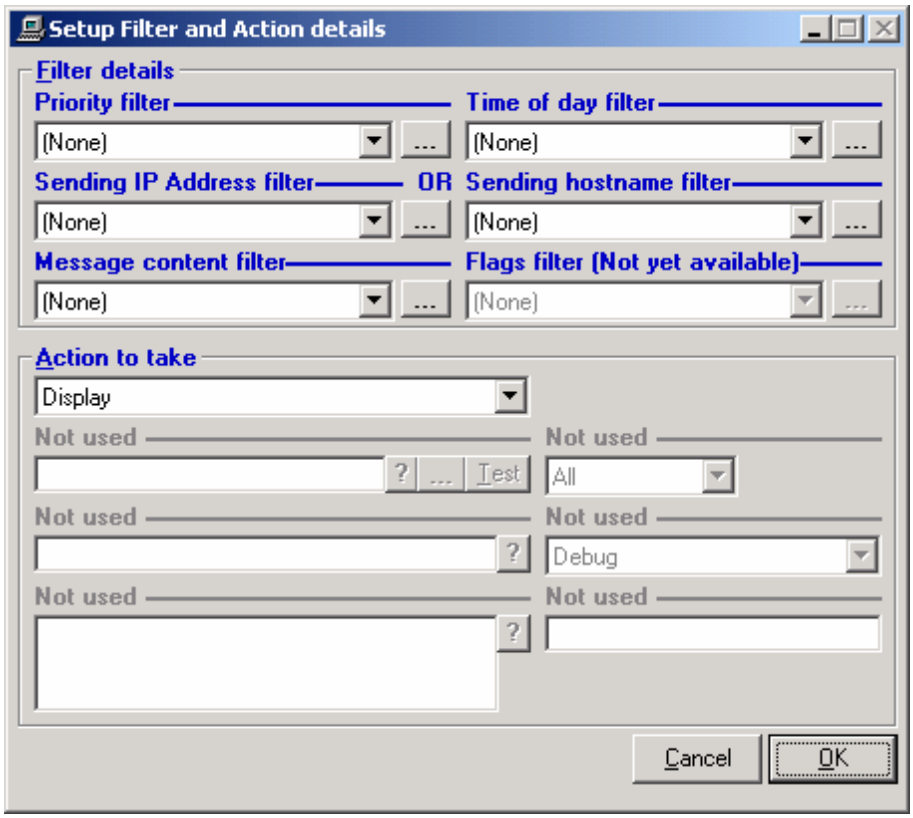


You will notice the columns at the top as discussed earlier. The toolbar at the bottom of the screen contains a "go / pause" button, as represented by the green arrow. If we wanted to pause the display because messages were coming through very quickly and we wished to analyze some of the messages, clicking the green arrow would pause the screen until we clicked it again. The button to the right of the green arrow will bring up the "properties" screen, which appears as follows:



From this screen, we can define and enable or disable (as identified by the checkboxes) all of the actions, options, filters, and all other parameters of Kiwi syslog. The list shown indicates seven actions that have been defined on this syslog server. The "Message" column indicates which (if any) filter triggers the specified action. In the case of the first two, they are the default actions which are present right after installation. These two, by default are configured to use no filters, but to display all syslog messages on the screen, to write all messages to the "SyslogCatchAll.txt" file. The remaining actions were defined by me and some will be shown as examples of how to use Kiwi syslog effectively.

Clicking the white-page icon on the toolbar here will bring up "Setup Filter and Action" screen shown below:



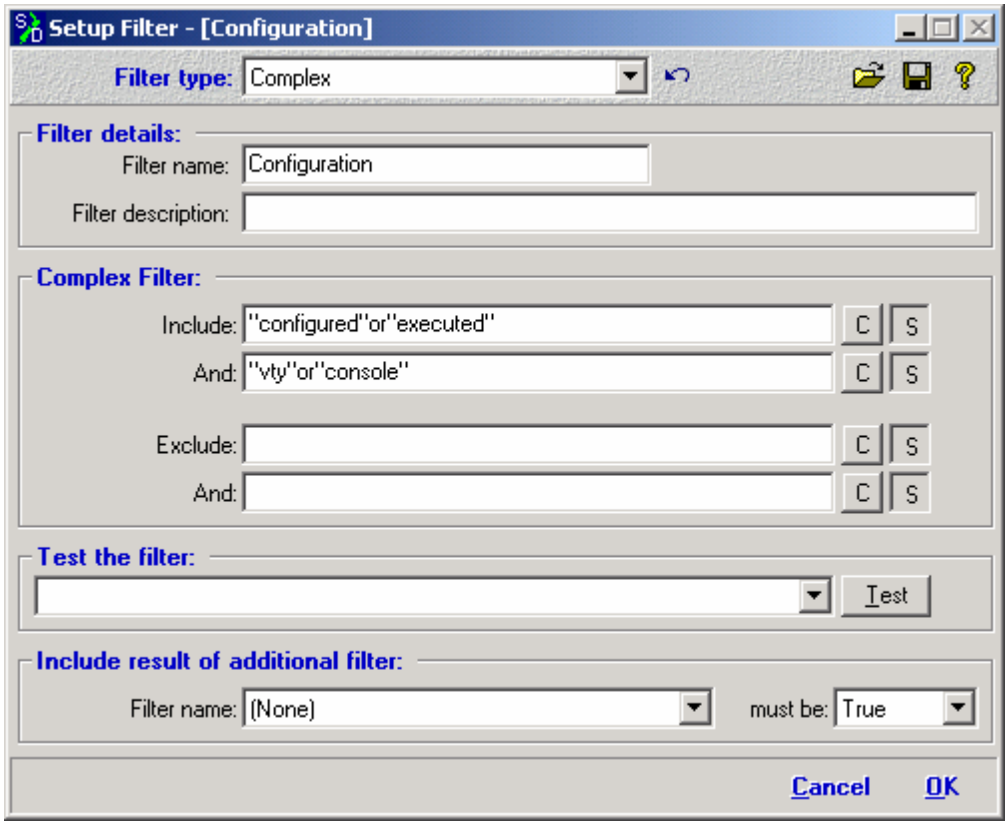
On this screen, we can define filters and actions which would then be displayed after the last item on the previous screen, (SYSLOG Daemon Properties). Under "Filter Details", if we have already defined a filter, we can simply select it from the drop-down box. Otherwise, we can click the icon next to the drop-down box and create a new one.

Filters and actions are where Kiwi syslog really shine!!! This is where you have the capability to (with very little effort) setup the application to examine syslog messages and take action based on those. This goes beyond simple logging to text files. Next we will see some examples of how to use this facility effectively.

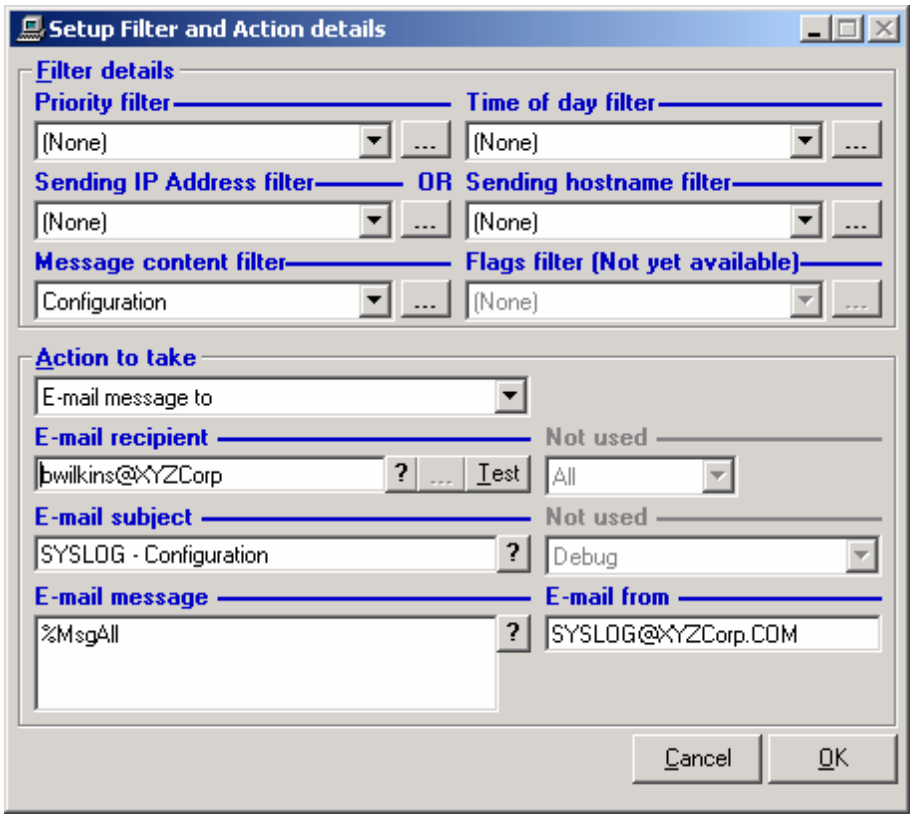
Example 1. Suppose I wanted to be notified by email anytime someone logged into a router or switch and performed some type of configuration. By clicking on the "Message Content Filter" button above, this screen will appear. From the drop-down box, I have chosen "Complex" for the filter type. Complex filtering allows for inclusions and exclusions using logical "and's" and "or's".

In this example, we have created a filter arbitrarily named "Configuration". For this filter, we have told Kiwi syslog to look for the words "configured" or "executed" in the syslog message, but the message must also include "vty" or "console" due to the "and" portion. In effect, what occurs is this: when someone logs into a router that is configured to send syslog messages to this syslog server, if they enter configuration mode and then exit out, a syslog message will be sent that reads something similar to "*IP Address* configured by

console" or "*IP address* configured by VTY*x*". The IP address would identify the device. The message sent to the syslog server would match this filter, so the syslog server would check to see what action is associated with this particular filter. Note: for the examples above, these are specific to Cisco devices and may be different for other vendors. The basic concept, however, is the same.



Once we click "OK" and get back to the "Setup Action and Filter Details" window, we can now assign an action to this filter. The screenshot below shows what we have configured the syslog server to do if it makes a match on this filter:



In this case, we have configured Kiwi syslog to send an email from "syslog@xyzcorp.com" to "`bwilkins@xyzcorp.com`". The "Test" button next to "E-mail recipient" will send a test message to verify that the email settings are correct and functional. The "%MsgAll" parameter under "E-mail message" is an application parameter that simply indicates that it should send the entire syslog message that was received. Clicking the "?" help button next to each box will bring up the help screen for that particular box. For the "E-Mail message" box, you can find all of the available parameters such as the "%MsgAll" mentioned above so that you can customize the message to your preferences. Note that this can also be combined with other filters to make it even more customized to your particular needs. For example, if we only wanted these email messages to be sent during certain times of the day, we could also apply a "Time of day" filter as well.

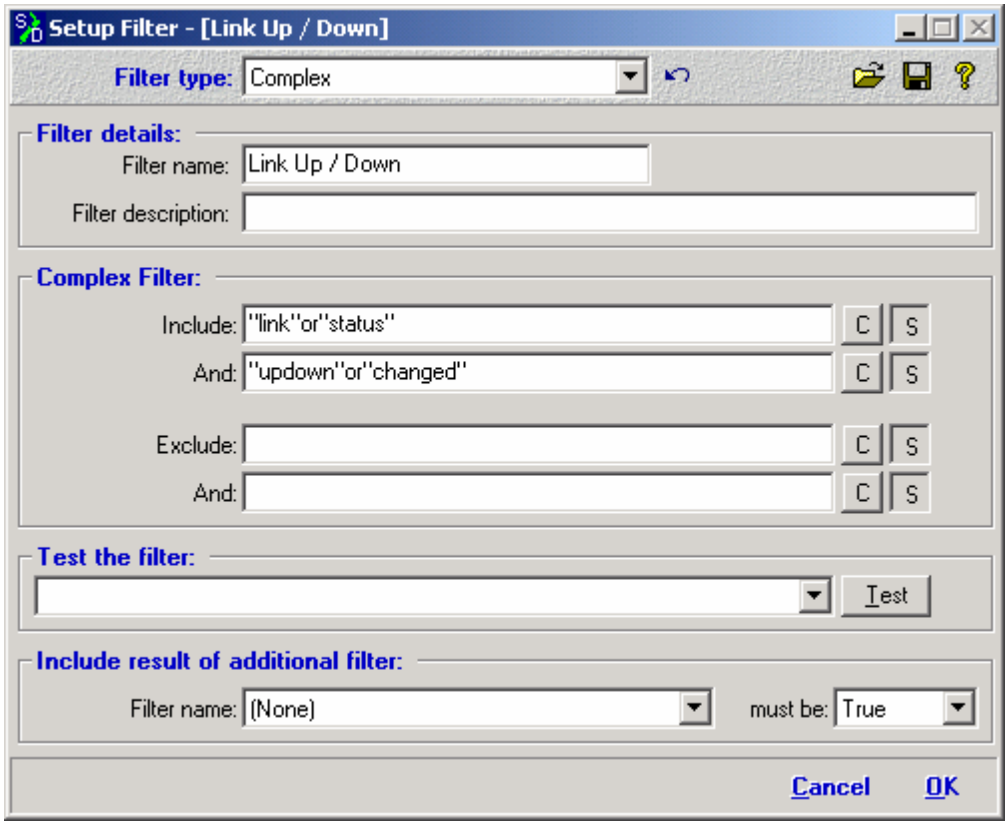
In essence, what we have created with a very easy to build filter and action, is a simple configuration management tool and quasi-intrusion detection system for any devices that are sending syslog messages to this syslog server. For example, if Joe is the only one authorized to login and make changes to routers or switches, and this particular filter and action is set to notify Joe, he will get a notification anytime someone logs into a router or switch and makes changes via email (under this example). Joe obviously knows whether or not it was him, and if it wasn't, he has now been notified and can take appropriate action based upon the security policy. He will likely also have the IP address of the

unauthorized individual contained within the message unless the action was performed from the router's console.

-

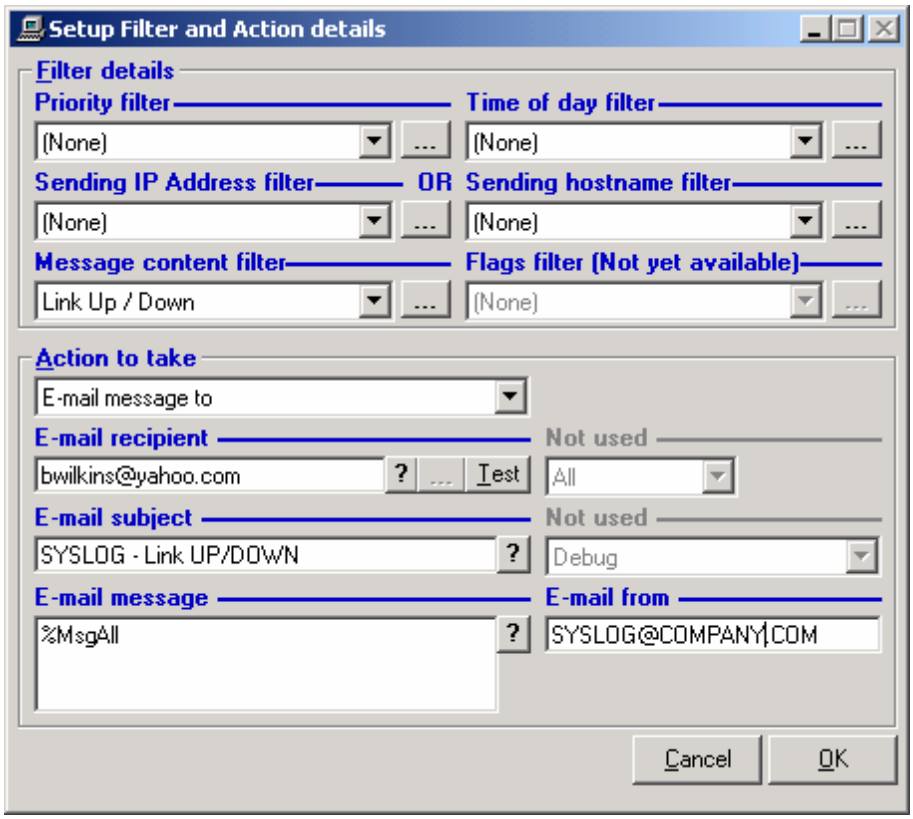
Example 2. For this example, let's assume that we have a mission-critical network link and we need to be notified anytime it goes down. If our router has syslog capabilities, we can simply setup an action / filter in Kiwi syslog as shown below:

First, we setup the filter to look for syslog messages containing the words "link" or "status" AND either the word "updown" or "changed". These are typical messages of Cisco routers, but may be different for other vendors.



Next, we setup an action to email `bwilkins@yahoo.com` a message stating that the link has gone up or down. As you can see, we have even included "Link UP / DOWN" in the subject line, so that the email recipient can see what is occurring even before opening the

email.



We could also combine this Action / Filter with others to create more complex filters such as time of day or restricting it to a device or group of devices based upon IP address. It is important to reiterate here that the device sending the message MUST have network connectivity with the syslog server for this to work. So, in the above example, if the link that went down happened to be the link that connected the router to the syslog server, this would not work. For this reason, it might be appropriate to not only have a filter and action defined for the router, but also the device that is connected to the router (a switch, for example). Then we would still get our notification. In essence here, we have used Kiwi syslog to create a basic network monitoring and notification service.

Other Examples – As you can see from the two above examples, Kiwi syslog can simply read the contents of each syslog message and take whatever action is defined. In our examples, we sent notification emails. These could also be sent to wireless devices that accept email, which is done frequently. They could also just as easily be written to a separate file, other than the normal SyslogCatchAll.txt. Another nice feather is that all files that are created as the result of a filter / action rule are automatically included in the archiving process which is discussed later.

Suppose your company policy states that employees are only allowed to visit work-related websites. Certainly there are systems that can be purchased to restrict access to

inappropriate websites, but to add an additional layer of protection, or to simply see if employees are attempting to visit inappropriate sites that might contain pornographic material, for example, we could setup a filter, (in this case, we called it "dirty words") and then have our firewall send syslog messages to the Kiwi syslog server for every URL request. In the filter, simply create a long list of words that might be found on an inappropriate website (I'm sure you can think of at least a few words that would likely only be found on such a site). Then have Kiwi syslog log those attempts to a file. If you review the file on a regular basis, you may find attempts (successful or unsuccessful) to gain access to inappropriate websites. To enable a Cisco PIX firewall to send syslog messages to your syslog server which contain the URLs, specific instructions may be found at the following link:
http://www.cisco.com/warp/public/110/pixsyslog.html

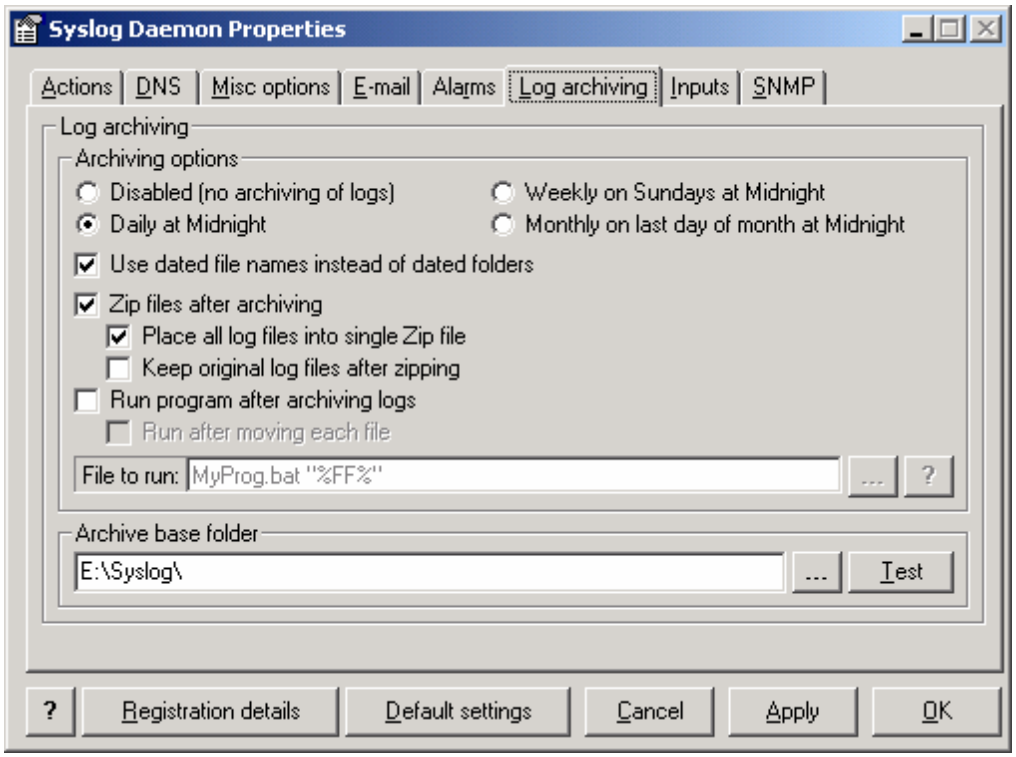
Please note that the more information you request firewalls, routers, or other devices to send via syslog, the more processor utilization will incurred on those devices as well as the syslog server, more disk space will be consumed on the syslog server, and more network traffic will occur. These considerations need to be balanced with the true organizational needs.

For specific instructions to configure Checkpoint firewall / VPN server for syslog, information may be found at the following link:
http://www.opsec.com/solutions/partners/downloads/fireproof_setup_guide.pdf

You could also just as easily create a filter to match only a single IP address. This would give you the ability to monitor the activities of a single device on your network.

Troubleshooting with Kiwi syslog can be achieved in a number of ways. For example, suppose you recently installed a new V.P.N. server on your network, but people are unable to connect to it. One method of troubleshooting might be to configure an access-list on your router that matched the ports used by the V.P.N. and have anything that matched that ACL sent to the syslog server. If your V.P.N. server has syslog capabilities, you could also set it to log to the syslog server and monitor it that way as well. The same type of troubleshooting could just as easily be performed for any ports or services. It is usually a good practice to either setup a file specifically for the matches that you are looking for, or to display ONLY those matches on the screen. When monitoring multiple devices it is important to be able to sort and disseminate the information in a way that is usable. Firewalls, routers, and switches can send especially large volumes of information to a syslog server so it is important to understand what is being displayed or logged and why.

Archiving – All of the messages received by Kiwi are stored in simple text files. You may optionally have these files archived on a periodic basis. Depending upon your industry and your security policy, this may also be a requirement. The screenshot below shows the archiving options:



In this example, we have configured Kiwi syslog to archive the log files daily at midnight into a folder named "syslog" on our E: drive. We have also indicated that we would like it to use the dates of the log files for the filenames and to place all of the log files from each day into single Zip files. These zip files may be opened using any file compression utility that works with the "zip" format. This functionality is also automatically built into Windows XP. You will notice that there are also options to perform backups on a weekly or monthly basis, as well as the ability to simply disable it.

Another option that can be used within this configuration screen is the ability to run a program after archiving the logs. This could be very useful for copying the files to a secondary location for backup. Again, depending upon your industry and / or security policy this may be something that is required and could be performed very easily though a small batch file.

Security Policy

It is important that your implementation of any syslog server be in accordance with your company's defined security policies. If you do not have a security policy specifically addressing syslog, it may fall under the umbrella of another policy or procedure, but a policy and procedures specific to syslog should be written if they are not already in existence. Some issues that should be addressed in a syslog security policy are as follows:

- How is the service implemented?
- What is being logged?
- Who is responsible for maintaining the server?
- Who is responsible for maintaining the logs?
- Who is responsible for reviewing the logs?
- What action should be taken if events occur that are caught by the syslog server that violate other policies?
- What are acceptable uses of the syslog server beyond simple logging, such as troubleshooting, monitoring links, etc.?
- Who is responsible for adding or removing these other services that the syslog server may be performing such as those mentioned above?
- What is the policy for retaining the log files?
- Who is responsible for long-term log file retention?
- How are log files secured so that only those with specific clearance are allowed to review them?
- Other industry or company specific policies that may be applicable.

References

Kiwi Enterprises Website
http://www.kiwisyslog.com/index.htm

IETF Syslog RFC

http://www.ietf.org/rfc/rfc3164.txt?number=3164

IETF Syslog Security Charter
http://www.ietf.org/html.charters/syslog-charter.html

Cisco-specific instructions to enable syslog functionality
http://www.cisco.com/warp/public/477/RME/rme_syslog.html#task1

Extreme Networks Recommended Tools
http://www.extremenetworks.com/support/ewrecommendednetworks.asp

Network-1 Cyberwall Plus syslog interoperability
http://www.network-1.com/website/products/centralized/centralized.asp

Cisco PIX firewall instructions to configure syslog
http://www.cisco.com/warp/public/110/pixsyslog.html

Cisco syslog exploit vulnerability information
http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

Checkpoint-specific instructions for configuring syslog
http://www.opsec.com/solutions/partners/downloads/fireproof_setup_guide.pdf

CERT advisory regarding Unix –based syslog
http://www.cctec.com/maillists/nanog/historical/9510/msg00137.html