Activeworx IDS Policy Manager 2.0: Rules management for multiple sensors

By Russ McRee

Prerequisites

Snort 2.4/2.6

Windows 2000/XP/Vista

.Net Framework v2.0

Introduction

If you've ever managed or deployed an IDS, odds are pretty good it was a Snort® unit. Sourcefire claims 3 million downloads and 150,000+ active users, and for good reason. I too am unabashedly a huge fan. As many as 45 commercial products, including ISS, use Snort as part of their offering[1]. Additionally, there are a number of other related products or open source tools to aid in your Snort use, such as Aanval, BASE, or Oinkmaster. There's even an open source offering called SnortCenter that resembles IDS Policy Manager (IDSPM).

I've chosen to cover IDSPM, first as an active user of their 1.8 version – and they've reached 2.0.0.7 beta for their next version. This version has a lot to offer for those among us who actively manage a number of Snort sensors. By the time you read this column the final version of 2.0 should already be available, as of December 17th. According to Activeworx:

> *IDS Policy Manager was written to manage SNORT® IDS sensors in a distributed environment. This is done by having the ability to take the text configuration files and allow you to modify them with an easy to use Graphical interface. With the added ability to merge new rule sets, manage preprocessors, configure output modules and securely copy rules to sensors, IDS Policy Manager makes managing Snort easy for most security professionals"*[2].

IDS Policy Manager was first released in 2000, was the first rules manager for Snort, and has over 10,000 users worldwide. One of the biggest benefits is active development, with a developer who listens. Activeworx indicates that the "new features in IDSPM are really user driven…we get a lot of suggestions from people and most of them are usually added. As long as it can benefit others and it continues to take the product in the right direction, they get added."

Feel free to submit requests or suggestions to idspm@activeworx.org.

1 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1069213,00.html

2 http://activeworx.org

There are numerous features now offered in IDSPM v.2, including:

- The ability to quickly disable/enable a rule across all policies
- The ability to use the same policy for multiple sensors, and set variables on the sensors to change specific values for the sensor policy when it is uploaded, thereby needing to maintain only one policy and push it to multiple sensors
- The ability to add suppress/threshold events from a certain ip/block when viewing a rule
- While updating the policy, you can now enable or disable rules before they are added to the policy
- Update from bleedingthreats.com, Snort community and any other rules locations
- IDSPM v2 stores all information in a database to enhance ability in working with multiple policies and sensors
- Windows Vista is a supported OS for IDSPM

For the Linux purists amongst us, keep in mind, this is a Windows tool, wherein you might run your preferred distro on your sensors. But to manage them via IDSPM, you must have a Windows workstation available.

Basic configuration

I manage IDS sensors differently, depending on how much traffic they are likely to process. Accordingly, I may use a smaller rule set under high traffic to avoid dropped packets, and where overall traffic may be less, I might enable more rules.

Therefore, when using IDSPM, I keep a few different policies.

IDSPM is of little use without defined policies (not unlike organizations trying to enforce infosec standards). To tune IDSPM for regular use, follow these critical steps. While I don't normally like to spend time on installation or configuration, in this case, my time spent optimizing and learning IDSPM v.2 may, hopefully, save you some time, as the process order plays a role in your success.

Step 1 – Settings and Update Locations

First, you must establish your Update Locations by choosing *Options*, then *Settings*. The Settings menu will allow you to enter your Oink Code. If you don't have one, let me suggest getting one by registering at Snort.org here: https://snort.org/pub-bin/register.cgi.

Select Update Locations then Add Update Location. You'll note Snort versions 2.4 and 2.6, as well as one of my favorite community

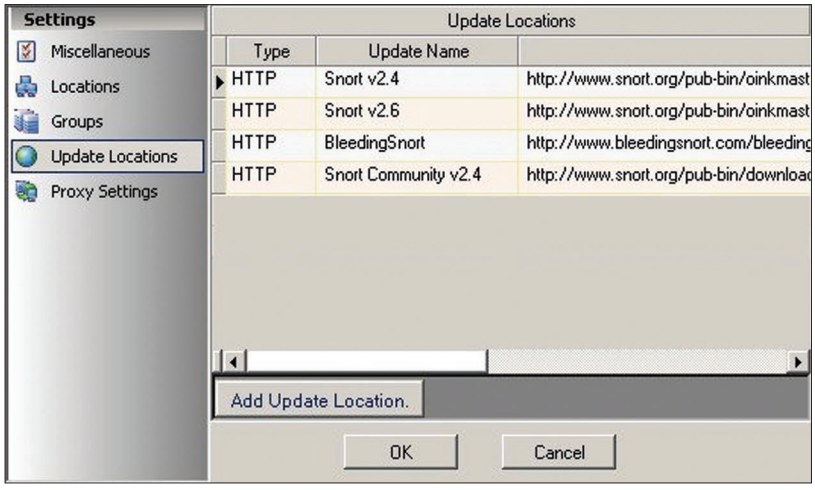

Figure 1 – Setting: Add Update Location

efforts, Matt Jonkman's BleedingSnort, now Bleeding Edge Threats. If you're new to Snort, definitely visit this site and consider contributing suggestions or rules you've written.

A personal note: Depending on the amount of traffic you're monitoring, as well as the number or nature of rules you may have enabled, you may be dropping packets. While more the subject of Snort IDS management guides and manuals, keep this in mind as you manage your policies and be wary of the issue.

I maintain policies locally on a fileserver, and have added the locations as a File type rather than HTTP, with the appropriate path according to what policy is best for the amount of traffic monitored as well as where the sensors live in our network topology.

Other optional settings include the opportunity to establish Location and Groups. With multiple sensors, in multiple locations, and a variety of monitored traffic patterns, this can be quite handy from an organizational perspective.

Under Miscellaneous, also take note of schedule setting for your update and database backups.

Step 2 – Add Policy

In the default IDSPM view you'll see Snort Policies. Right-click Snort Policies and choose Add Policy. Choose your version of Snort under Policy Setting and add the update location you defined in, yep, you guessed it, Update Locations.

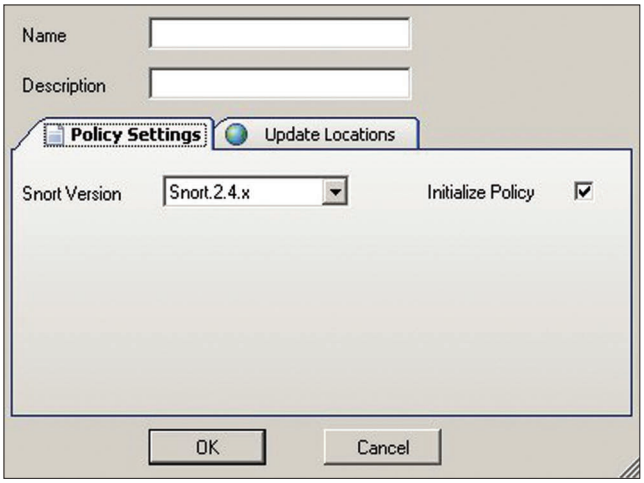

Figure 2 – Add Policy

Step 3 – Add Sensor

Again, starting from the default view, select *Snort Sensors*, right-click and click *Add Sensor*. You'll note a number of tabs; all are important or useful. When you name your sensor host, you'll also choose the policy or one of the policies you defined in Step 2. You may also choose from groups or locations as established in Step 1.

Of vital importance is the Authentication tab. Snort best practices suggest the use of a unique account to run Snort (running as root is a huge no-no). For a great Snort install doc, I suggest Patrick Harper's doc here: http://snort.org/docs/. You'll enter these credentials under Authentication.

Equally important are the Upload Settings. Please don't bother with any method other than SFTP. It'd break my heart to hear of a Snort sensor running FTP. Be certain to define the exact directory where your rules and snort.conf reside on the sensor in the Upload Directory field. It is best, if not imperative, when using IDSPM to keep your rules files and snort.conf in the same place.

Under Add Sensor you may also take advantage of unique variables you wish to define, as well as sensor restart options. I've not yet spent a great deal of time using either of these so I'll not offer any feedback.

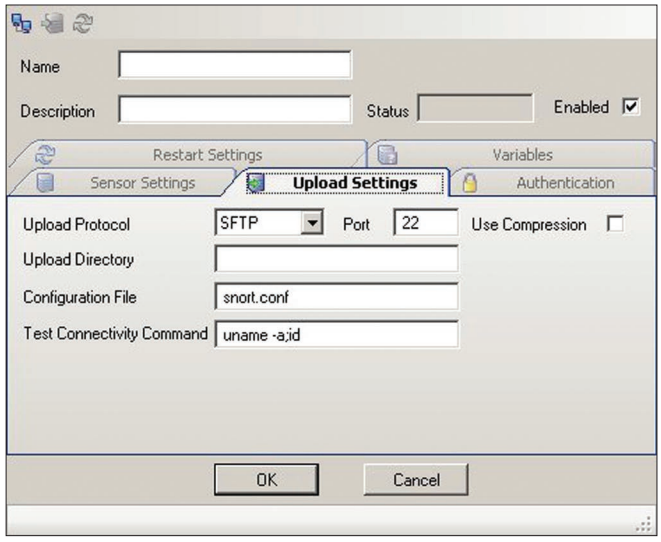

Figure 3 – Add Sensor

Use scenarios

Now that you have this most productive tool configured, how now to put it to good use?

Spyware be gone

Let's consider this scenario. A recent implementation of stringent spyware controls has established that there is no longer a need to monitor spyware traffic, and you'd like to disable all *spyware-put* (all 641 of them at the time of this writing) rules in your policy.

Expand your policy list in the default view, select the relevant policy, and expand it in the left pane until you can highlight the Rule Groups heading. Then in the right pane, highlight the spyware-put ruleset and select Disable Item. The names of my policies and sensors have been masked in successive screenshots to protect the innocent.

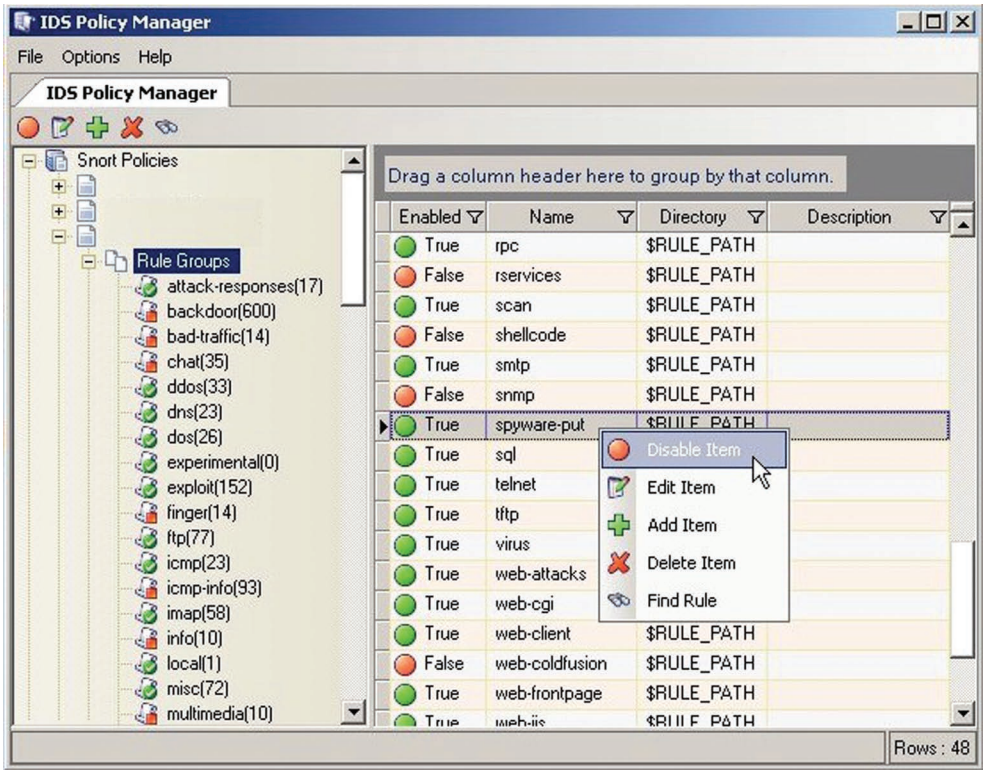

Figure 4 – Disable Rules

Once you've confirmed a disabled state by taking note of the red "false" icon, it's time to update your policy to your sensors.

Revert to the default view, select Snort Sensors, select the sensors you wish to update (holding Shift while selecting will allow multiples), right-click and select *Upload Policies to Sensors*.

An *Update Server Policies* window will open, allowing you to simply check the correct sensors and click *Start*.

While I tend to happily right-click, keep in mind that options such as *Upload Policies to Sensors* or *Disable Item* are available as icons on the menu bar above the left pane.

Suppress me

Another probable scenario is one of a false positive that is consistent in your environment and can be suppressed across the board.

As an example, we'll assume that all traffic from an internally hosted vulnerability scanner is to be considered legitimate traffic throughout your environment. Accordingly, you don't want any alerts from the scanner showing up on your IDS console or SEM.

Select the relevant policy and expand until you can highlight the Suppressions heading. Do so, then right-click in the right pane and choose *Add Item*.

Set the Generator ID to 1, leave the Signature ID blank because you're suppressing *all* traffic from this host, opt for Track by src, as your scanner's IP is the source traffic, then enter the scanner's IP address.

It's that simple, and again, follow the same before-mentioned process to upload the policy to the appropriate sensors.

IDSPM roadmap

The developer has indicated that a number of features will be added in version 2.1, including:

- SCP/SFTP support, to download existing policies from sensors and import them
- The ability to load configuration options from a text box. You could paste thresholds or suppressions into a text box, in turn, installing them into a policy

Conclusion

For the Type A personality in all of us (Hi, I'm Russ, and I'm a control freak), there's no better way to manage all your Snort sensors than from one centralized, powerful, easy-to-use platform like ID-

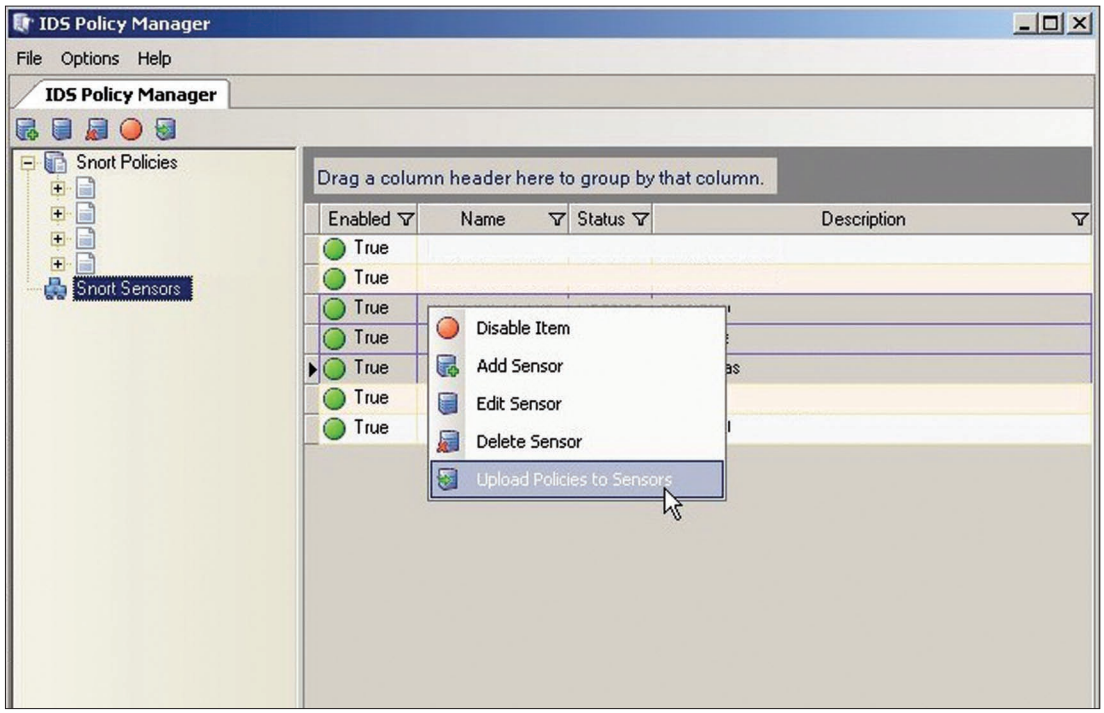

Figure 5 – Upload Policies

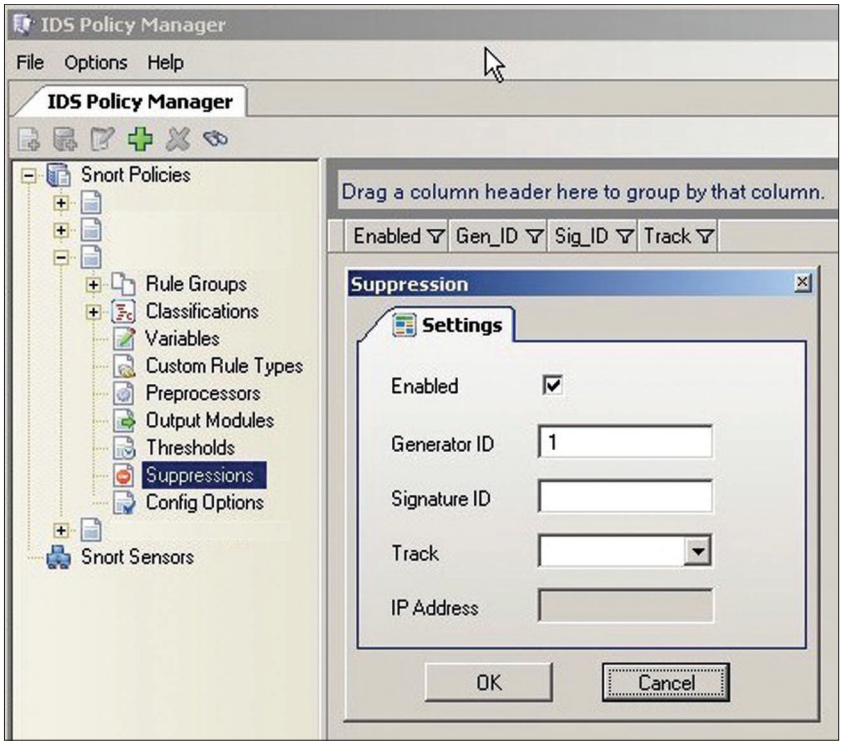

Figure 6 – Suppression

SPM v.2. Stay tuned for further development from Activeworx, and remember to offer suggestions or requests for additional features. This tool truly exists to help you do your job more easily. Until next month…

Legalese

Snort is a registered trademark of Sourcefire, Inc.

Acknowledgments

Russ would like to thank Steve Lynch for introducing him to IDSPM v1.8 and for heckling him until his dropped packets fell below 25 percent in high-volume environments.

Russ would also like to thank Jeff Dell, IDSPM's developer, for his feedback and contributions to this month's column.

References

http://activeworx.org/

https://snort.org/pub-bin/register.cgi

http://oinkmaster.sourceforge.net/

http://bleedingthreats.com/

About the Author

Russ McRee, GCIH, is a security analyst working in the Seattle area. He is a member of ISSA, Pacciso, InfraGard, and CCSA (Cyber Conflict Studies Association). Russ maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.