

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 1



IBM Security Network Intrusion Prevention System V4.4

Adding and importing SNORT rules



Security Intelligence.
Think Integrated.

Smarter security solutions from IBM



This is a self-running demonstration that shows you how to complete a task.
Controls are available at the bottom of the screen.

© Copyright IBM Corporation 2012. All rights reserved.



Objectives

When you complete this module, you will be able to perform these tasks:

- Add a SNORT rule manually
- Import a SNORT rule

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 3

The screenshot shows the SiteProtector interface for configuring SNORT rules. The window title is "SiteProtector" and the menu includes "Object", "Edit", "View", "Action", "Tools", and "Help". The address bar shows "Go to: Edit Policy". The main content area is titled "SNORT Configuration and Rules : Default : version 1 (Default Repository)" and has three tabs: "SNORT Execution", "SNORT Configuration", and "SNORT Rules".

Under the "SNORT Rules" tab, there is an "Import SNORT Rule File" section with a text box "Update 'Rules' below with contents of file(s):" and a button "Select *.rules file(s) to import...". A yellow callout bubble points to the "+" icon in the toolbar, stating: "To add a SNORT rule manually, click the **Add** icon."

Below this is a "Rules" section with a toolbar containing icons for edit, add, delete, import, export, and filter. A table is displayed with the following columns: "File", "Enabled", "SID", "Message", and "Rule String". The table is currently empty.

A purple callout bubble at the bottom of the table area contains the text: "This demonstration shows you how to add and import SNORT rules on the SNORT Rules tab of the SNORT Configuration and Rules policy. SNORT must be enabled on the SNORT Execution tab. This task has been performed for you."

The bottom of the interface includes a "Find..." search box, the user name "administrator", and a "Notifications" icon.

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 4

The screenshot shows the SiteProtector interface for configuring SNORT rules. The main window is titled "SNORT Configuration and Rules : Default : version 1 (Default Repository)". A sub-window titled "Add Rules" is open, showing the following fields and options:

- Enabled
- SID: 0
- File: [empty]
- Message: [empty]
- Rule String: [empty] (highlighted with a red box)
- Comment: [empty]
- Display: Without Raw
- Severity: medium
- User Override
- Responses: Email, Quarantine

Three callout boxes provide instructions:

- A yellow callout points to the "Enabled" checkbox: "In the Add Rules window, verify that the **Enabled** option is selected."
- A yellow callout points to the "Rule String" field: "In the Rule String field, type a SNORT rule."
- A blue callout points to the bottom of the "Add Rules" window: "Since the Network IPS does not check SNORT rule syntax, review the integrity of your rules using a SNORT rule syntax checker such as [Dumbpig](#) or [Oinkmaster](#)."

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 5

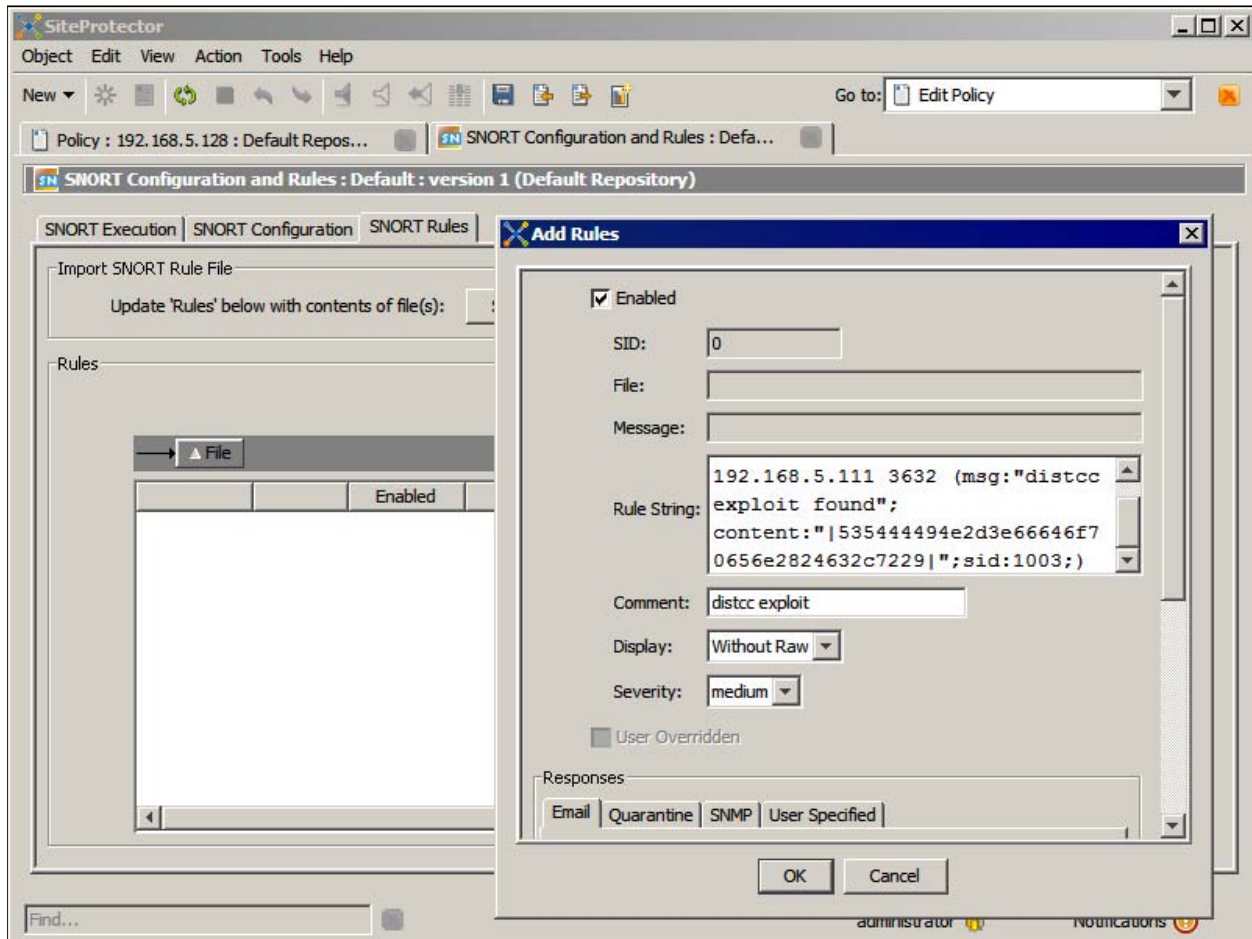
The screenshot shows the SiteProtector interface with the 'Add Rules' dialog box open. The dialog box contains the following fields and options:

- Enabled
- SID: 0
- File: (empty)
- Message: (empty)
- Rule String: `192.168.5.111 3632 (msg:"distcc exploit found"; content:"|535444494e2d3e66646f70656e2824632c7229|";sid:1003;)`
- Comment: (empty)
- Display: Without Raw
- Severity: medium
- User Overridden
- Responses: Email | Quarantine | SNMP | User Specified

A blue callout box on the left contains the text: "This rule alerts on TCP traffic from any source IP address and any source port destined for 192.168.5.111 to TCP 3632 in which the packet has the hexadecimal string listed in the rule." A yellow callout box points to the Rule String field with the text: "Type **distcc exploit**."

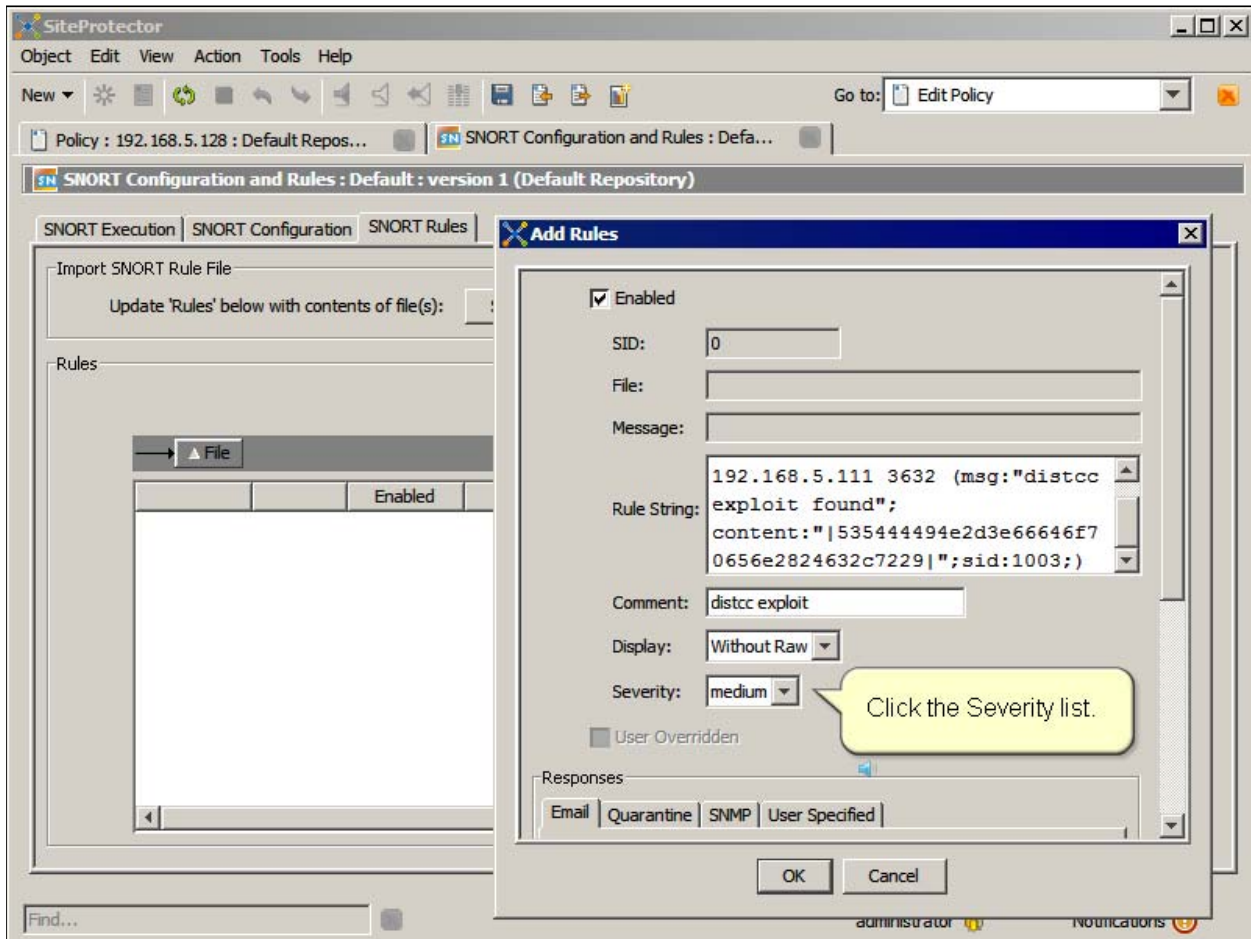
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 6



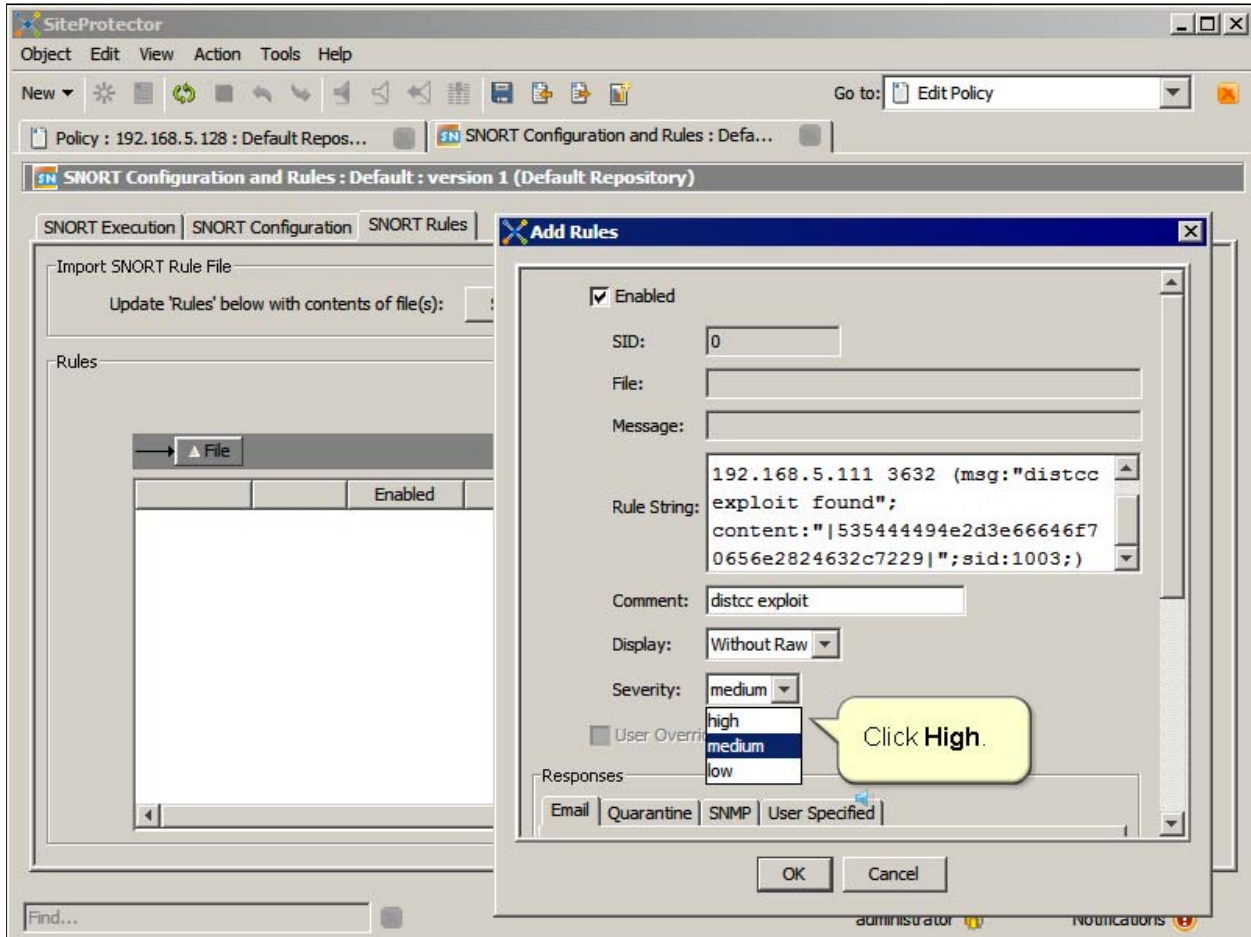
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 7



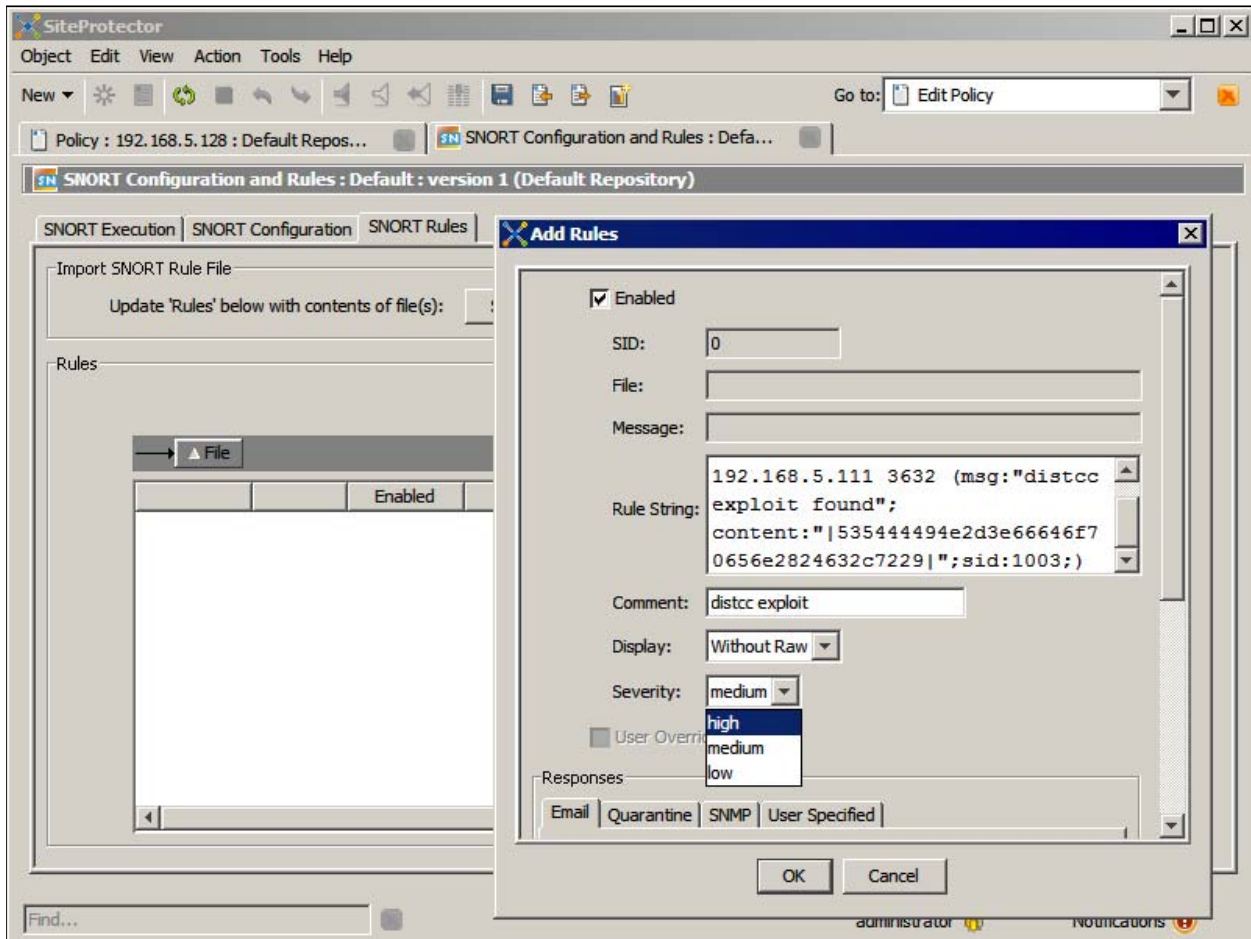
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 8



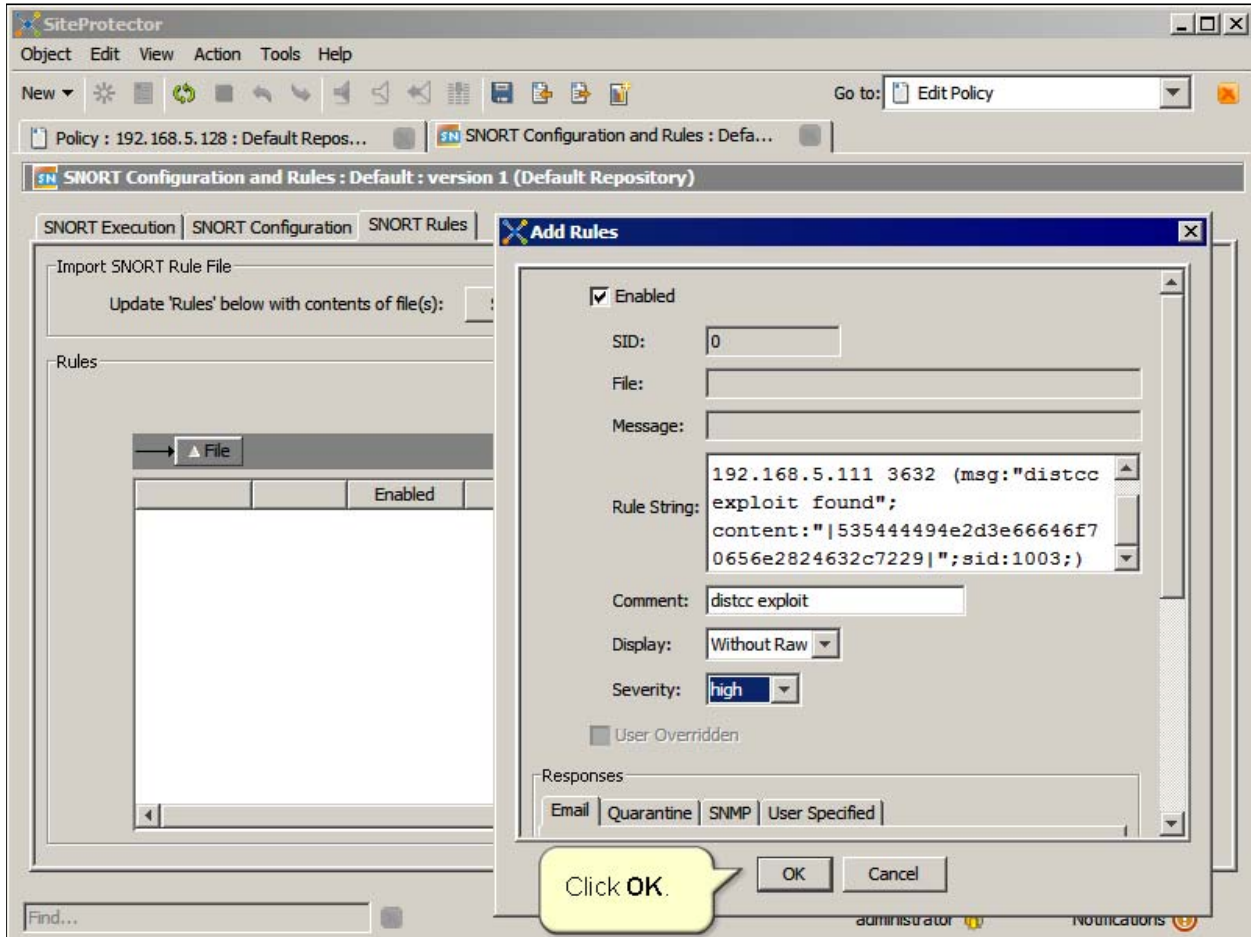
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 9



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 10



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 11

The screenshot shows the SiteProtector web interface for configuring SNORT rules. The main window is titled "SNORT Configuration and Rules : Default : version 1 (Default Repository)". It has three tabs: "SNORT Execution", "SNORT Configuration", and "SNORT Rules", with the last one being active. Below the tabs, there is an "Import SNORT Rule File" section with a text input field "Update 'Rules' below with contents of file(s):" and a button "Select *.rules file(s) to import...".

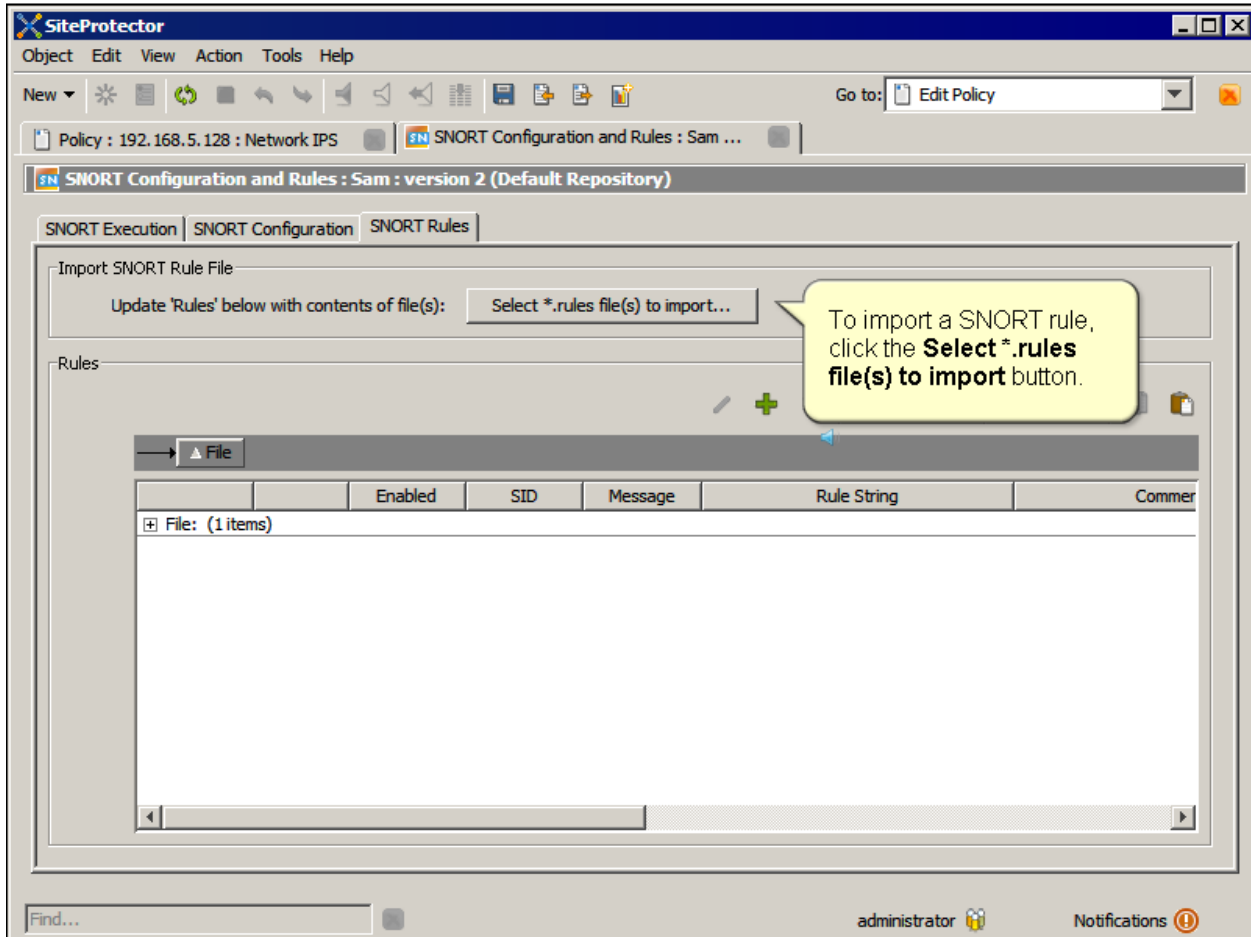
The "Rules" section contains a table with the following columns: "File", "Enabled", "SID", "Message", and "Rule String". A single rule is listed in the table:

File	Enabled	SID	Message	Rule String
File: (1 items)	<input checked="" type="checkbox"/>	0		alert tcp any any -> 192.168.5.111 36

A yellow callout box points to the rule entry with the text: "Verify that the rule is added to the Rules list." The interface also includes a "Find..." search bar at the bottom left, a user indicator "administrator" at the bottom right, and a "Notifications" icon.

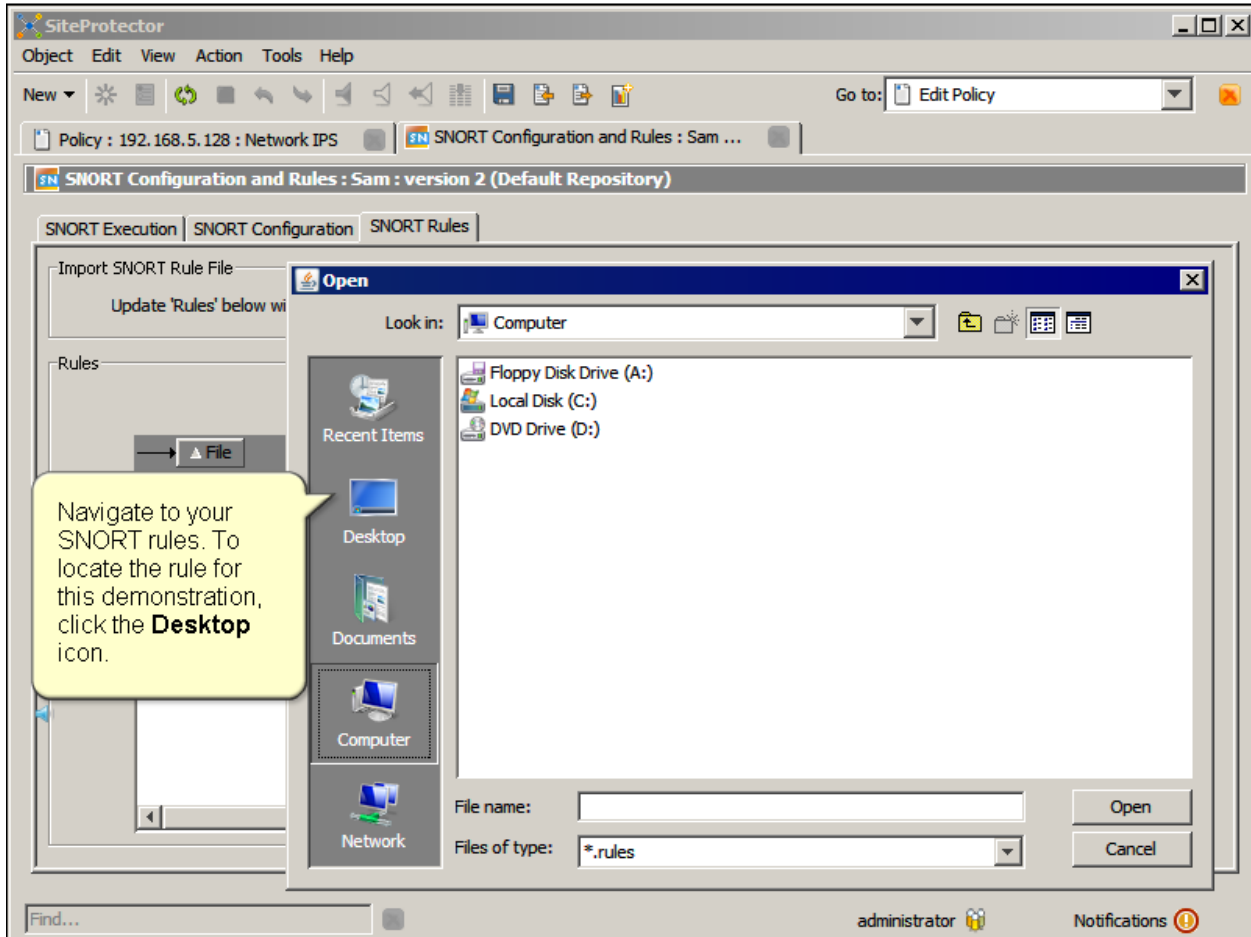
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 12



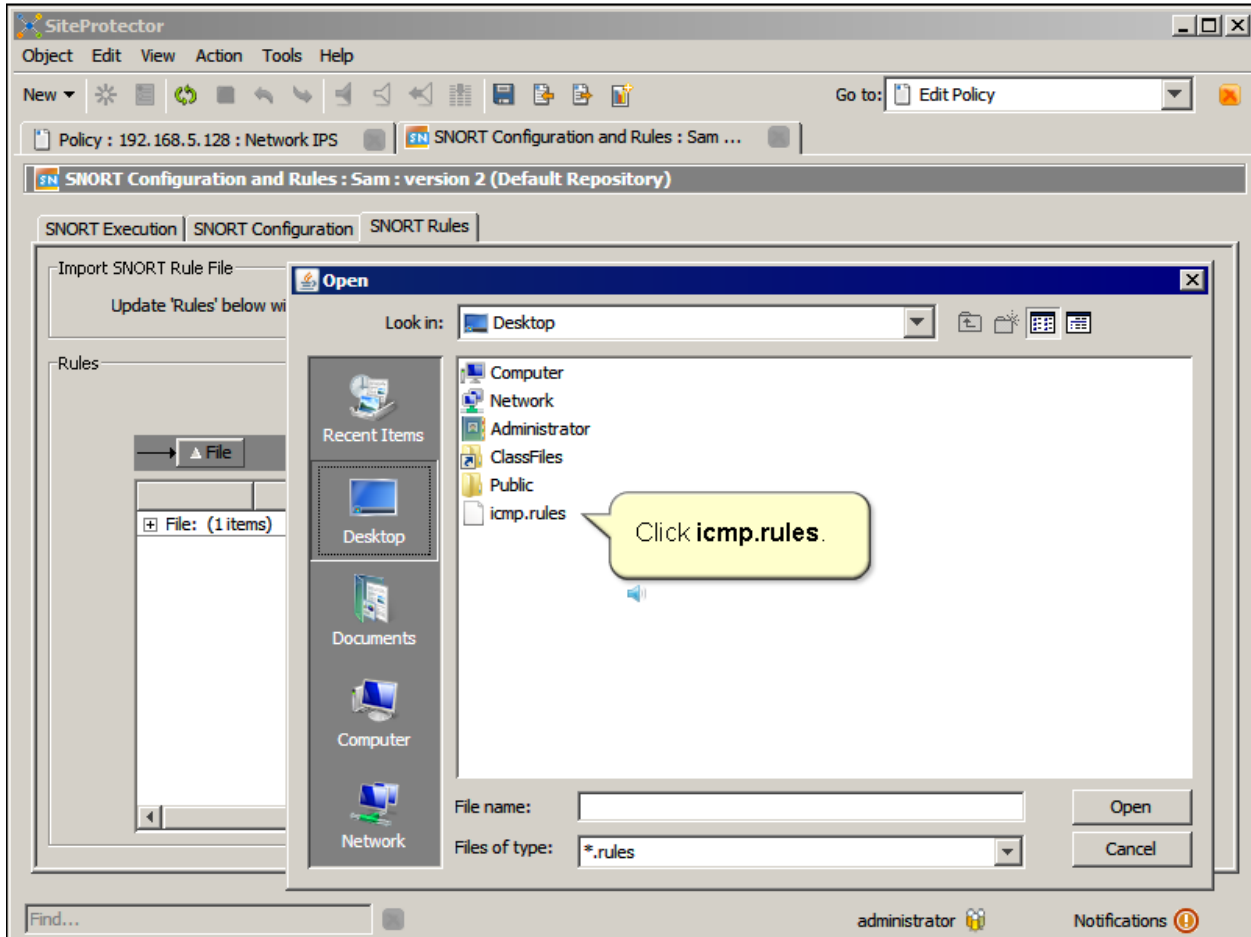
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 13



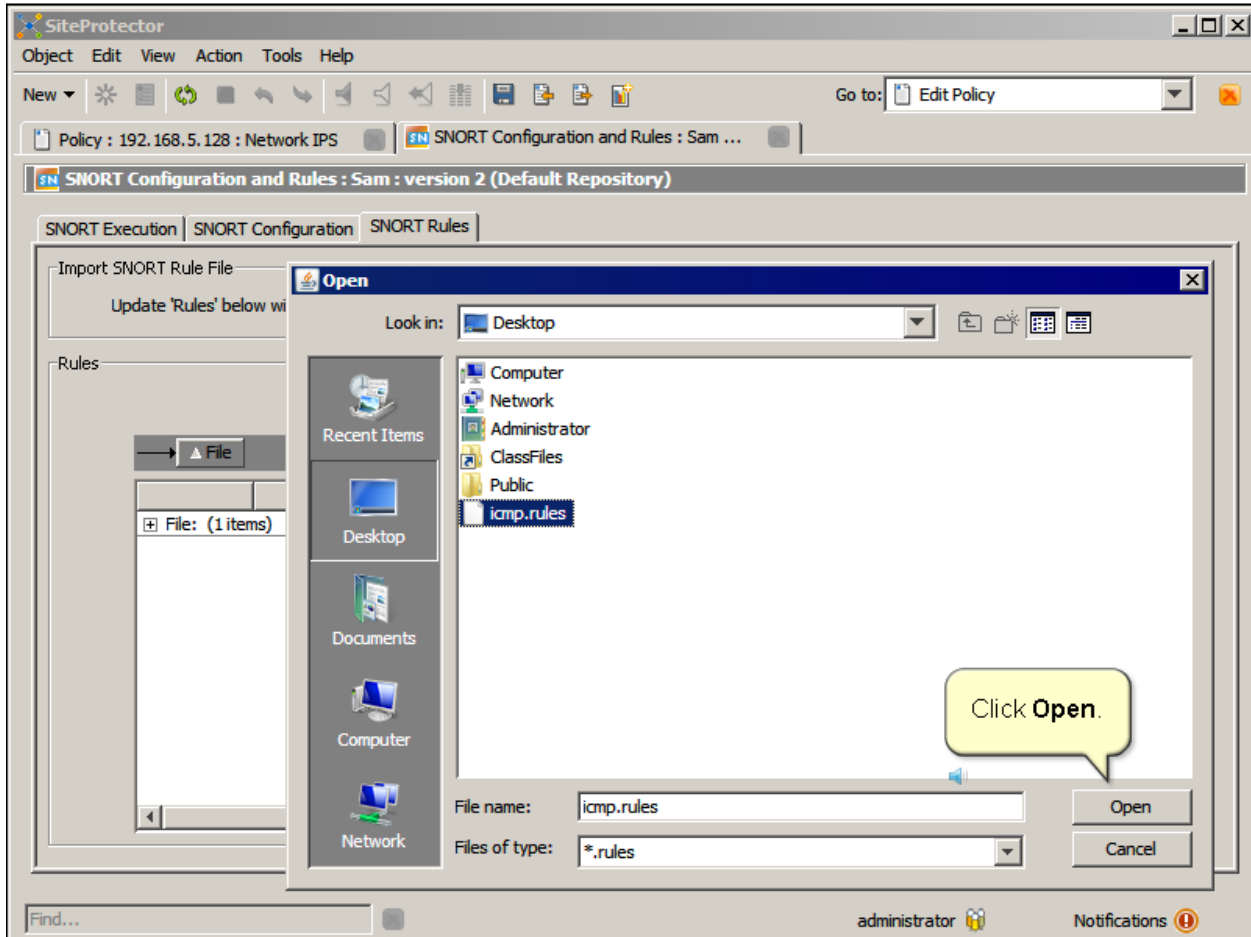
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 14



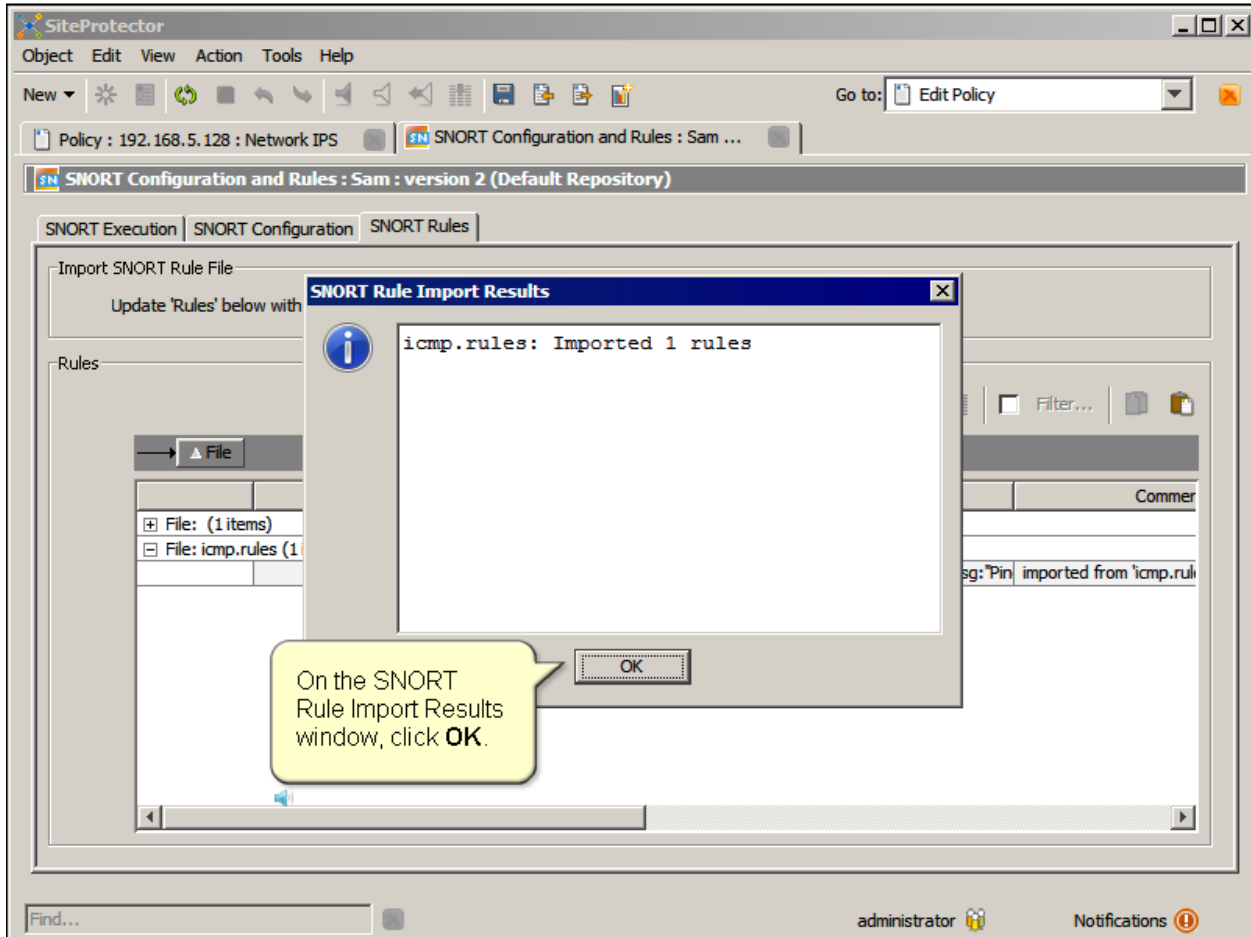
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 15



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 16



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 17

The screenshot shows the SiteProtector interface for SNORT Configuration and Rules. The 'SNORT Rules' tab is active, and the 'Import SNORT Rule File' section is visible. A button labeled 'Select *.rules file(s) to import...' is present. Below this, a table lists the imported rules. A yellow callout box points to the table with the text: 'Verify that the rule is added to the Rules list.'

File	Enabled	SID	Message	Rule String	Comment
File: icmp.rules (1 items)	<input checked="" type="checkbox"/>	2100001	Ping	alert icmp any any -> any any (msg:'Pin	imported from 'icmp.rul

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 18

SiteProtector

Object Edit View Action Tools Help

New * [Refresh] [Home] [Back] [Forward] [Print] [Export] [Import] [Help]

Go to: Edit Policy

Policy : 192.168.5.128 : Network IPS | SNORT Configuration and Rules : Sam ...

SNORT Configuration and Rules : Sam : version 2 (Default Repository)

SNORT Execution | SNORT Configuration | **SNORT Rules**

Import SNORT Rule File

Update 'Rules' below with contents of file(s):

Rules

File

	Enabled	SID	Message	Rule String	Commer
File: (1 items)					
File: icmp.rules (1 items)					
<input checked="" type="checkbox"/>		2100001	Ping	alert icmp any any -> any any (msg:'Pin	imported from 'icmp.rul

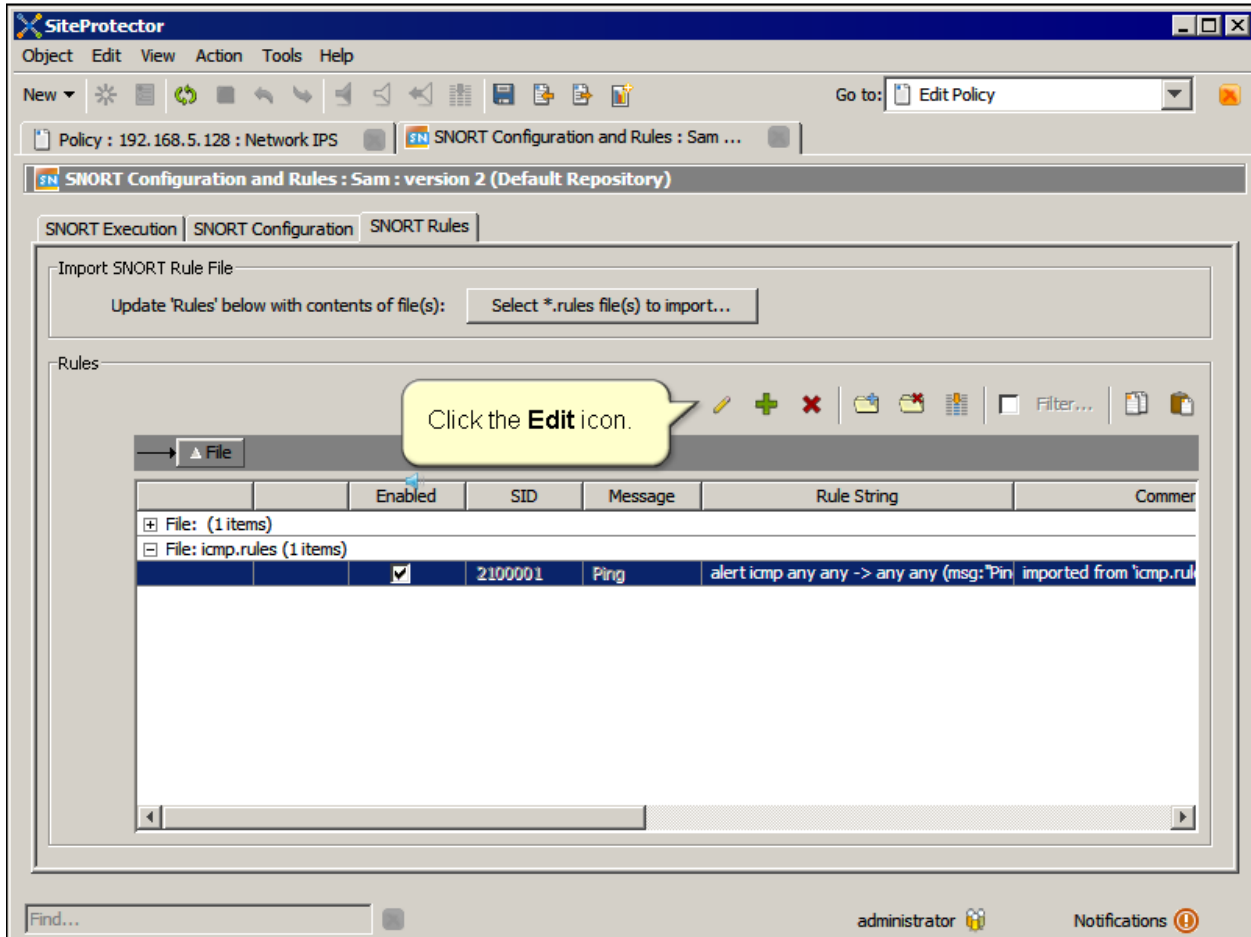
To examine the rule contents, select the rule.

Find...

administrator [User Icon] Notifications [Warning Icon]

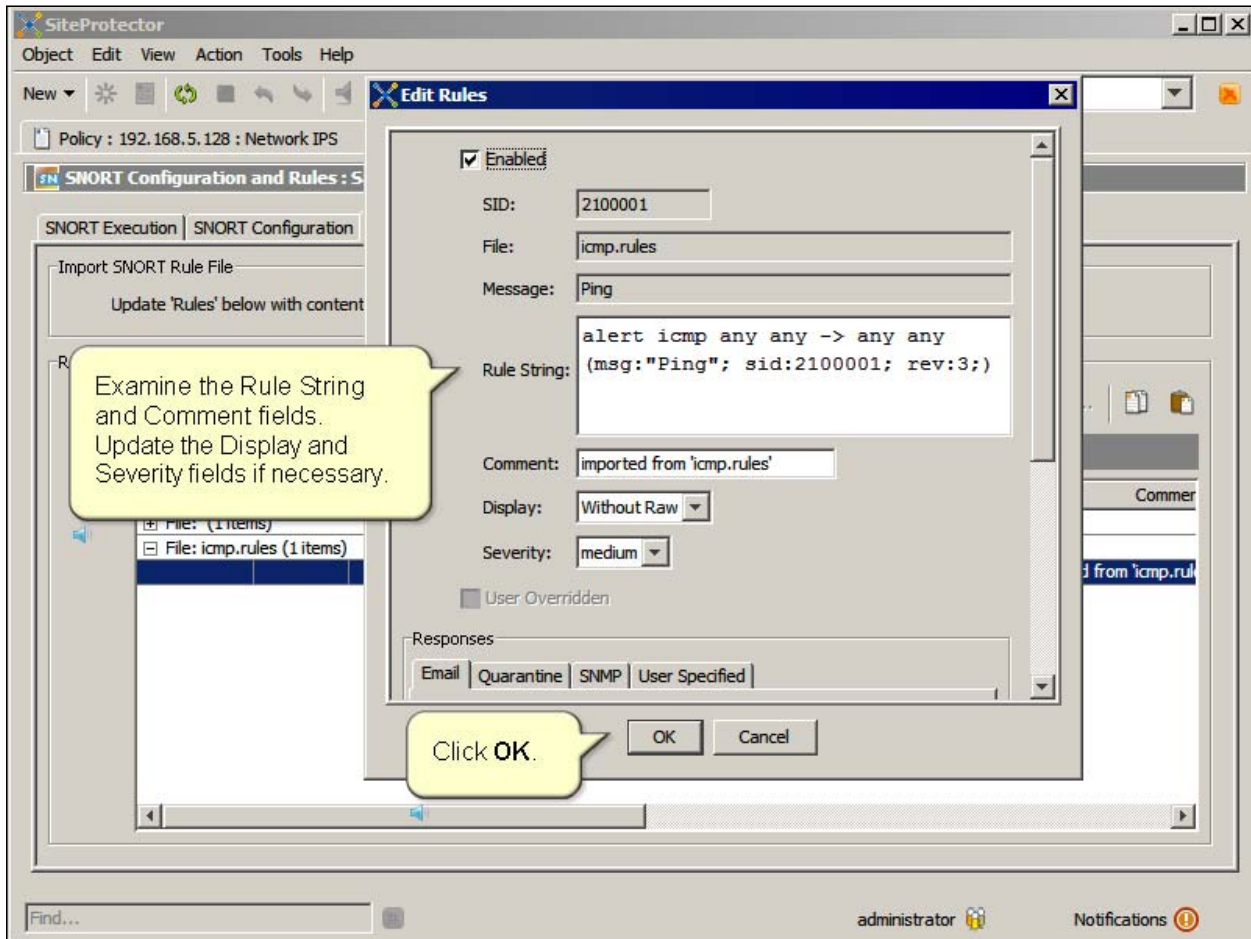
IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 19



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 20



IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 21

SiteProtector

Object Edit View Action Tools Help

Policy : 192.168.5.128 : Network IPS

SNORT Configuration and Rules : Sam : version 2 (Default)

SNORT Execution | SNORT Configuration | **SNORT Rules**

Import SNORT Rule File

Update 'Rules' below with contents of file(s):

Rules

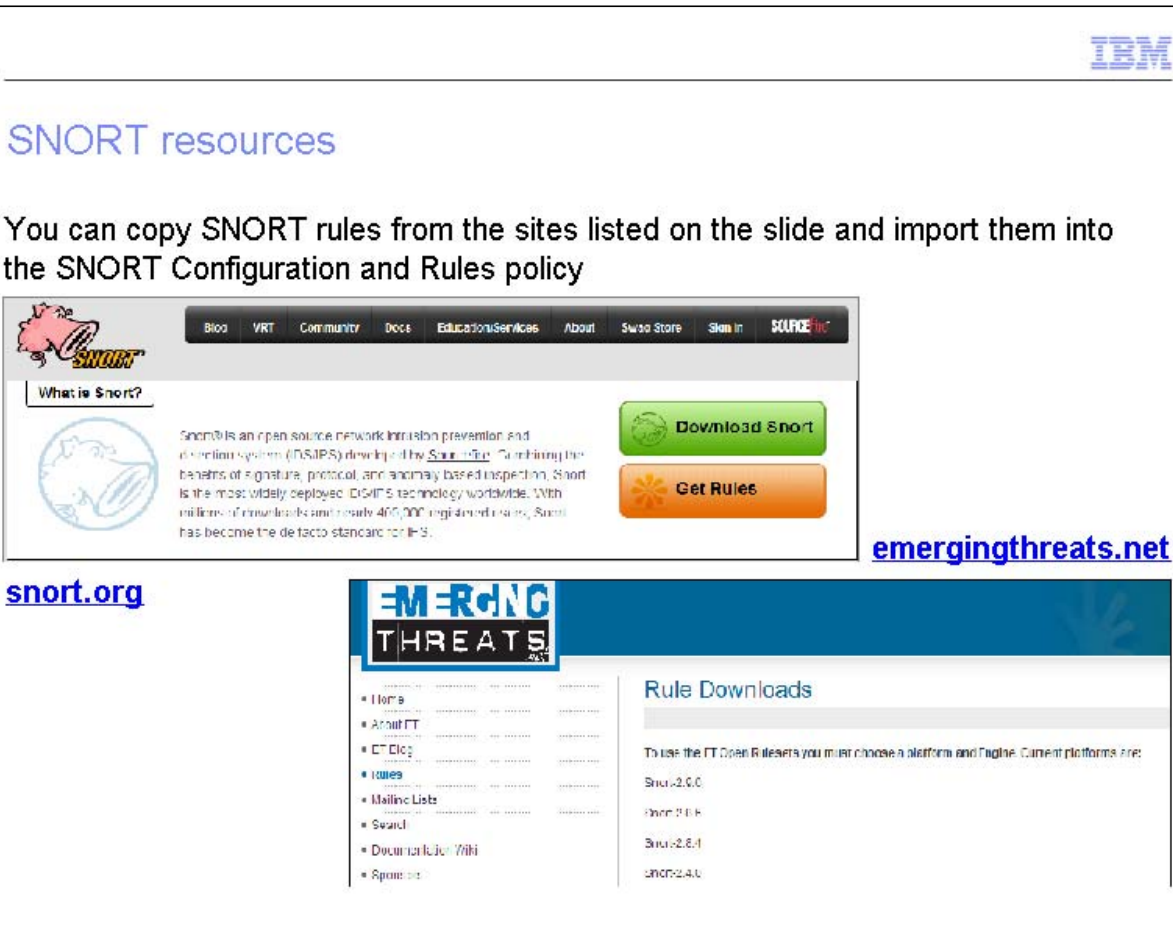
	Enabled	SID	Message	Rule String	Commer
File: (1 items)					
File: icmp.rules (1 items)					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2100001	Ping	alert icmp any any -> any any (msg:'Pin	imported from 'icmp.rul

IBM Customer Support does not support SNORT rules.

Find... administrator Notifications

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 22



The screenshot shows the SNORT website interface. At the top right is the IBM logo. Below it, the heading "SNORT resources" is displayed. A text block states: "You can copy SNORT rules from the sites listed on the slide and import them into the SNORT Configuration and Rules policy". The main content area features a navigation bar with links: Blog, VRT, Community, Docs, Education/Services, About, Swag Store, Sign in, and SOURCEfire. A "What is Snort?" section includes a globe icon, a description of Snort as an open-source network intrusion prevention and detection system, and two buttons: "Download Snort" and "Get Rules". The URL "emergingthreats.net" is shown to the right. Below this, the "snort.org" URL is listed. The "EMERGING THREATS" website is also shown, featuring a "Rule Downloads" section with a list of rule sets: Snort-2.0.0, Snort-2.8.8, Snort-2.8.1, and Snort-2.4.0.

You can copy SNORT rules from the sites listed on the slide and import them into the SNORT Configuration and Rules policy.

IBM Security NIPS V4.4, Adding and importing SNORT rules

Slide 23



Further reference

For more information use the following resources:

- [Configuring SNORT overview](#) IBM Education Assistant module
- [IBM Security Network Intrusion Prevention System firmware 4.4 announcement](#)



Summary

Now that you have completed the module, you are able to:

- Add a SNORT rule manually
- Import a SNORT rule

Now that you have completed the module, take a moment to review the module objectives.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2012. All rights reserved.