IBM Security Network Intrusion Prevention System V4.4

Configuring SNORT overview

© 2012 IBM Corporation

IBM Security Network Intrusion Prevention System V4.4, Configuring SNORT overview

Objectives

When you complete this module, you can perform these tasks:

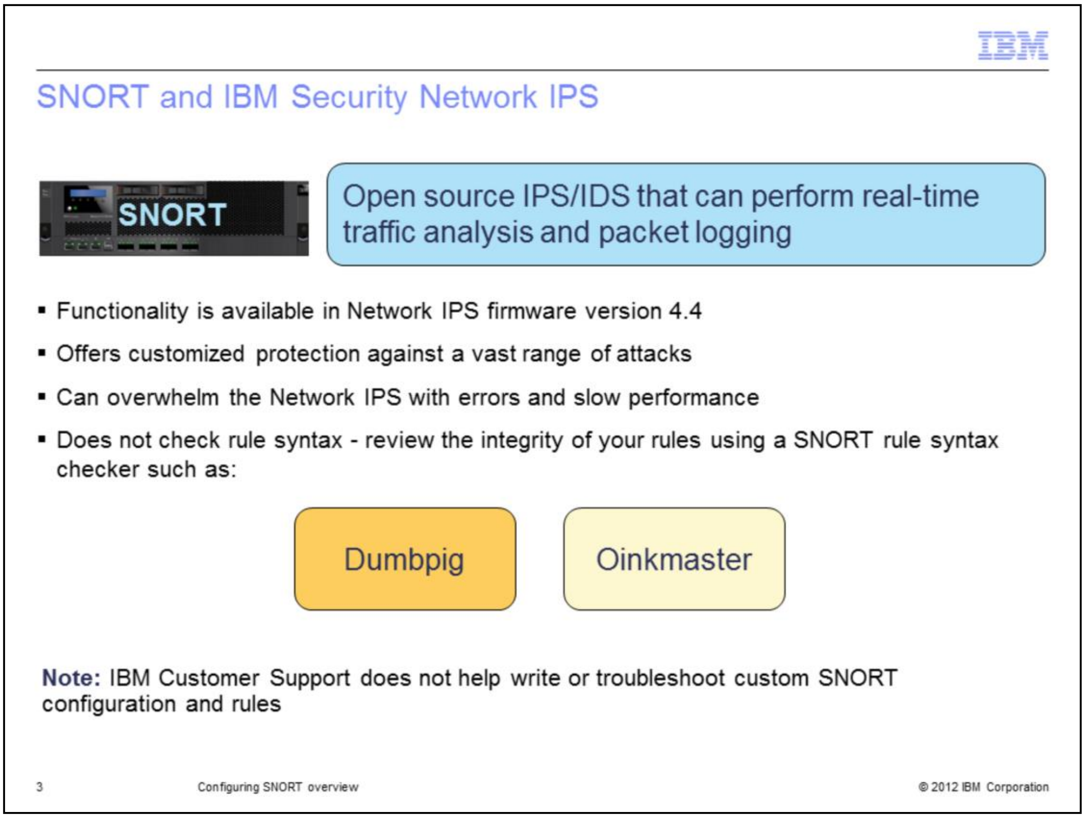
- Enable SNORT functionality on the Network IPS
- Configure how SNORT is applied to an appliance
- Create SNORT rules

When you complete this module, you can perform these tasks:

- Enable SNORT functionality on the Network IPS

- Configure how SNORT is applied to an appliance

- Create SNORT rules



IBM

SNORT and IBM Security Network IPS

SNORT

Open source IPS/IDS that can perform real-time traffic analysis and packet logging

- Functionality is available in Network IPS firmware version 4.4
- Offers customized protection against a vast range of attacks
- Can overwhelm the Network IPS with errors and slow performance
- Does not check rule syntax - review the integrity of your rules using a SNORT rule syntax checker such as:

Dumbpig

Oinkmaster

Note: IBM Customer Support does not help write or troubleshoot custom SNORT configuration and rules

3 Configuring SNORT overview © 2012 IBM Corporation

SNORT is an open source intrusion prevention and detection system that can perform real-time traffic analysis and packet-logging on networks. With firmware version 4.4, some SNORT capability is integrated into the IBM Security Network IPS.

SNORT offers customized protection against a vast range of attacks, but if it is not used correctly, SNORT can overwhelm the Network IPS with errors and slow performance.

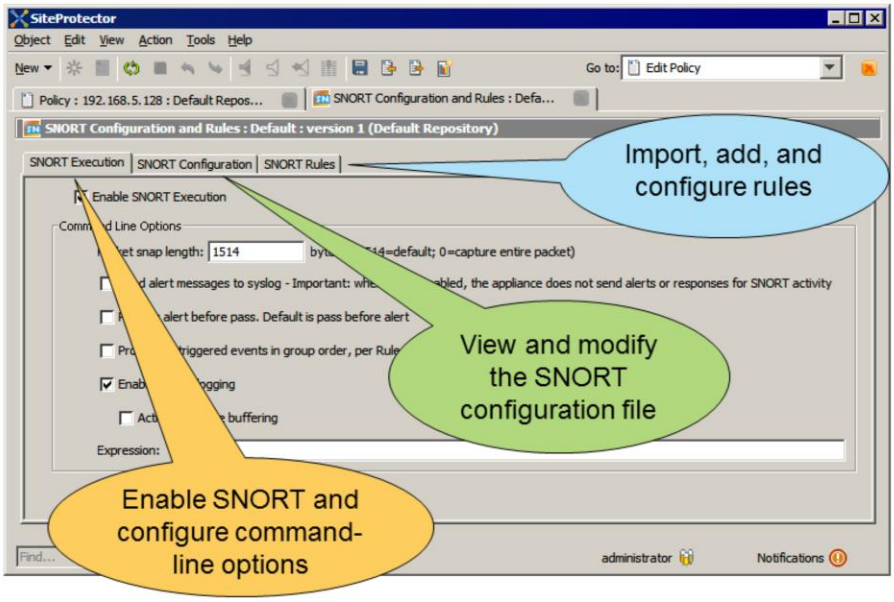
Because SNORT does not check rule syntax, it is important to review the integrity of your rules using a SNORT rule syntax checker such as.

* Dumbpig - http://leonward.wordpress.com/dumbpig/

* Oinkmaster - http://oinkmaster.sourceforge.net/

Note: IBM Customer Support does not help write or troubleshoot custom SNORT configuration and rules.

SNORT Configuration and Rules policy


SiteProtector
Object Edit View Action Tools Help
New
Go to: Edit Policy
Policy : 192.168.5.128 : Default Repos...
SNORT Configuration and Rules : Defa...
SNORT Configuration and Rules : Default : version 1 (Default Repository)
SNORT Execution
SNORT Configuration
SNORT Rules
Find...
administrator
Notifications

☑ Enable SNORT Execution

Comm d Line Options

ket snap length: 1514 by 14=default; 0=capture entire packet)

□ d alert messages to syslog - Important: whe abled, the appliance does not send alerts or responses for SNORT activity

□ F alert before pass. Default is pass before alert

□ Pro triggered events in group order, per Rule

☑ Enab ogging

□ Acti buffering

Expression:

Import, add, and configure rules

View and modify the SNORT configuration file

Enable SNORT and configure command-line options

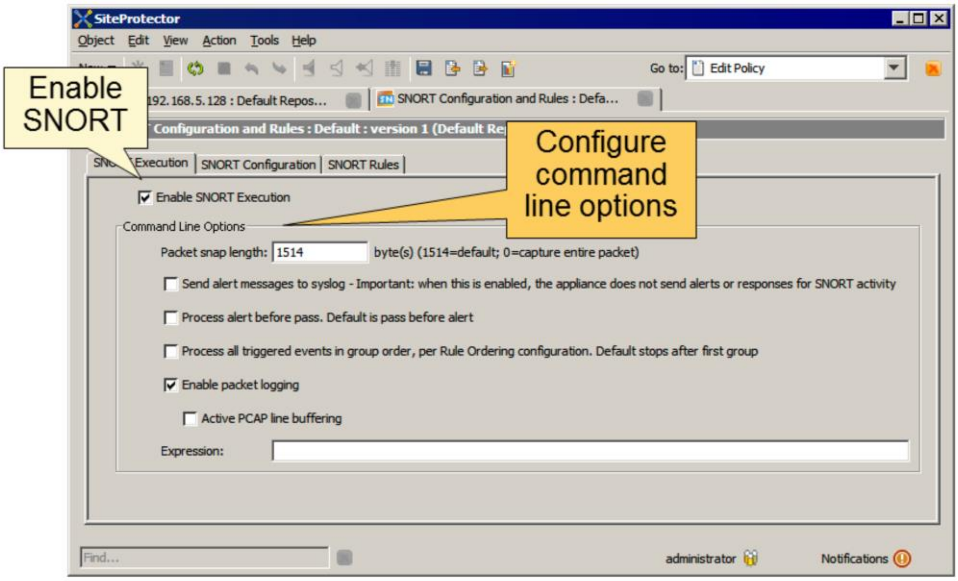
There are three tabs in the SNORT Configuration and Rules policy. You use the:

* SNORT Execution tab to enable the SNORT engine and configure SNORT command-line options.

* SNORT Configuration tab to view the default SNORT configuration file and modify the configuration.

* SNORT Rules tab to import SNORT rules file, add SNORT rules, and configure the rules.

SNORT Execution tab


SiteProtector
Object Edit View Action Tools Help
Go to: Edit Policy
192.168.5.128 : Default Repos...
SNORT Configuration and Rules : Defa...
Configuration and Rules : Default : version 1 (Default Re
SNORT Execution
SNORT Configuration
SNORT Rules
Find...
administrator
Notifications

Enable SNORT

Configure command line options

☑ Enable SNORT Execution

Command Line Options

Packet snap length: 1514 byte(s) (1514=default; 0=capture entire packet)

☐ Send alert messages to syslog - Important: when this is enabled, the appliance does not send alerts or responses for SNORT activity

☐ Process alert before pass. Default is pass before alert

☐ Process all triggered events in group order, per Rule Ordering configuration. Default stops after first group

☑ Enable packet logging

☐ Active PCAP line buffering

Expression:

5 Configuring SNORT overview © 2012 IBM Corporation

Notes:

* By default, SNORT functionality is disabled.

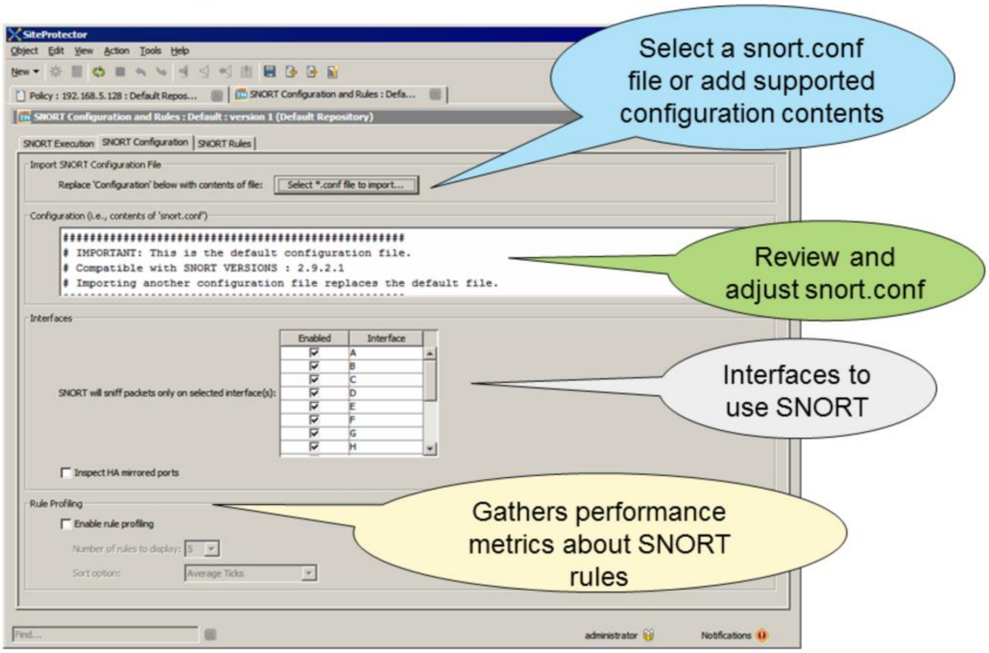
* If you enable the **Send alert messages to syslog** option, the SNORT system does not send events to the Analysis view or send email, SNMP, quarantine, or user specified responses for SNORT activity, even if they are enabled on the SNORT Rules tab.

* The **Process alert before pass** option processes alert rules before it applies pass rules. This option can decrease false negatives, but can hinder performance and increase false positives.

* The **Activate PCAP line buffering** option improves performance, but you cannot view SNORT packets immediately in the SNORT packet capture file.

* The **Expression** field tells the SNORT engine to filter traffic that is true to the expression. If there is no expression, all traffic is processed.

SNORT Configuration tab


SiteProtector
Object Edit View Action Tools Help
New
Policy : 192.168.5.128 : Default Repos...
SNORT Configuration and Rules : Defa...
SNORT Configuration and Rules : Default : version 1 (Default Repository)
SNORT Execution
SNORT Configuration
SNORT Rules
Find...
administrator
Notifications

Import SNORT Configuration File

Replace 'Configuration' below with contents of file: Select *.conf file to import...

Configuration (i.e., contents of 'snort.conf')

```
##################################################
# IMPORTANT: This is the default configuration file.
# Compatible with SNORT VERSIONS : 2.9.2.1
# Importing another configuration file replaces the default file.
```

Interfaces

SNORT will sniff packets only on selected interface(s):

Enabled	Interface
☑	A
☑	B
☑	C
☑	D
☑	E
☑	F
☑	G
☑	H

□ Inspect HA mirrored ports

Rule Profiling

□ Enable rule profiling

Number of rules to display: 5

Sort option: Average Ticks

Select a snort.conf file or add supported configuration contents

Review and adjust snort.conf

Interfaces to use SNORT

Gathers performance metrics about SNORT rules

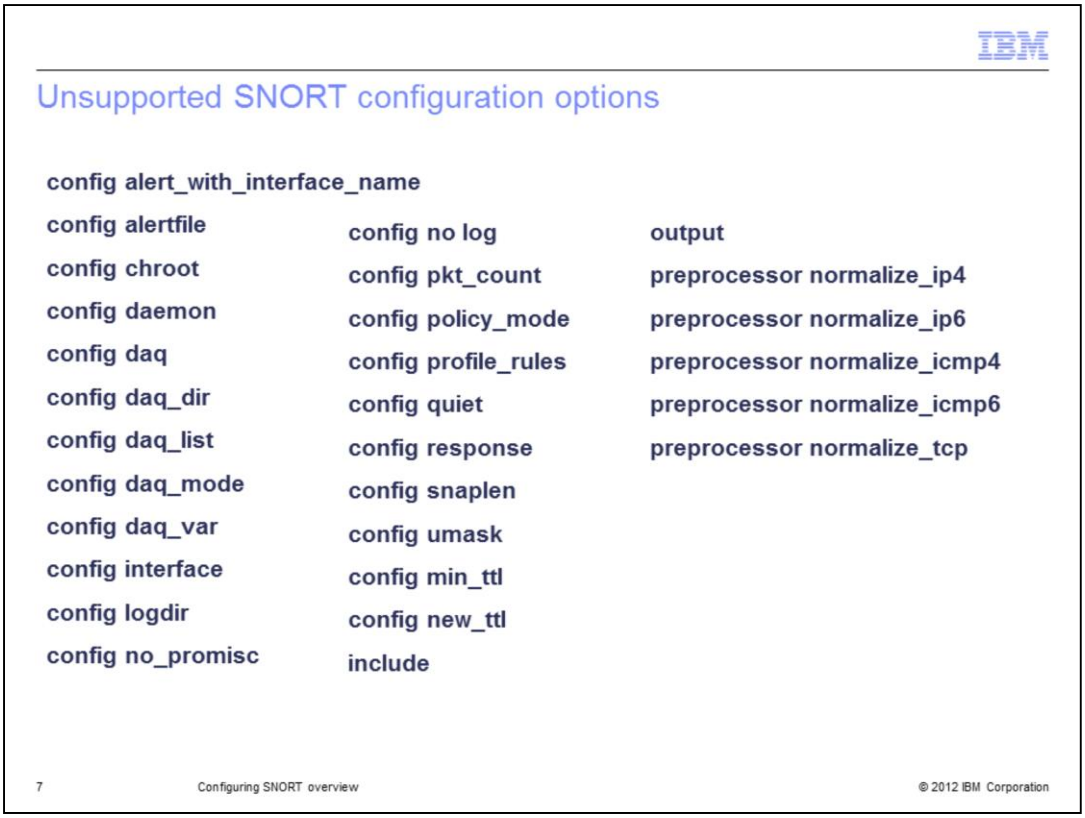
On the SNORT Configuration tab, you can configure the snort.conf file, apply the file to specific appliance interfaces, and enable rule profiling.

The SNORT Configuration and Rules policy includes a default configuration file. You can modify the default configuration file so that it works in your network environment. You can also use the **Select *.conf file to import** button to import another configuration file or add supported configuration content. If the system detects an error in the policy, the apply policy job fails.

In the Interfaces area, you can apply the configuration file to the appropriate appliance interfaces. To enable SNORT on appliances in a high availability pair to analyze packets on mirrored ports, select the **Inspect HA mirrored ports** check box. Enabling this option increases the possibility of duplicate global responses and SiteProtector alerts but decreases the chance that SNORT misses an attack. Disabling this option (the default) minimizes the possibility of duplicate global responses and SiteProtector alerts, but limits the ability of SNORT to analyze all traffic.

Rule profiling analyzes the performance of SNORT rules and can be used to troubleshoot performance issues.

Note: Rule profiling can impact the SNORT engine’s performance.



Unsupported SNORT configuration options

config alert_with_interface_name

config alertfile

config chroot

config daemon

config daq

config daq_dir

config daq_list

config daq_mode

config daq_var

config interface

config logdir

config no_promisc

config no log

config pkt_count

config policy_mode

config profile_rules

config quiet

config response

config snaplen

config umask

config min_ttl

config new_ttl

include

output

preprocessor normalize_ip4

preprocessor normalize_ip6

preprocessor normalize_icmp4

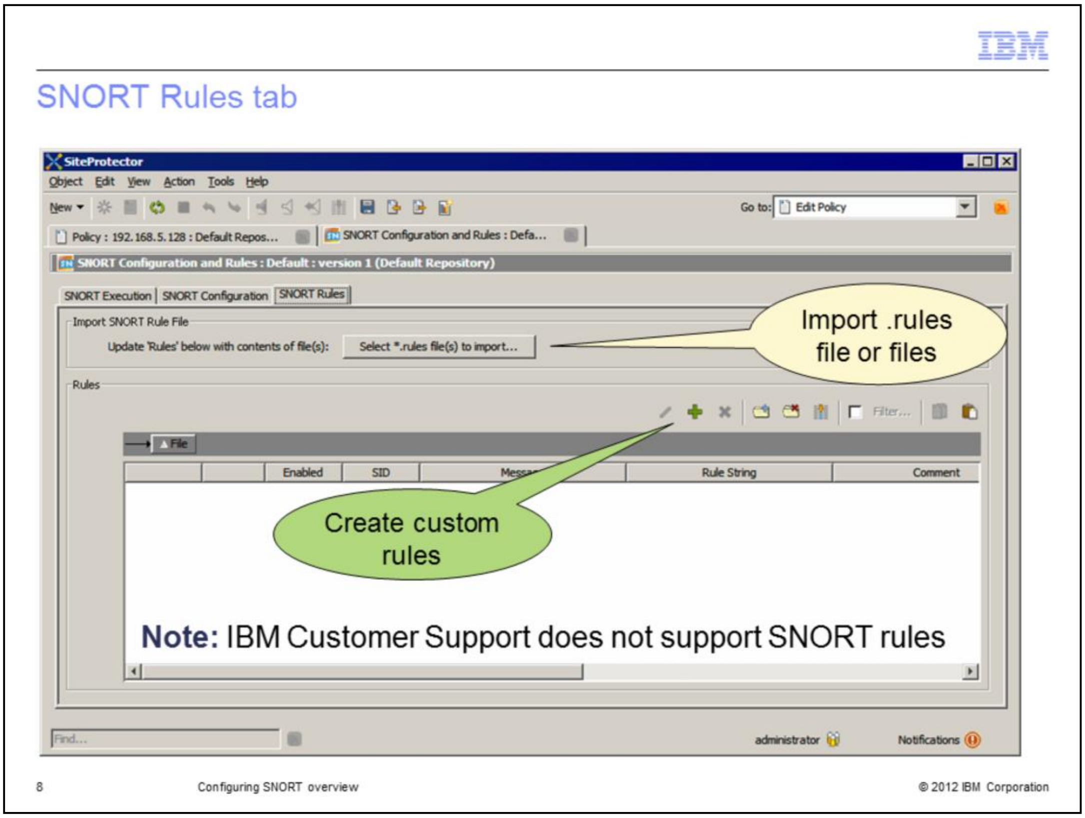
preprocessor normalize_icmp6

preprocessor normalize_tcp

7 Configuring SNORT overview © 2012 IBM Corporation

IBM Security Network IPS does not support the SNORT configuration options listed on the slide.

SNORT Rules tab


SiteProtector
Object Edit View Action Tools Help
New
Go to: Edit Policy
Policy : 192.168.5.128 : Default Repos...
SNORT Configuration and Rules : Defa...
SNORT Configuration and Rules : Default : version 1 (Default Repository)
SNORT Execution
SNORT Configuration
SNORT Rules
Import SNORT Rule File
Update 'Rules' below with contents of file(s):
Select *.rules file(s) to import...
Rules
Filter...
File
Enabled
SID
Message
Rule String
Comment
Find...
administrator
Notifications

Import .rules file or files

Create custom rules

Note: IBM Customer Support does not support SNORT rules

8 Configuring SNORT overview © 2012 IBM Corporation

Because IBM Security Systems does not provide SNORT content, there are no SNORT rules available in the Rules list. You can import multiple .rules files. When importing SNORT rules, consider the following guidelines:

* Import no more than 9000 rules from a .rules file.

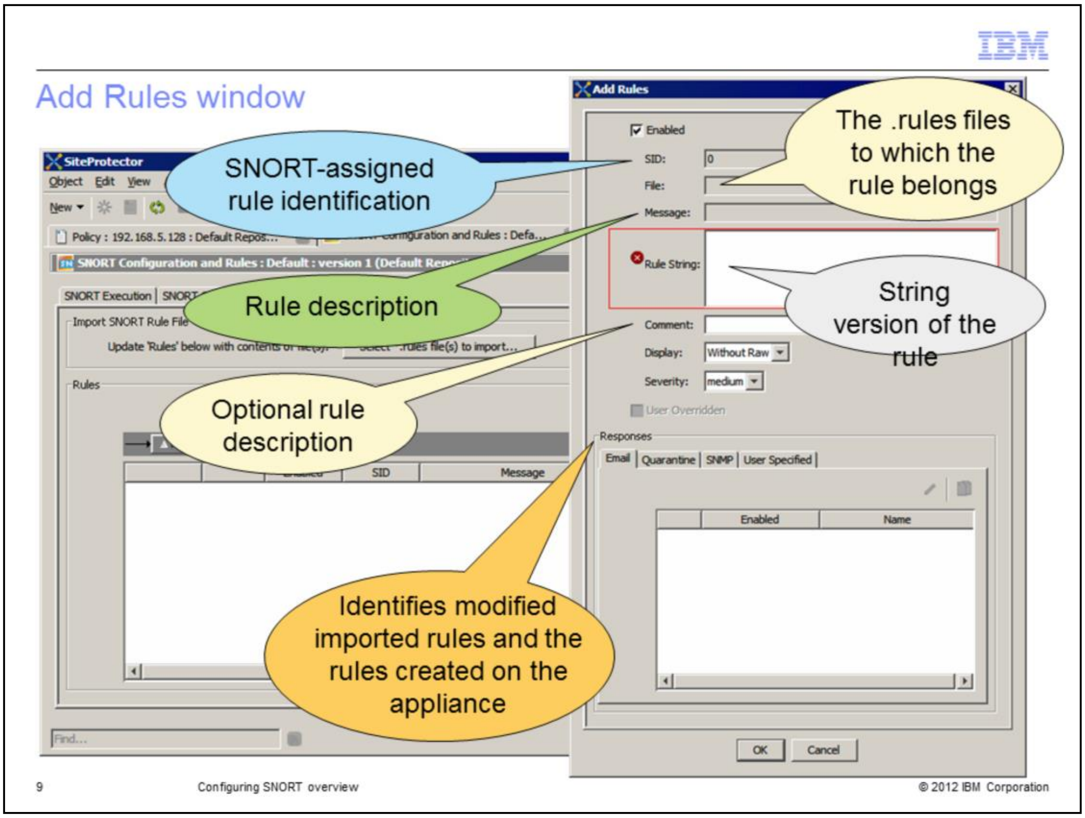
* Import .rules files that are no bigger than 5 MB.

* Check the syntax of your rules with a SNORT rule syntax checker before importing them. The Network IPS does not check rule syntax.

* Dynamic rules for SNORT are not supported.

* The block response is not supported.

You can import .rules files or click the **Add** icon to configure a rule.



Add Rules window

SNORT-assigned rule identification

The .rules files to which the rule belongs

Rule description

String version of the rule

Optional rule description

Identifies modified imported rules and the rules created on the appliance

☑ Enabled

SID: 0

Display: Without Raw

Severity: medium

9 Configuring SNORT overview © 2012 IBM Corporation

When you create a rule using the Add icon, you:

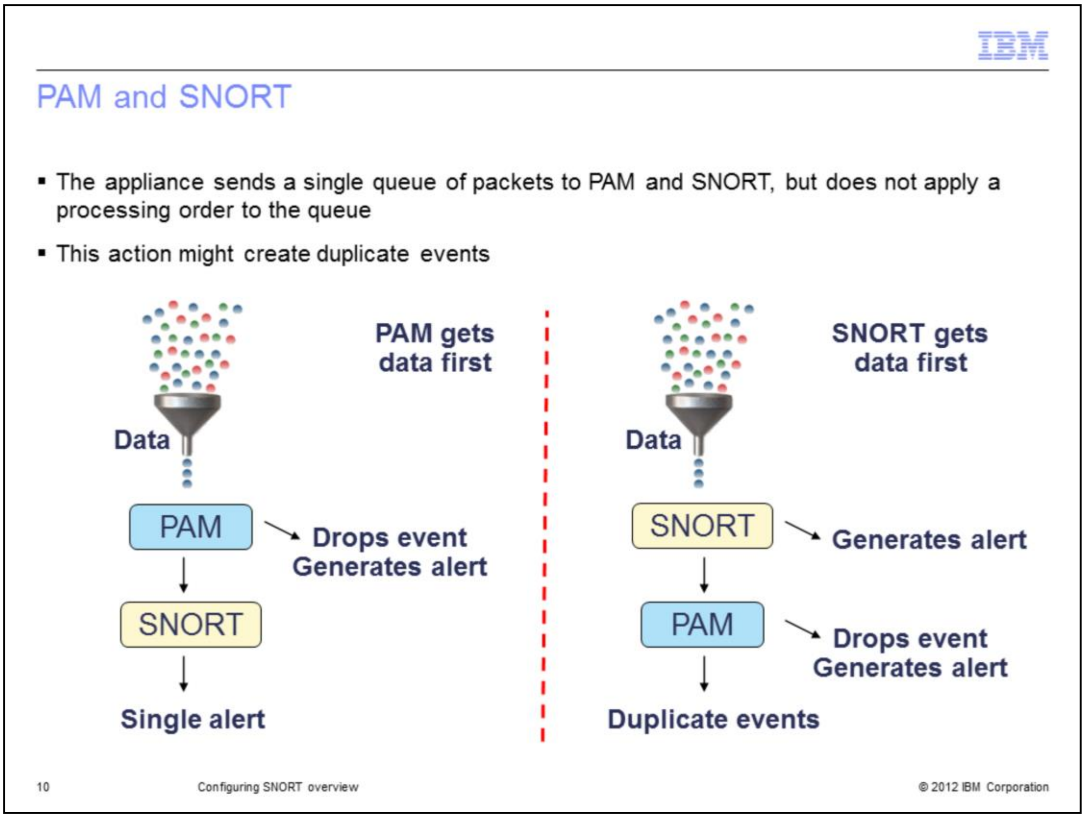
* Add the rule string

* An optional comment that describes the rule

* Select the appropriate severity level and

* Select any appropriate predefined responses

When you save the rule, the appliance assigns the SID and groups the rule in a .rules file. If there is an error in the rule, the appliance does not save it.



PAM and SNORT

- The appliance sends a single queue of packets to PAM and SNORT, but does not apply a processing order to the queue
- This action might create duplicate events

PAM gets data first

Data

PAM → Drops event Generates alert

SNORT

Single alert

SNORT gets data first

Data

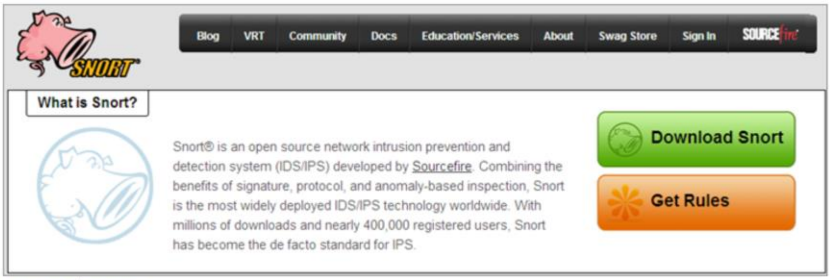
SNORT → Generates alert

PAM → Drops event Generates alert

Duplicate events

The appliance sends a single queue of packets to PAM and SNORT, but does not apply a processing order to the queue. This action might create duplicate events. For example, if PAM gets the data first, it might drop the event and generate an alert. Because PAM dropped the event, SNORT does not process it. If SNORT gets the data first, it generates an alert. PAM then processes the same data, drops the event, and generates an alert. In the second scenario, you might have duplicate events because both SNORT and PAM generated alerts on the same packet.

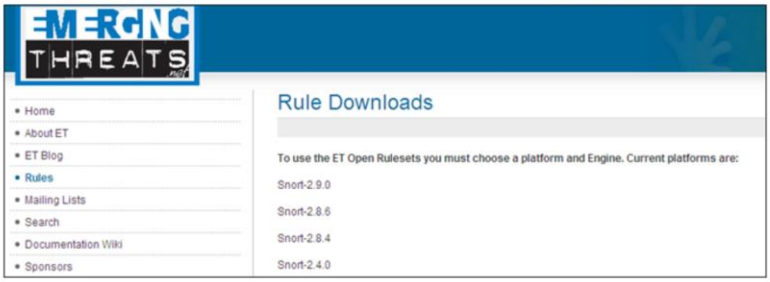
SNORT resources



Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

snort.org

emergingthreats.net



Rule Downloads

To use the ET Open Rulesets you must choose a platform and Engine. Current platforms are:

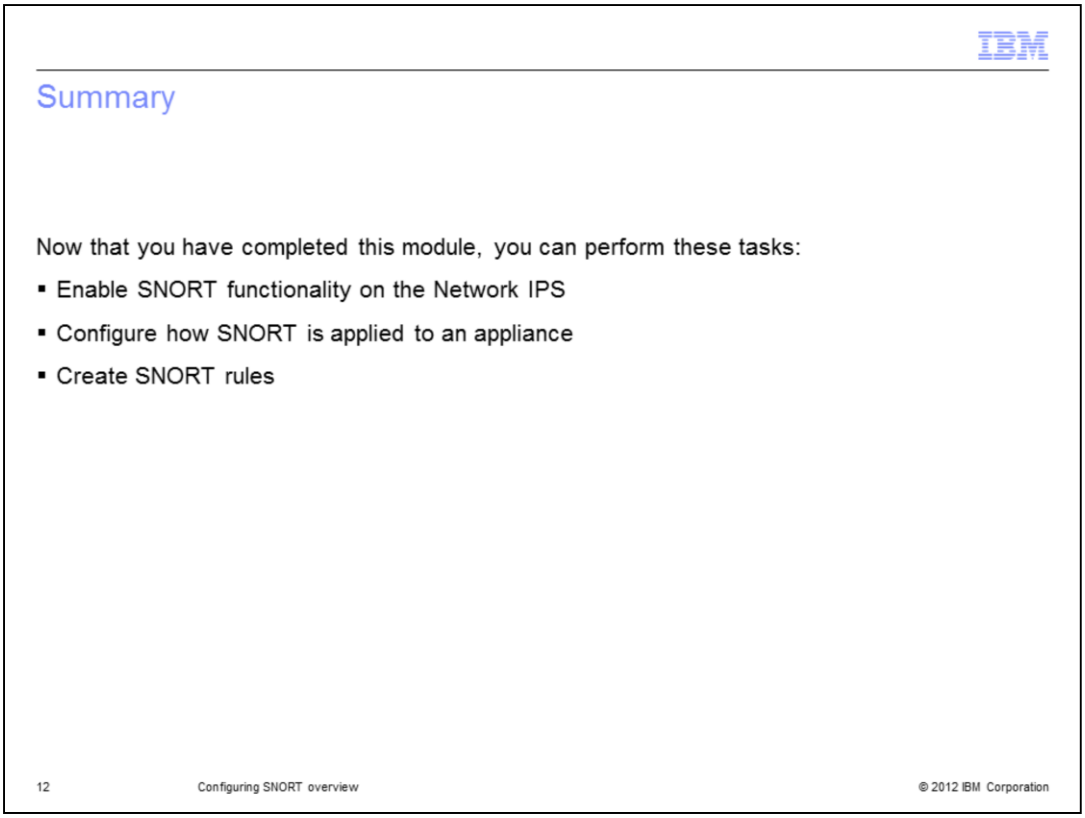
Snort-2.9.0

Snort-2.8.6

Snort-2.8.4

Snort-2.4.0

SNORT rules are available from the sites listed on the slide.

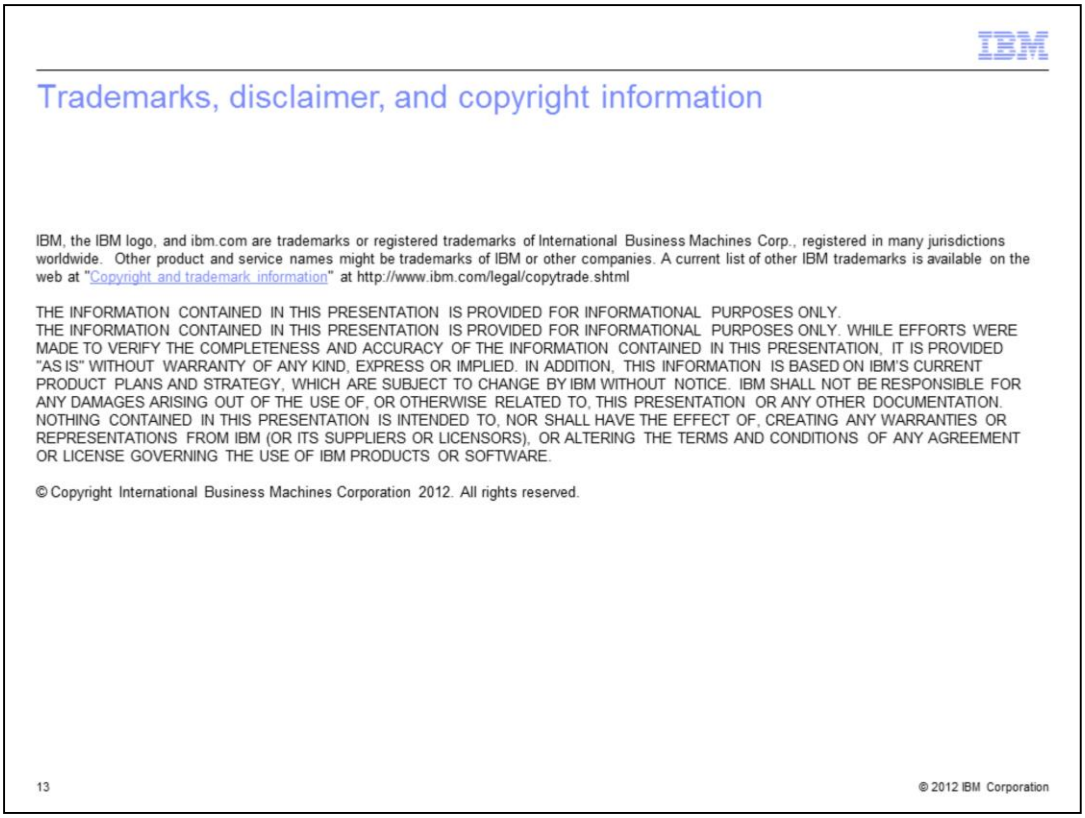


Summary

Now that you have completed this module, you can perform these tasks:

- Enable SNORT functionality on the Network IPS
- Configure how SNORT is applied to an appliance
- Create SNORT rules

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



Trademarks, disclaimer, and copyright information

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" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
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.