

GSM: IDS Optimization

Content

- [Preparing the Sourcefire Defense Center](#)
- [Preparing the Greenbone Security Manager](#)
- [Sending results to the Sourcefire Defense Center](#)
- [Viewing results in the Sourcefire Defense Center](#)

Introduction

Network based Intrusion Detection Systems (NIDS) are used to identify attacks on the network and to alert administrators in the case of an attack. They do this by capturing the network traffic and analyzing it for suspicious activities. This includes identifying even complex attack patterns.

Usually the IDS functionality is coupled with an Intrusion Prevention System (IPS) which reacts immediately to a threat by deleting data packets, closing connection or altering the transmitted data in a way that the threat is eliminated.

The NIDS/IPS can only provide optimal performance if the entirety of the network traffic is routed through it, enabling it to identify all potential threats. But this causes it to become the bottleneck of the network infrastructure, meaning that every improvement to the NIDS performance will benefit the throughput of the entire network.

This is where the Greenbone Security Manager comes into play: Contrary to the passive approach of waiting for attacks which the NIDS/IPS employs, the GSM collects information about weak and possibly vulnerable systems in the IT infrastructure. This information helps the NIDS/IPS to optimize its performance, for example by prioritizing vulnerable systems.

- **GSM-NIDS/IPS coupling method 1: Manual data transfer from GSM to NIDS/IPS**

Every report of a vulnerability scan can be sent to the NIDS/IPS. This can be done by exporting and importing the report (in case of an unknown or unreachable NIDS/IPS) or with the simple push of a button (if the GSM and the NIDS/IPS have been matched before).

The user can send entire reports or custom filtered reports.

- **GSM-NIDS/IPS coupling method 2: Automatic data transfer from GSM to NIDS/IPS**

If the GSM and the NIDS/IPS have been configured to interact with one another, data transfer from the GSM to the NIDS/IPS becomes as easy as every other escalation routine in the GSM. Scan results can be transmitted automatically to the NIDS/IPS once the scan is finished. Coupled with scheduled tasks this can be used to create a fully automatized system for alerts and optimization.

- **GSM-NIDS/IPS coupling method 3: Active control of the GSM by the NIDS/IPS**

If the NIDS/IPS discovers suspicious activities directed around systems which have been classified as

being especially at-risk, it can use the GSM to perform a vulnerability assessment of these systems. Once the GSM has finished its analysis, it reports the results back to the NIDS/IPS. In the mean time, both systems continue to operate fully independent, without any blocking of the other.

Once GSM and NIDS/IPS have been set up to communicate with one another, no further human interaction with the GSM is necessary. The operation of the GSM is entirely controlled by the NIDS/IPS.

The following NIDS/IPS are currently supported by Greenbone:

- Sourcefire Defense Center (GSM 1.5 or higher)

You will find a step-by-step guide for this product on this page.

Preparing the Sourcefire Defense Center

To enable your Sourcefire Defense Center to receive results from a Greenbone Security Manager (GSM), you first need to add the GSM to the Defense Center as a so called Host Input Client and create a certificate for it.

To do so, use the configuration menu of the Host Input Clients which can be accessed via "Operations" and "Configuration". Click the "Create Client" button on this page. Enter the IP or host name of your GSM. It is not necessary to enter a password.





























Once the Host Input Client has been created you can download the certificate by clicking on the link labeled "Certificate Location". Save this certificate locally.



Preparing the Greenbone Security Manager

On the GSM you will need the report format plugin "Sourcefire Host Input Import". If you have not installed it already, you can find on the [Report Format Downloads page](#). You can install the plugin by accessing the "Report Formats" menu on your GSM, selecting the plugin you downloaded in the "Import Report Format Plugin" entry and clicking on "Import Report Format". The plugin will now appear in the list of report formats.

NBE (Legacy OpenVAS report.)	nbe	text/plain	yes (May 27 2011)	yes	    
PDF (Portable Document Format report.)	pdf	application/pdf	yes (May 27 2011)	yes	    
Sourcefire (Sourcefire Host Input Import.)	csv	text/csv	yes (May 30 2011)	no	    
TXT (Plain text report.)	txt	text/plain	yes (May 27 2011)	yes	    
XML (Raw XML report.)	xml	text/xml	yes (May 27 2011)	yes	    

In order to use the report format plugin, you have to activate it first. Before activating any plugin, please ensure that the plugin is trustworthy; the column "Trust" should show the value "yes". If this is the case, click on the  icon and set the option "Active" to "yes". Click the "Save Report Format" button to save your changes.

Edit Report Format ?

Name	<input style="width: 90%;" type="text" value="Sourcefire"/>
Summary	<input style="width: 90%;" type="text" value="Sourcefire Host Input Import."/>
Active	<input checked="" type="radio"/> yes <input type="radio"/> no

Parameters: None

The next step is creating an escalator which connects your GSM to the Sourcefire Defense Center. To do so, open the "Escalators" menu on the GSM and create a new escalator. After specifying a name for the escalator, choose the method "Sourcefire Connector". Enter the IP and port number of your Defense Center and use the "PKCS12 file" entry to select the certificate you downloaded from your Sourcefire Defense Center.

New Escalator ?

Name

Comment (optional)

Event Task run status changed to

Condition Always
 Threat level is at least
 Threat level

Method Email
 To Address
 From Address
 Content Simple notice
 Include report


System Logger (Syslog)







SNMP


HTTP Get
 URL

Sourcefire Connector
 Defense Center IP
 Defense Center Port
 PKCS12 file

Sending results to the Sourcefire Defense Center

To transfer an existing report to the Sourcefire Defense Center, start by opening the report. In the report summary you can now transfer the entire report or a filtered selection by selecting the escalator you just created in the "Escalate" column of the appropriate row and clicking on the  icon.

	High	Medium	Low	Info	Errors	Total	Escalate	Download
Full report:	11	22	19	10	0	62	Sourcefire DC 	PDF 
All filtered results:	11	22	0	0	0	33	Sourcefire DC 	PDF 
Filtered results 1 - 33:	11	22	0	0	0	33	Sourcefire DC 	PDF 

Like every other escalator you can use the Sourcefire Connector to automatically transfer your results to the Defense Center. Just select the escalator you created when creating a new task or modify an existing task using the  icon.

New Task ?

Name: Scan Webserver and report to DC

Comment (optional): e result to the Sourcefire Defense Center

Scan Config: Full and fast

Scan Targets: Webserver

Escalator (optional): Sourcefire DC

Schedule (optional): --

Slave (optional): --

Create Task

It is also possible to transfer the results only if certain conditions are met. You can specify the conditions when creating a new escalator and use this escalator for your tasks as described above.

New Escalator ?

Name: Threat Increase to Sourcefire DC

Comment (optional): e Center if the Threat level has increased

Event: Task: run status changed to Done

Condition: Always
 Threat level is at least High
 Threat level increased

Viewing results in the Sourcefire Defense Center

To view the transmitted results in the Sourcefire Defense Center, select the "Analysis & Reporting: RNA" menu entry and look under "RNA Events". You will now find entries for the hosts scanned by the GSM and information about the detected vulnerabilities.

Scan Vulnerability Detail

Scan Type	OpenVAS
Vulnerability ID	1
Name	Check SSL Weak Ciphers and Supported Ciphers
Description	Server will not supports SSLv2 Ciphers. Server will not supports SSLv3 Ciphers. Server will not supports TLSv1 Ciphers. None of the weak ciphers are supported
BugTraq ID	0
CVE ID	NOCVE