Monitoring Nokia IPSO Firewall

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Nokia IPSO firewall appliance is built based on the IPSO operating system, which was developed from a branch of the FreeBSD operating system, with numerous hardening features applied. This basis makes the Nokia IPSO firewall very stable and more secure to the environments. Nokia IPSO firewall helps organizations that are determined to keep control over their network resources from endlessly increasing security threats. The IPSO firewall reliably protects the environment, provides the ability to sustain the malicious attacks and assures the data confidentiality, integrity and availability of the resources in the environment.

As the firewall plays a very sensitive role in the environment, the uninterrupted firewall operation is imperative to keep the hackers and security attacks at bay. Any issue in the configuration, state, or resource usage of the firewall can stall its operations, leaving your network and all mission-critical applications operating within defence against malicious threats and unscrupulous users! It is hence important that the performance of the Nokia IPSO firewall is monitored 24x7. This can be easily done using a specialized monitoring model offered by eG Enterprise.

Chapter 2: How to Monitor Nokia IPSO Firewall Using eG Enterprise

eG Enterprise monitors the Nokia IPSO firewall using an eG external agent that is deployed on a remote Windows host. This eG agent polls the SNMP MIB of the target firewall to collect the statistics related to performance of the firewall at configured intervals. Before attempting to monitor the firewall, ensure that the firewall is SNMP-enabled.To enable the eG agent to access the SNMP MIB, specify the following while configuring the tests:

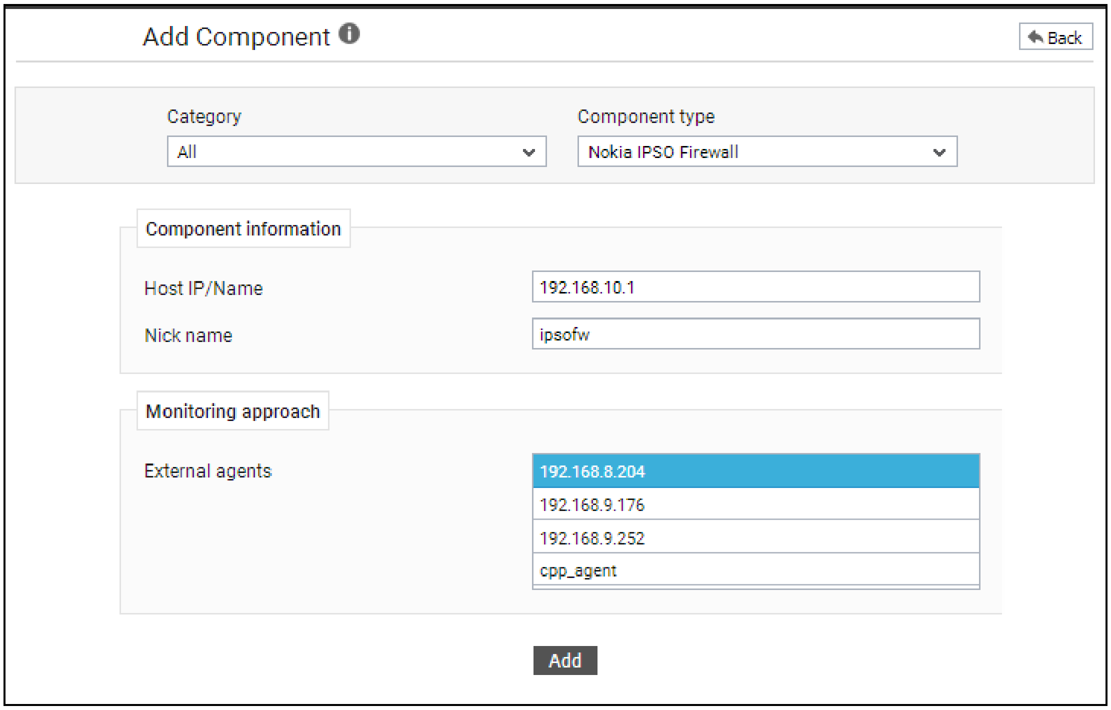
- Port number on which the target firewall exposes its MIB
- SNMP community to be used for accessing the MIB

To start monitoring the target router, first manage the *Nokia IPSO Firewall* component using the steps explained in the section below.

2.1 Managing Nokia IPSO Firewall

Using eG Enterprise, you can auto-discover the Nokia IPSO firewall as well as manually add the component for monitoring. To manage a *Nokia IPSO Firewall* component, do the following:

1. Log into the eG admin interface.
2. If the Nokia IPSO firewall is already discovered, then directly proceed towards managing it using the **Components – Manage/Unmanage/Delete** page.
3. However, if the target firewall is yet to be discovered, then run discovery (Infrastructure -> Components -> Discovery) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **Components** page. Remember that components manually added are managed automatically.
4. In the **Components** page that appears next, select *Nokia IPSO Firewall* as the **Component type**. Then, click the **Add New Component** button. This will invoke the **Add Component** page (Figure 2.1).



Category: All

Component type: Nokia IPSO Firewall

Component information

Host IP/Name: 192.168.10.1

Nick name: ipsofw

Monitoring approach

External agents: 192.168.8.204 (selected), 192.168.9.176, 192.168.9.252, cpp_agent

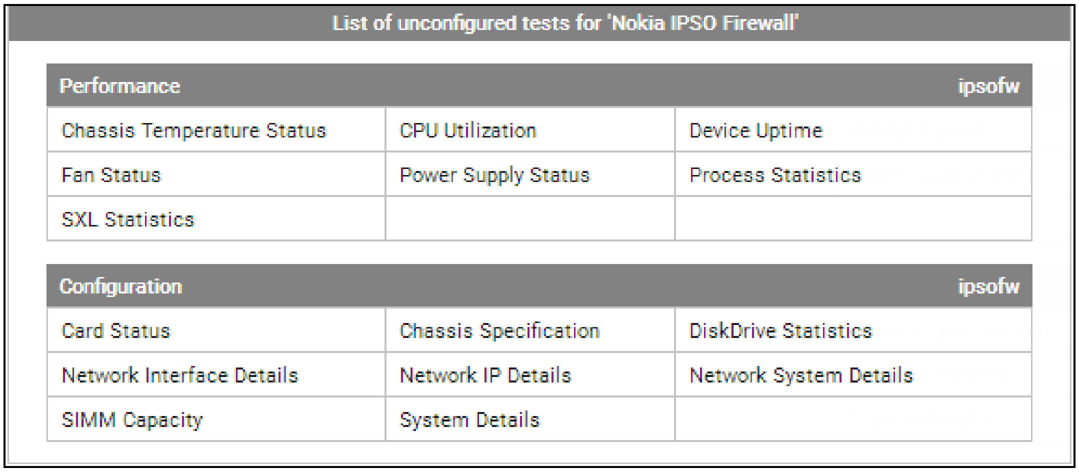
Figure 2.1: Adding the Nokia IPSO Firewall component

5. Specify the **Host IP/Name** and the **Nick name** for the *Nokia IPSO Firewall* component in the **Add Component** page.

6. Choose an external agent for the target router by picking an option from the **External agents** list box.

7. Then, click the **Add** button to register the changes (see Figure 2.1).

8. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.



List of unconfigured tests for 'Nokia IPSO Firewall'

Performance		ipsofw
Chassis Temperature Status	CPU Utilization	Device Uptime
Fan Status	Power Supply Status	Process Statistics
SXL Statistics		

Configuration		ipsofw
Card Status	Chassis Specification	DiskDrive Statistics
Network Interface Details	Network IP Details	Network System Details
SIMM Capacity	System Details	

Figure 2.2: A list of tests that need to be configured for the Nokia IPSO Firewall

9. Click on any test in the list of unconfigured tests to configure. To know how to configure the tests, refer to **Monitoring Nokia IPSO Firewall**.

10. Finally, signout of the eG admin interface.

Chapter 3: Monitoring Nokia IPSO Firewall

eG Enterprise provides a specialized Nokia IPSO firewall monitoring model (see Figure 3.1) that enables administrators to continuously track the resource utilization and status of hardware components of the target firewall. In addition, administrators can also determine critical statistics on processes running on the firewall and the connections handled by the Secure XL.

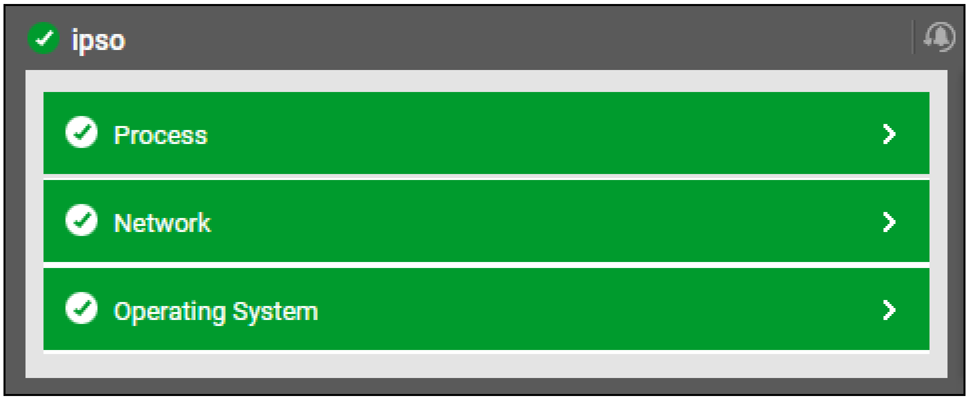


Figure 3.1: The layer model of a Nokia IPSO Firewall

Every layer of Figure 3.1 is mapped to a variety of tests which reports a host of metrics using which administrators can easily find quick and accurate answers to the following performance questions:

- How well the CPU is utilized by the firewall?
- What is the current status of each fan?
- What is the current temperature state of the firewall chassis and each power supply unit?
- What is the current status of the power supply unit?
- What is the CPU utilization of each process running on the target firewall?
- How much memory is utilized by each process on the firewall?
- Is the Secure XL feature enabled on the firewall?
- How many connections are added/deleted by the Secure XL?

The **Network** layer of the Nokia IPSO firewall is similar to that of a Windows Generic Server Monitoring Model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, the sections to come focus on others layer.

3.1 The Operating System Layer

Using the tests mapped to this layer, administrators can easily find out the CPU utilization, temperature and status of the fans and power supply units of the target firewall, and take remedial measures before any serious issues occur.

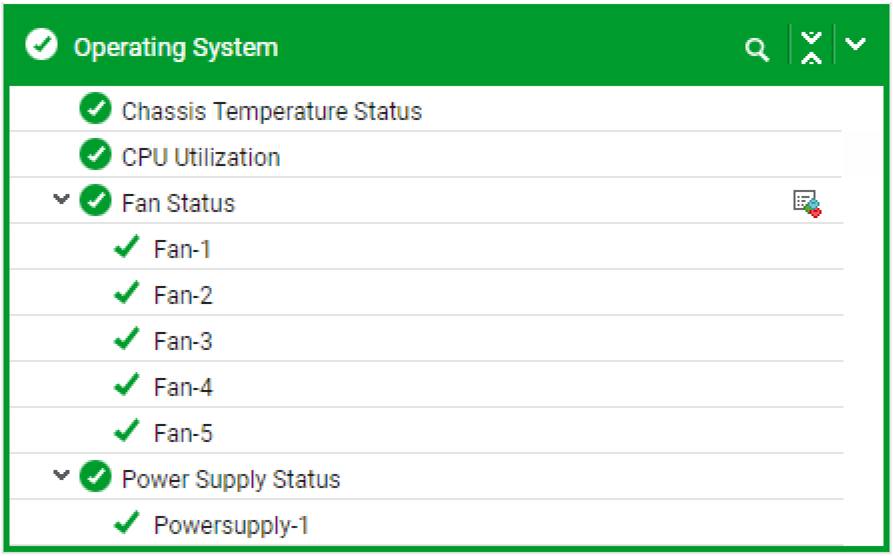


Figure 3.2: The tests mapped to the Operating System layer

3.1.1 CPU Utilization Test

This test monitors the current CPU utilization of the firewall. Using this revelation, administrators can easily determine the excessive usage of CPU resources and troubleshoot the CPU issues (if any) better.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

Parameter	Description
	- **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percentage of CPU utilized by the firewall.	Percent	A value close to 100% is a cause for concern which requires further investigation.

3.1.2 Chassis Temperature Status Test

This test monitors the temperature state of the chassis of the target firewall and reports when the temperature threshold of the chassis is violated beyond the permissible levels.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the

Parameter	Description
	UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Temperature status</td><td>Indicates the current temperature state of the firewall chassis.</td><td></td><td>The values that this measure can report and their corresponding numeric values are tabulated below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Over temperature</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>Measure Value</b>s while indicating the current temperature state of the chassis. However, in the graph of this measure will be represented using the numeric equivalents only.</td></tr>
</table>

3.1.3 Fan Status Test

The Nokia IPSO firewall contains fans to ensure that the internals of the target firewall always receive adequate air flow and the temperature of the firewall is maintained at permissible levels at all times. Unavailability and poor functioning of the fans can hence hamper air flow, which in turn may have disastrous effects on the health of the core components of the firewall. By periodically monitoring the state of the fans, administrator can determine the availability and find out whether/not the fan is currently running. To achieve this, administrators can use the **Fan Status** test.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan of the firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.

Parameter	Description
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this fan.		The values reported by this measure and its numeric equivalents are

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Not available</td><td>0</td></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not running</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each fan. The graph of this measure however is represented using the numeric equivalents only i.e., 0 to 2.</td></tr>
</table>

3.1.4 Power Supply Status Test

Frequent interruptions and temperature fluctuations may damage the power supply unit and, sometimes, could even make the power supply unit unavailable. If the abnormality left unattended for longer duration, it may halt the functioning of the target Nokia IPSO firewall. This in turn may leave the security of the IT environment at risk. To avoid such power fluctuations/interruptions, administrators should be able to detect the unavailability and failure of the power supply unit at the earliest. This is where the **Power Supply Status** test helps!

For each power supply unit of the target firewall, this test reports the current health and temperature status. This way, administrators are alerted to failures (if any) of the power supply units at the earliest and rectify failures before the operation of the target firewall is completely affected.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each power supply unit of the target firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.

Parameter	Description
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this power		The values that this measure can report and their corresponding numeric values

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>supply unit.</td><td></td><td>are tabulated below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Not available</td><td>0</td></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not running</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>Measure Value</b>s while indicating the current status of each power supply unit. However, in the graph of this measure will be represented using the numeric equivalents only.</td></tr>
<tr><td>Temperature state</td><td>Indicates the current temperature state of this power supply unit.</td><td></td><td>The values that this measure can report and their corresponding numeric values are tabulated below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Not available</td><td>0</td></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Over temperature</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>Measure Value</b>s while indicating the current temperature state of this power supply unit. However, in the graph of this measure will be represented using the numeric equivalents only.</td></tr>
</table>

3.2 The Process Layer

The tests pertaining to this layer tracks various statistics pertaining to the processes running on the target Nokia IPSO firewall and the Secure XL feature enabled on the firewall.

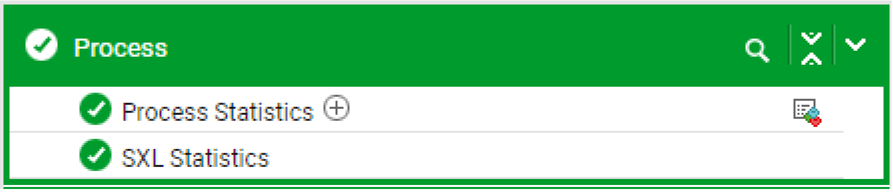


Figure 3.3: The tests associated with the Process layer

3.2.1 Process Statistics Test

This test auto-discovers the processes running on the Nokia IPSO firewall, and reports the CPU and memory utilization of each process. Using these details, administrators can quickly find out the process that is utilizing excessive CPU and memory resources of the firewall.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each process on the target firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This

Parameter	Description
	parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following

Parameter	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percentage of CPU utilized by this process.	Percent	Comparing the values of these measures across the processes will reveal the process that is over-utilizing the CPU and memory resources. This way, administrators can determine whether the process is legitimately utilizing the resources or unusually consuming excessive resources due to malicious attacks.
Memory	Indicates the amount of memory utilized by this process.	KB	

3.2.2 SXL Statistics Test

Secure XL (SXL) is the security performance architecture of Check Point VPN-1/FireWall-1 and Nokia security appliances. When the SXL feature is enabled for the Nokia IPSO firewall, the architecture offloads multiple CPU intensive security operations to optimize Nokia IPSO code running on Intel x86 hardware or on network processor hardware. The optimized IPSO code reduces the overhead involved in performing the security operations. As a result of the reduced overhead, SXL accelerates firewall performance, throughput and connection rate by remembering certain attributes of packets and packet flows that have already been validated by the firewall. If the SXL is disabled abruptly due to any abnormal reason, the firewall may not be able to handle the traffic faster as the firewall needs to validate the connection details everytime. Therefore, it is important for administrators to continuously monitor the current status of the SXL and the traffic handled by the SXL at regular intervals. This can be easily achieved using the **SXL Statistics** test!

Using this test, administrators can instantly find out whether/not the Secure XL feature is enabled for the target firewall. In the process, this test also reveals the count of connections that are added to the firewall/deleted, by the SXL.

Target of the test : Nokia IPSO Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target firewall that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the target firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the

Parameter	Description
	required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>SXL Status</td><td>Indicates whether the Secure XL is enabled or not.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>1</td></tr>
<tr><td>Disabled</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of the Secure XL. The graph of this measure however is represented using the numeric equivalents only i.e., 0 to 1.</td></tr>
<tr><td>Existing connections</td><td>Indicates the number of connections that have already been validated by the Secure XL.</td><td>Number</td><td>A low value of this measure may indicate that the count of connections validated by the SXL is less. Therefore, the firewall needs to natively verify the connection details everytime. This approach may increase the processing</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			overheads and time required to establish the connections through the target firewall.
Accepted connections	Indicates the number of connections that are added to the firewall by the Secure XL.	Number	
Deleted connections	Indicates the number of connections that are deleted by the Secure XL.	Number	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.