Monitoring Juniper Netscreen SSG

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW TO MONITOR JUNIPER NETSCREEN SSG USING EG ENTERPRISE? 2

2.1 Managing the Juniper Netscreen SSG 2

2.2 Configuring the tests 3

CHAPTER 3: MONITORING THE JUNIPER NETSCREEN SSG 4

3.1 The Operating System Layer 5

3.1.1 Nsc Batteries Test 5

3.1.2 Nsc Fan Test 8

3.1.3 Nsc Power Test 11

3.1.4 Nsc TemperatureTest 13

3.2 The NSC Server Layer 16

3.2.1 Nsc Resources Test 16

3.3 The NSC Service Layer 19

3.3.1 Nsc Attacks Test 19

3.3.2 Nsc Interfaces Test 25

3.3.3 Nsc Policies Test 28

3.3.4 Nsc Vpns Test 31

ABOUT EG INNOVATIONS 35

Table of Figures

Figure 2.1: Adding the Juniper Netscreen SSG 3
Figure 2.2: A list of unconfigured tests for Juniper Netscreen SSG 3
Figure 3.1: Layer model of the Netscreen Firewall 4
Figure 3.2: The tests mapped to the Operating System layer 5
Figure 3.3: Tests associated with the NSC Server layer 16
Figure 3.4: The tests associated with the NSC Service layer 19

Chapter 1: Introduction

NetScreen's full-featured firewall uses technology based on stateful inspection, securing against intruders and denial-of-service attacks. NetScreen's custom-built ASIC processes the firewall access policies and encryption algorithms in hardware.

If the access policies of the Netscreen firewall are misconfigured, then the environment will be exposed to harmful virus attacks and intrusion from malicious users. It is therefore imperative that the firewall is monitored 24 x 7 for availability and all-round health. This is where eG Enterprise helps administrators.

Chapter 2: How to Monitor Juniper Netscreen SSG Using eG Enterprise?

eG Enterprise adopts agentless approach to monitor the Juniper Netscreen SSG firewall. A single eG external agent is all that is required to monitor a firewall. This agent, when deployed on a remote host, executes tests that connect to the SNMP MIB of the firewall device to be monitored, and collects statistics of interest from it. The key pre-requisite for monitoring the firewall device is enabling SNMP on the target firewall device. Once this requirement is kept in place, start monitoring the firewall device. There are two broad steps for monitoring the firewall device:

- Managing the Juniper Netscreen SSG
- Configuring the tests

2.1 Managing the Juniper Netscreen SSG

The eG Enterprise cannot automatically discover the Juniper Netscreen SSG firewall device. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Juniper Netscreen SSG firewall device, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Juniper Netscreen SSG* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

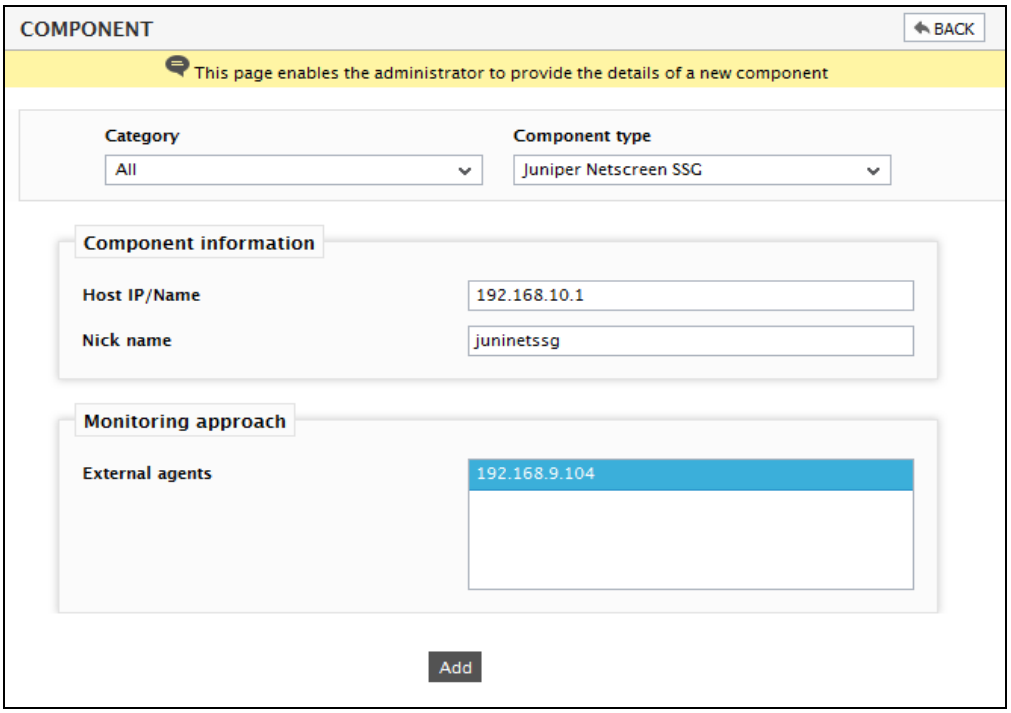
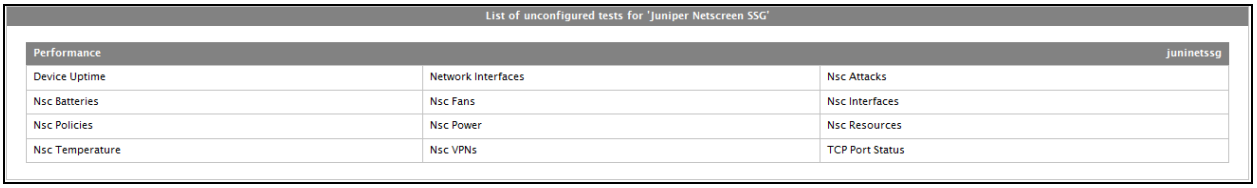


Figure 2.1: Adding the Juniper Netscreen SSG

4. Specify the **Host IP** and the **Nick name** of the Juniper Netscreen SSG firewall device in Figure 2.1. Then click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2) listing the tests that require manual configuration.


List of unconfigured tests for 'Juniper Netscreen SSG'

Performance		juninetssg
Device Uptime	Network Interfaces	Nsc Attacks
Nsc Batteries	Nsc Fans	Nsc Interfaces
Nsc Policies	Nsc Power	Nsc Resources
Nsc Temperature	Nsc VPNs	TCP Port Status

Figure 2.2: A list of unconfigured tests for Juniper Netscreen SSG

2. Click on the tests to configure. To know how to configure the tests, refer to the **Monitoring the Juniper Netscreen SSG** chapter.
3. Then, try to signout of the eG administrative interface. Now, you will be prompted to configure the **Device Uptime** test and the **Network Interfaces** test. To know more about how to configure the **Device Uptime** and **Network Interfaces** tests, refer to the *Monitoring Cisco Router* document.
4. Finally, signout of the administrative interface.

Chapter 3: Monitoring the Juniper Netscreen SSG

eG Enterprise has designed a specialized Juniper Netscreen SSG monitoring model (see Chapter 3), which periodically monitors the Netscreen firewall device and reports the following key statistics, which provide administrators with effective pointers to the source of their firewall problems, and tips to fine-tune their firewall configuration.

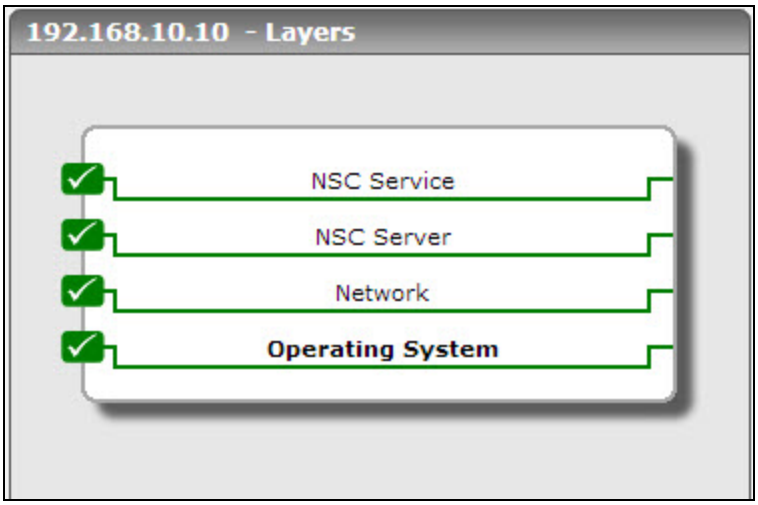


Figure 3.1: Layer model of the Netscreen Firewall

Each layer of the layer model is mapped with number of tests that report the metrics related to performance of the Netscreen firewall device. These metrics provide the accurate answers for the following performance queries;

- Is the Firewall device experiencing a shortage of resources?
- Were any malicious attacks attempted on the environment recently? What type of attacks were they?
- Is the data flow between the network interfaces smooth, or were too many data packets dropped?
- Is traffic to the Netscreen policies optimal?
- Is the Netscreen VPN tunnel available and healthy?

The sections to come discuss each layer of the layer model elaborately.

3.1 The Operating System Layer

The tests mapped to this layer proactively alert administrators to the potential failure of the Netscreen batteries, fans, and power supply units, and any abnormal increase in the temperature of the board or any core component of the Netscreen SSG.

Figure 3.2: The tests mapped to the Operating System layer

3.1.1 Nsc Batteries Test

A defective battery, if not detected in time and replaced, can bring firewall operations to a halt. To avert it, you can use this test to continuously track the status of the Netscreen batteries, so that you can be promptly alerted when any of the batteries encounter errors/failures.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

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

Parameter	Description
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 • **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

Parameter	Description
	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
Battery status	Indicates the current status of the firewall battery.		If the installed battery encounters an errors, the value of this measure will be *Error*. If the battery is operating normally, then the value of this measure will be *Good*. The numeric values that correspond to these measure values have been listed in the table below: **Measure Value** / **Numeric Value** Good – 100 Error – 0 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports one of the **Measure Value**s listed in the table above to indicate battery status. In the graph of this measure however, the battery status will be represented using the numeric equivalents - 100 or 0.

3.1.2 Nsc Fan Test

Fans ensure that the temperature of the core components of the firewall are well-within operable limits. If one/more fan modules fail, then the temperature of sensitive hardware may soar causing permanent hardware damage. With the help of this test, you can instantly detect a fan failure, so that remedial measures can be swiftly initiated to prevent any irrepairable damage to hardware.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan module that is installed in the Netscreen firewall being managed.

Configurable parameters for the test

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

Parameter	Description
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 encryption types:

Parameter	Description
	• **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
Fan Status	Indicates the current status of this fan module.		If any fan module fails, then the value of this measure will be *Failed*. If the fan is operating normally, then the value of this measure will be *Good*. The numeric values that correspond to these measure values have been listed in the table below: **Measure Value** / **Numeric Value** Good – 100 Failed – 0 **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate fan status. In the graph of this measure however, the fan

Measurement	Description	Measurement Unit	Interpretation
			status will be represented using the numeric equivalents - 100 or 0.

3.1.3 Nsc Power Test

This test reports the status of the power supply unit of the Netscreen firewall.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

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

Parameter	Description
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.
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.

Parameter	Description
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
Power Status	Indicates the current status of the power supply unit.		The values that this measure reports and the numeric values that correspond to these measure values have been listed in the table below: Measure Value / Numeric Value Good – 100 Failed – 0 Not Installed – 2 **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate power status. In the graph of this measure however, the same will be represented using the numeric equivalents - 100, 0, or 2.

3.1.4 Nsc TemperatureTest

Sudden spikes in the temperature of critical Netscreen hardware - eg., its board/core components - can prove to be fatal, causing permanent hardware damage and bringing firewall operations to a standstill. By periodically monitoring the temperature of such components, the test notifies you of any abnormal increase in temperature, so that you can promptly intervene and do the needful to control it.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

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

Measurement	Description	Measurement Unit	Interpretation
Temperature Status	Indicates the current temperature of the board/core component.	Celsius	A sudden spike or a consistent increase in the value of this measure, is a cause for concern.

3.2 The NSC Server Layer

The test associated with this layer monitors the resource usage of the Netscreen firewall.

Figure 3.3: Tests associated with the NSC Server layer

3.2.1 Nsc Resources Test

This test measures the resource (CPU and memory) utilization of the Netscreen firewall device.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for every interface of the Netscreen firewall being managed.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the firewall device for which this test is to be configured.

Parameter	Description
Port	The port at which the specified firewall device listens.
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:

Parameter	Description
	• **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
CPU utilization	Indicates the percentage of CPU utilized.	Percentage	
CPU usage in the last minute	Indicates the percentage of CPU utilized during the last minute	Percent	
CPU usage in the	Indicates the percentage	Percent	

Measurement	Description	Measurement Unit	Interpretation
last 5 minutes	of CPU utilized during the last five minutes.		
Memory allocated	Indicates the allocated memory.	MB	
Free memory	Indicates the free memory.	MB	
Failed sessions	Indicates the number of failed session allocation counters.	Number	
Active sessions	Indicates the number of sessions that are currently active.	Number	
Allocated sessions	Indicates the number of sessions allocated by the Netscreen Firewall.	Number	

3.3 The NSC Service Layer

The tests mapped to this layer measure the overall health of the Netscreen firewall service (see Figure 3.4).

Figure 3.4: The tests associated with the NSC Service layer

3.3.1 Nsc Attacks Test

This test reports statistics pertaining to the attack attempts made on the Netscreen Firewall device.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

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

Parameter	Description
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

Measurement	Description	Measurement Unit	Interpretation
Syn attacks	A SYN attack involves a system sending hundreds of requests to a server on the Internet. This measure reveals the number of syn attacks on the Netscreen firewall during the last measurement period.	Number	
Tear drop attacks	If the attacker's IP puts a confusing value in the offset of the packet fragment, such that the packet cannot be reassembled properly, then such an attack is termed as a Tear drop attack. This measure reports the number of tear drop attacks on the Netscreen firewall during the last measurement period.	Number	
Source route attacks	Source route option attacks are attacks that occur when the sender sends the route for the packets to travel to the destination memory. This measure reveals the number of source route option attacks on the firewall during the last measurement period.	Number	
Ping of death attacks	If the attacker sends an IP packet larger than 65536 bytes due to which the system crashes, then such	Number	

Measurement	Description	Measurement Unit	Interpretation
	an attack can be called a ping death attack. This measure reports the number of such attacks during the last measurement period.		
Address spoof attacks	If the IP address is spoofed when systems are attacked, then it becomes an address spoof attack. This measure reveals the number of address spoof attacks that were encountered by the firewall during the last measurement period.	Number	
Land attacks	A Land attack is a remote denial-of-service condition caused by sending a packet to a machine with the source host/port the same as the destination host/port. This measure indicates the number of land attacks on the Netscreen firewall device during the last measurement period.	Number	
ICMP flood attacks	An ICMP flood occurs when ICMP pings overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. This measure indicates the number of ICMP flood	Number	

Measurement	Description	Measurement Unit	Interpretation
	attacks on the firewall during the last measurement period.		
Udp flood attacks	UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. This measure reports a count of such attacks during the last measurement period.	Number	
Netbios attacks	Netbios is an interface between the PC operating system, I/O bus and network. Name resolution, file and print sharing (SMB), netbios browsing and logon are its activities. This measure reveals the number of weird Netbios attacks during the last measurement period.	Number	Attacks related to NETBIOS network: If port 139 is open, files are shared over the network. Other components of NETBIOS can expose one's computer name, workgroup, user name and other information. One can use 'nbtstat' to enumerate a network by listing NETBIOS names tables and sessions as a prelude to further penetration.
Port scan attacks	A port scan attack is where an IP sends packets to different ports of the same destination IP, so that atleast one service could be identified as target of the attack. This measure indicates the number of port scan attacks that occurred during the last measurement period.	Number	
IP sweep attacks	A sweep attack is where a range of IP addresses are scanned to show which IP	Number	

Measurement	Description	Measurement Unit	Interpretation
	addresses are in use. This measure indicates the number of such sweep attacks during the last measurement period.		

3.3.2 Nsc Interfaces Test

This test reveals key statistics pertaining to the dropped packets collected from the interface.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

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

Measurement	Description	Measurement Unit	Interpretation
Packets dropped by policy	Indicates the number of packets that were dropped since they were denied by the Firewall policy.	Number	
Authentication failures	Indicates the number of packets that were dropped due to authentication failure	Number	
Drops by URL blocks	Indicates the number of packets dropped due to URL blocking.	Number	
Packets queued	Indicates the number of packets in queue due to traffic management.	Number	
Packet drops due to high traffic	Indicates the number of packets dropped due to heavy traffic.	Number	
Packet drops for no SA	Indicates the number of packets dropped due to no SA (Security Association) found for incoming SPI (Security Parameters	Number	

Measurement	Description	Measurement Unit	Interpretation
	Index)		
SA policy drops	Indicates the number of packet dropped due to no policy associated with found SA.	Number	
Inactive SA drops	Indicates the number of packets dropped due to SA being inactive.	Number	
No SA policy drops	Indicates the number of packets dropped due to denial of SA policy.	Number	

3.3.3 Nsc Policies Test

This test reports the policy-based traffic information of the Netscreen firewall device.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Netscreen firewall being managed.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the firewall device for which this test is to be configured.
Port	The port at which the specified firewall device listens.
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
Packet rate	Indicates the number of packets going through the Netscreen policy per second.	Packets/Sec	
Packet count	Indicates the total number of packets going through the policy.	Number	
Data traffic	Indicates the number of bytes going through the policy per second.	MB/Sec	
Data handled	Indicates the total number of bytes going through the policy.	Number	
Session rate	Indicates the number of sessions going through the	Sessions/Sec	

Measurement	Description	Measurement Unit	Interpretation
	policy per second.		
New sessions	Indicates the number of new sessions going through the policy.	Sessions	

3.3.4 Nsc Vpns Test

This test monitors the VPN tunnels of the Netscreen Firewall component.

Target of the test : A Juniper Netscreen SSG Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for every VPN tunnel in the Netscreen Firewall being monitored.

Configurable parameters for the test

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

Parameter	Description
	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 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

Measurement	Description	Measurement Unit	Interpretation
Monitor state	Indicates the current monitoring status of the VPN tunnel.	Boolean	If the monitoring status is 'true', then an ICMP ping is sent over the tunnel to test the connectivity and latency.
Tunnel state	Indicates the current status of the VPN tunnel.	Boolean	If the Monitor_state is 'true, then the ICMP ping that is sent over the tunnel will reveal the current state of the tunnel.
Last delay	Indicates the latency during the last measurement period.	Secs	If this measure returns an 'Unknown' value, it indicates that the tunnel is either inactive or the tunnel monitor is not turned on.
Avg delay	Indicates the average of latency.	Secs	
Incoming data traffic	Indicates the rate of data coming into the tunnel.	KB/Sec	
Outgoing data traffic	Indicates the rate of data going out of the tunnel.	KB/Sec	
Incoming packets	Indicates the rate at which data packets entered the tunnel.	Packets/Sec	
Outgoing packets	Indicates the rate at which	Packets/Sec	

Measurement	Description	Measurement Unit	Interpretation
	data packets went out of the tunnel.		

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.