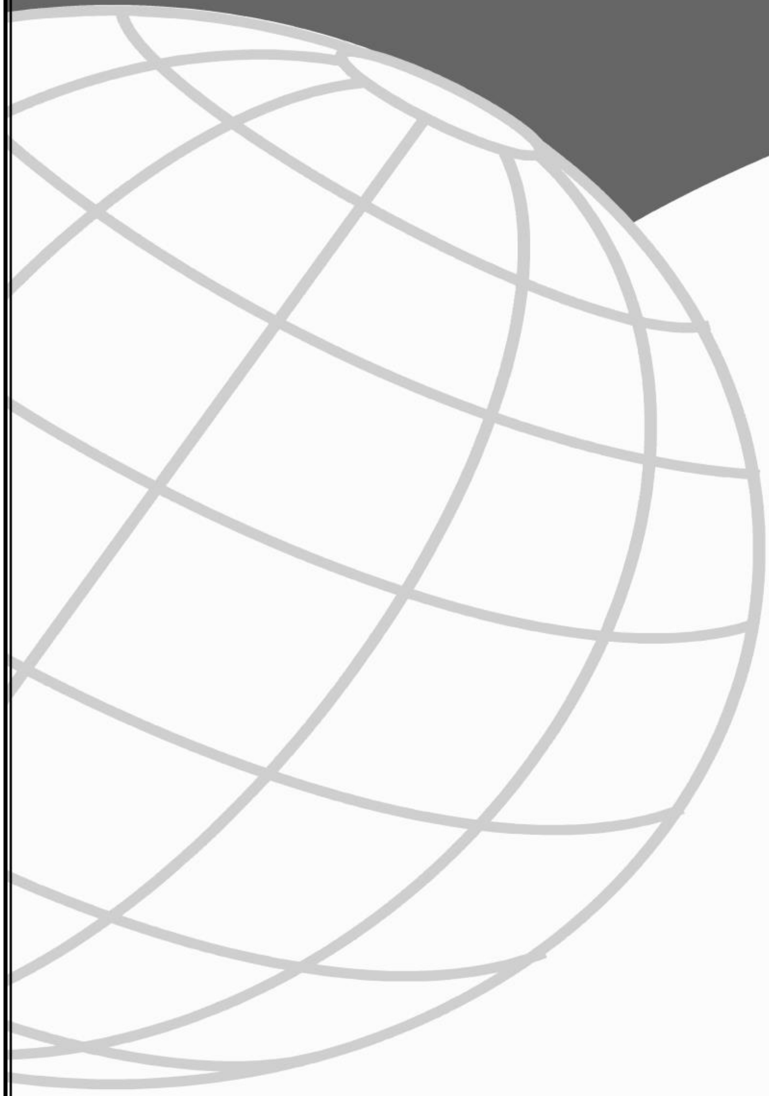


Enabling Service Excellence

Monitoring Firewalls

eG Enterprise v6.0

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2003, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Table of Figures

Chapter

1

Introduction

A firewall is a network security device positioned between two different networks, usually between an organization’s internal, trusted network and the Internet. A firewall ensures that all communications attempting to cross from one network to the other meet the security policy of the organization. A firewall tracks and controls communication, deciding whether to allow, reject or encrypt the data being transmitted.

Firewalls play an important role in an IT infrastructure. They serve to guard the web site from malicious attacks. Multiple levels of firewalls may also be used to protect the application servers and databases. Since a firewall lies on all data communications to and from an eBusiness site, a problem with the firewall can affect all accesses to the site. Hence, the eG Enterprise suite of products includes customized monitoring capabilities for firewalls.

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.

This document details the metrics that the eG agent collects from each of the popular firewall devices it provides monitoring support to.

Chapter

2

Monitoring the CheckPoint Firewall - 1

Integrated into the VPN-1 product line, FireWall-1 is the industry's leading firewall solution, delivering the most secure line of defense. Using INSPECT, the most adaptive and intelligent inspection technology, FireWall-1 integrates both network and application-layer firewall protection. This means that problems with FireWall-1 can driill holes in this 'wall of defence', thus exposing both the network and application layers to malicious attacks.

Continuous monitoring of FireWall-1 can however keep such problems at bay.

eG Enterprise provides a specialized *CheckPoint* monitoring model (see Figure 2.1) , that enables administrators to keep an eye on the accesses to the protected environment and judge whether the firewall succeeds in preventing unauthorized accesses.

To obtain statistics specific to a Check Point Firewall-1, the eG agents rely on the SNMP interface supported by the Check Point Firewall. Through the eG Enterprise's administrative interface, the port number on which the Check Point Firewall exposes its MIB as well as the SNMP community to be used for accessing the MIB must be specified.

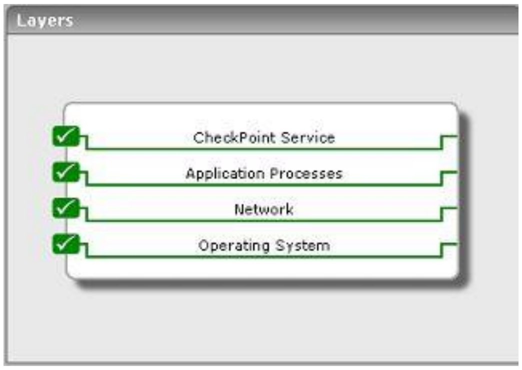


Figure 2.1: Layer model for a Check Point firewall

As the three layers at the bottom of Figure 2.1 have already been discussed in the *Monitoring Unix and Windows Servers* document, the sections to come will discuss the **CheckPoint Service** layer alone.

2.1 The CheckPoint Service Layer

This layer monitors the health of the Check Point firewall using the CheckPoint test shown in Figure 2.2.

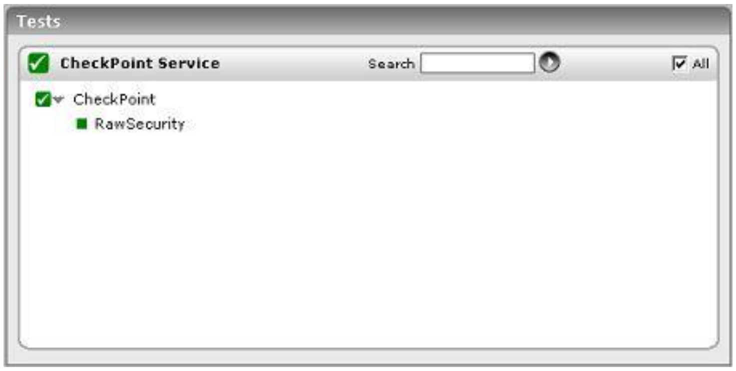


Figure 2.2: Tests mapping to the CheckPoint Service layer.

RawSecurity is the name of the policy configured for the firewall being monitored.

2.1.1 CheckPoint Test

This test monitors the service provided by a Check Point Firewall-1.

Purpose	To measure the performance of a Check Point Firewall-1.
Target of the test	A Check Point Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Firewall server 3. **PORT** - The port number through which the Check Point Firewall communicates. 4. **SNMPPORT** – The SNMP Port number of the Check Point Firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for every Check Point Firewall being managed.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Processing rate: This measure indicates the rate at which the packets are being handled by the firewall.	Pkts/Sec	A high value indicates an increasing load on the firewall.
	Accepts: Indicates the percentage of packets that have been permitted to pass through by the firewall.	Percent	A value much lower than 100% may indicate a problem with the firewall policy configured or that the eBusiness site may be under attack.
	Rejects: Indicates the percentage of packets that have been rejected by the firewall.	Percent	A high value is indicates that one or more rules of the firewall policy are causing rejection of packets. A review of the firewall logs will provide more details regarding the details of the rejections.
	Packet drops: Indicates the percentage of packets that have been dropped by the firewall. Note that when a firewall rejects a packet, it generates an explicit rejection message to the sender, whereas when the firewall drops a packet, no explicit message is sent back.	Percent	A high value denotes that unauthorized accesses may be attempted and hence the corresponding packets are being dropped by the firewall.

Chapter

3

Monitoring Cisco PIX Firewalls

Cisco PIX 500 Series Firewalls are purpose-built security appliances that deliver enterprise-class security services including stateful inspection firewalling, standards-based IPsec Virtual Private Networking (VPN), intrusion protection and much more.

In an environment where a Cisco PIX firewall is used, the continuous availability of the firewall device and its error-free functioning is very crucial to the safety of the data that is transacted within the environment. Continuous monitoring of the Cisco PIX firewall hence becomes imperative.

eG Enterprise offers a 100% web-based *Cisco PIX* monitoring model (see Figure 3.1) that monitors the status of the hardware and connections to the Cisco PIX firewall, and in the process, reports abnormalities (if any).

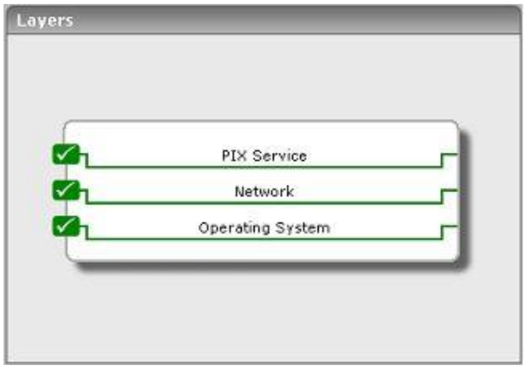
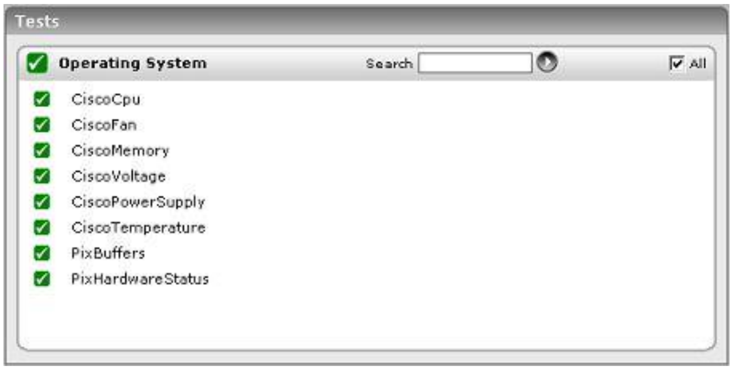


Figure 3.1: The layer model of a Cisco PIX firewall

Every layer of Figure 3.1 is mapped to one/more tests that execute on the firewall, and extract critical performance statistics from the SNMP MIB of the firewall. The sections to come discuss each layer in great detail.

3.1 The Operating System Layer

This layer reveals whether the firewall is loaded with sufficient hardware resources to enable optimum performance (see Figure 3.2).



Tests

☑ Operating System Search ☑ All

☑ CiscoCpu
☑ CiscoFan
☑ CiscoMemory
☑ CiscoVoltage
☑ CiscoPowerSupply
☑ CiscoTemperature
☑ PixBuffers
☑ PixHardwareStatus

Figure 3.2: The tests associated with the Operating System layer of a Cisco PIX firewall

The CiscoCpu, CiscoFan, CiscoMemory, CiscoVoltage, CiscoTemperature, and CiscoPowerSupply tests have been discussed elaborately in Chapter 2 of the *Monitoring Network Elements* document. The sections that follow will hence provide details about the PixBuffers and PixHardwareStatus test only.

3.1.1 PixBuffers Test

The PixBuffers test measures the system buffer usage of a Cisco PIX device.

Purpose	To measure the system buffer usage of a Cisco PIX device
Target of the test	A Cisco PIX Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Cisco PIX firewall 3. **SNMPPORT** – The SNMP Port number of the Cisco PIX firewall (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

Outputs of the test	One set of results for every Cisco PIX firewall being managed.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Maximum allocated: The maximum number of allocated blocks since system startup.	Number	
	Buffers available: The current number of available blocks.	Number	A low value indicates a memory bottleneck.
	Fewest available: The fewest blocks available since system startup.	Number	By tracking this value over time, an administrator can determine times when buffer availability was at its minimum.

3.1.2 PixHardwareStatus Test

This test reports the status of various hardware units of a Cisco PIX device.

Purpose	Reports the status of various hardware units of a Cisco PIX device
Target of the test	A Cisco PIX Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Cisco PIX firewall 3. **SNMPPORT** – The SNMP Port number of the Cisco PIX firewall (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: ➢ The eG manager license should allow the detailed diagnosis capability ➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for every hardware unit associated with a Cisco PIX firewall being managed.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Status: The current status of various hardware units like memory, disk, power, network interface, cpu, primary unit, secondary unit etc.	Number	The value 1 indicates that the hardware unit is functioning properly. A value of 0 indicates a problem.

3.2 The Network Layer

The **Network** layer, as always, checks whether the firewall device is available over the network or not, and monitors the percentage of bandwidth used by each network interface supported by the firewall.

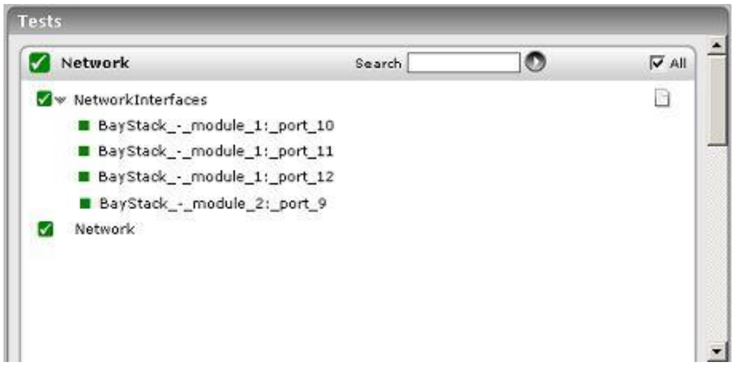

Tests
Network
Search
All
NetworkInterfaces
BayStack_-_module_1:_port_10
BayStack_-_module_1:_port_11
BayStack_-_module_1:_port_12
BayStack_-_module_2:_port_9
Network

Figure 3.3: The tests mapped to the Network layer of the Cisco PIX firewall

3.3 The PIX Service Layer

The test associated with this layer measures the workload on the firewall device in terms of the number of connections to it.

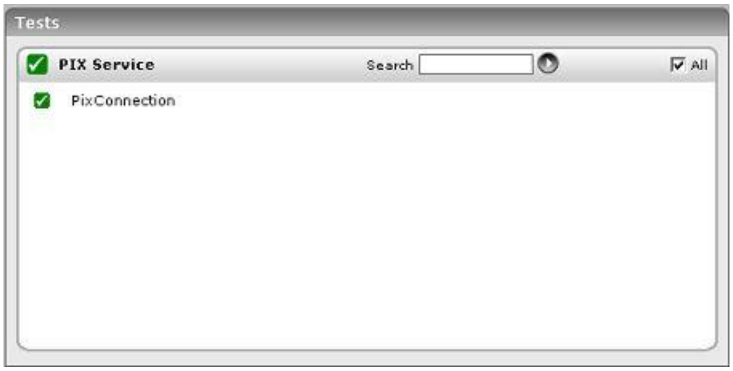


Figure 3.4: The test associated with the PIX Service layer

3.3.1 PixConnection Test

The PixConnection test reports the connection-related statistics pertaining to a Cisco PIX firewall.

Purpose	Reports the connection-related statistics pertaining to a Cisco PIX firewall
Target of the test	A Cisco PIX Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Cisco PIX firewall 3. **SNMPPORT** – The SNMP Port number of the Cisco PIX firewall (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

Outputs of the test	One set of results for every Cisco PIX firewall being managed.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Open connections: The number of currently opened connections	Number	This metric is an indicator of the current workload.
	Closing connections: The number of currently closing connections	Number	
	Half open connections: The number of half opened connections	Number	
	Connections in use: The number of connections currently in use	Number	

Chapter

4

Monitoring the Juniper Netscreen SSG

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.

eG Enterprise has designed a specialized *Juniper Netscreen SSG* monitoring model (see Figure 4.1), 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.

- 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?

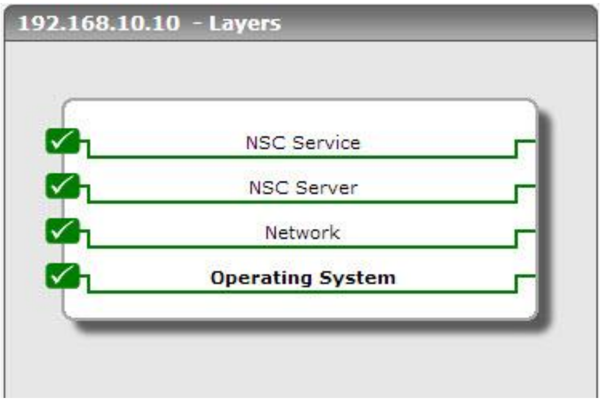


Figure 4.1: Layer model of the Netscreen Firewall

The sections to come discuss each layer of Figure 4.1 elaborately.

4.1 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.

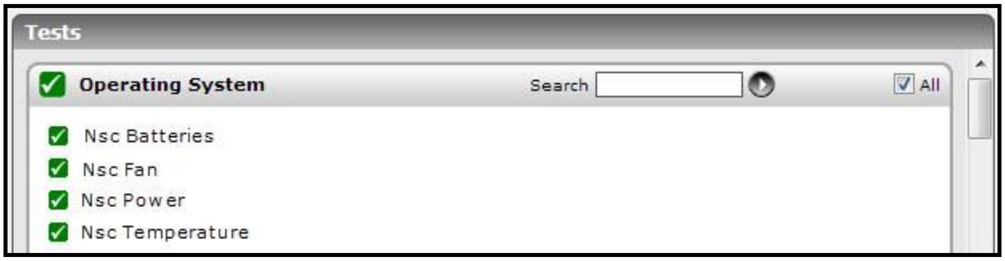


Figure 4.2: The tests mapped to the Operating System layer

4.1.1 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.

Purpose	Continuously tracks 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 Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b>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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the Netscreen firewall being managed</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Battery status:</b>
Indicates the current status of the firewall battery.</td><td></td><td>If the installed battery encounters an errors, the value of this measure will be <i>Error</i>. If the battery is operating normally, then the value of this measure will be <i>Good</i>. The numeric values that correspond to these measure values have been listed in the table below:<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>100</td></tr><tr><td>Error</td><td>0</td></tr></table><b>Note:</b>
By default, this measure reports one of the <b>Measure Values</b> 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.</td></tr>
</table>

4.1.2 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.

Purpose	Instantly detects and reports a fan failure, so that remedial measures can be swiftly initiated to prevent any irrepairable damage to hardware
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b>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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan module that is installed in the Netscreen firewall being managed</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Fan Status:</b>
Indicates the current status of this fan module.</td><td></td><td>If any fan module fails, then the value of this measure will be <i>Failed</i>. If the fan is operating normally, then the value of this measure will be <i>Good</i>. The numeric values that correspond to these measure values have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>100</td></tr>
<tr><td>Failed</td><td>0</td></tr>
</table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Values</b> listed in the table above to indicate fan status. In the graph of this measure however, the fan status will be represented using the numeric equivalents - 100 or 0.</td></tr>
</table>

4.1.3 Nsc Power Test

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

Purpose	Reports the status of the power supply units of the Netscreen firewall
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b>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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the Netscreen firewall being managed</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Power Status:</b>
Indicates the current status of the power supply unit.</td><td></td><td>The values that this measure reports and the numeric values that correspond to these measure values have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>100</td></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Not Installed</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Values</b> 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.</td></tr>
</table>

4.1.4 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.

Purpose	Periodically monitors the temperature of board/core components and notifies administrators of abnormal increase in temperature
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Netscreen firewall being managed		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Temperature Status: Indicates the current temperature of the board/core component.	Celcius	A sudden spike or a consistent increase in the value of this measure, is a cause for concern.

4.2 The NSC Server Layer

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

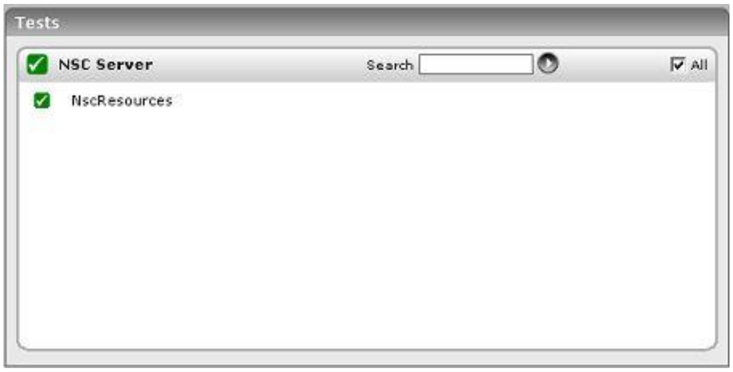


Figure 4.3: Tests associated with the NSC Server layer

4.2.1 Nsc Resources Test

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

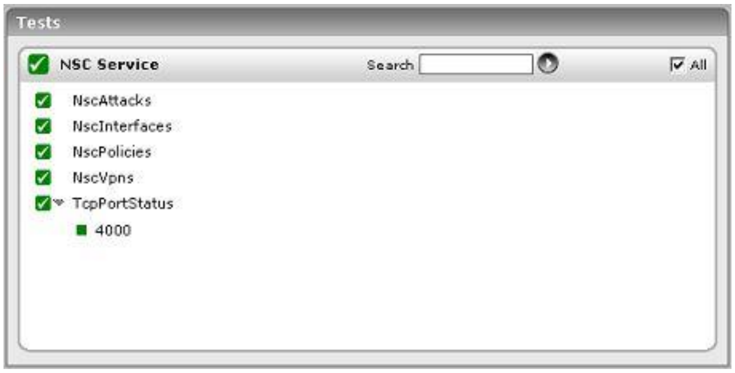
Purpose	Measures the resource (CPU and memory) utilization of the Netscreen firewall device
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for every interface of the Netscreen firewall being managed		
Measurements made by the test	**Measurement**	**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 last 5 minutes: Indicates the percentage of CPU utilized during the last five minutes.	Percent	
	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	

4.3 The NSC Service Layer

The tests mapped to this layer measure the overall health of the Netscreen firewall service (see Figure 4.4).



Tests

☑ NSC Service Search ☑ All

☑ NscAttacks
☑ NscInterfaces
☑ NscPolicies
☑ NscVpns
☑ TcpPortStatus
🟩 4000

Figure 4.4: The tests associated with the NSC Service layer

4.3.1 Nsc Attacks Test

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

Purpose	Reports statistics pertaining to the attack attempts made on the Netscreen Firewall device
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Netscreen firewall being managed		
Measurements made by the test	**Measurement**	**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 an attack can be called a ping death attack. This measure reports the number of such attacks during the last measurement period.	Number	
	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 attacks on the firewall during the last measurement period.	Number	
	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 addresses are in use. This measure indicates the number of such sweep attacks during the last measurement period.	Number	

4.3.2 Nsc Interfaces Test

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

Purpose	Reveals key statistics pertaining to the dropped packets collected from the interface
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Netscreen firewall being managed		
Measurements made by the test	**Measurement**	**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 Index)	Number	
	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	

4.3.3 Nsc Policies Test

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

Purpose	Reports the policy-based traffic information of the Netscreen firewall device
Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Netscreen firewall being managed		
Measurements made by the test	**Measurement**	**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 policy per second.	Sessions/Sec	
	New sessions: Indicates the number of new sessions going through the policy.	Sessions	

4.3.4 Nsc Vpns Test

The NscVpns test monitors the VPN tunnels of the Netscreen Firewall component.

Purpose	Monitors the VPN tunnels of the Netscreen Firewall component

Target of the test	A Netscreen Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Netscreen firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Netscreen firewall (161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for every VPN tunnel in the Netscreen Firewall being monitored		
Measurements made by the test	**Measurement**	**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 data packets went out of the tunnel.	Packets/Sec	

Chapter

5

Monitoring FortiGate Firewalls

FortiGate's firewall series of ASIC accelerated antivirus firewalls are the new generation of real time protection systems for LAN, VPN, WAN and wireless network security. Capable of providing anitvirus/worm protection for emails, network inrusion detection, web content filtering based on URLS and keywords and traffic shaping, the FortiGate Antivirus Firewall products secure the network without degrading its performance.

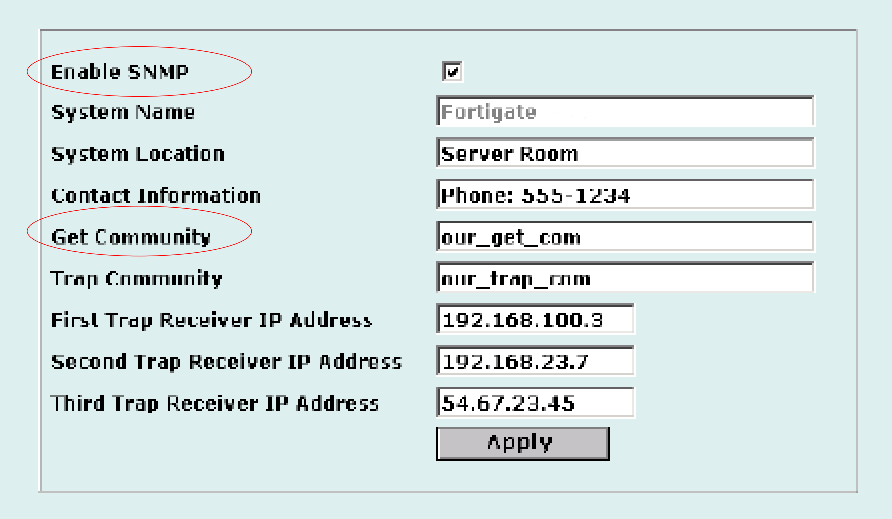
High availability of the firewall is therefore imperative to ensure the safety of the mission-critical environment it protects. If the availability of the firewall is challenged, then the IT environment is rendered defenceless against unsavory virus attacks and unauthorized access, both of which can cause irreparable damage. Hence, to make sure that an IT environment stays protected 24X7x365 from network threats, the availability and performance of the firewall should be continuously monitored.

eG Enterprise offers two specialized monitoring models to monitor different versions of the FortiGate Firewall - the *Fortigate Firewall 3x* model that performs a thorough, top-down monitoring of the various aspects of performance of FortiGate Firewall v3 (and its variants), and the *Fortigate Firewall* model that provides indepth insights into the performance of the FortiGate Firewall v4 (and above) .

With the help of both these models, you can keep track of the variations in a wide range of critical performance parameters - from the session activity on the firewall to its resource utilization and its ability to detect attacks. Analysis of the statistics collected enable administrators to proactively detect performance anomalies at the firewall, and promptly initiate remedial measures, so as to ensure continuous firewall availability.

To gather the statistics of interest, the eG agent polls the SNMP-MIB of the firewall. To facilitate this data retrieval, SNMP should be enabled on the FortiGate firewall. In order to enable SNMP on FortiGate firewall, do the following:

1. Follow the menu sequence: System>Config> SNMP v1/v2c on the firewall**.**
2. Select the check box **Enable SNMP** (see Figure 5.1).



Enable SNMP	☑
System Name	Fortigate
System Location	Server Room
Contact Information	Phone: 555-1234
Get Community	our_get_com
Trap Community	our_trap_com
First Trap Receiver IP Address	192.168.100.3
Second Trap Receiver IP Address	192.168.23.7
Third Trap Receiver IP Address	54.67.23.45

Figure 5.1: Enabling SNMP

3. To retrieve information from SNMP MIB, ensure that you specify a **Get Community** string, which is a password to identify SNMP get requests sent to the FortiGate unit. The default get community string is “public”. You can change the default **Get Community** string if need be (see Figure 5.1).
4. In the Figure 5.1, click the **Apply** button to save the details.

Also, before the eG agent connects to the FortiGate agent, an administrator must configure one or more FortiGate interfaces to accept SNMP connections. The configuration depends upon whether the FortiGate unit is operating in NAT/Route mode or Transparent mode.

In order to configure SNMP access to an interface in NAT/Route mode, do the following:

1. Follow the menu sequence: Systems>Network>Interface.
2. Choose an interface that eG agents connect to and select **Modify**.
3. For Administrative Access, select SNMP.
4. Select **OK**.

In order to configure SNMP access to an interface in Transparent mode:

1. Follow the menu sequence: System> Network>Management.
2. Select the interface that the SNMP manager connects to and select SNMP.
3. Select **Apply**.

Having enabled the SNMP agent to extract the performance measures from FortiGate Firewall, you can now proceed to configure the eG agent to pull out statistics from the SNMP MIB. The metrics collected by the agent are then presented in the eG monitor interface using the unique *Fortigate Firewall* or *Fortigate Firewall 3x* layer model (depending upon the version being monitored).

This chapter discusses both these models.

5.1 Monitoring the FortiGate Firewall v3x

Figure 5.2 below depicts the *Fortigate Firewall 3x* monitoring model offered out-of-the-box by the eG Enterprise Suite. As stated earlier, this model focuses on the overall health of the FortiGate Firewall v3 (and its variants).

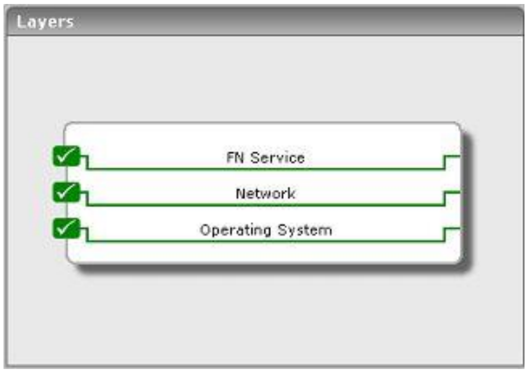


Figure 5.2: Layer model of the FortiGate Firewall

Every layer displayed by Figure 5.2 is mapped to a series of tests, which when executed on the firewall reveals a wealth of performance information pertaining to the firewall. These statistics provide quick and accurate answers to the following frequently asked performance-oriented questions:

- Has the firewall been consuming excessive CPU, meory, and disk resources?
- Are too many sessions currently active on the firewall?
- Is the network and data traffic on the firewall cluster unit very heavy?
- How effective are the anti-virus and IPS mechanisms configured on the firewall cluster unit? Have they been able to detect and prevent all attempted attacks?

The sections that follow discuss in detail the first and the last layer of Figure 5.2, and the tests mapped to these layers. The second layer, which is the **Network** layer, has already been discussed in the previous chapters.

5.1.1 The Operating System Layer

Using the FnSystem test, this layer monitors the CPU, memory, and disk utilization of the FortiGate firewall.

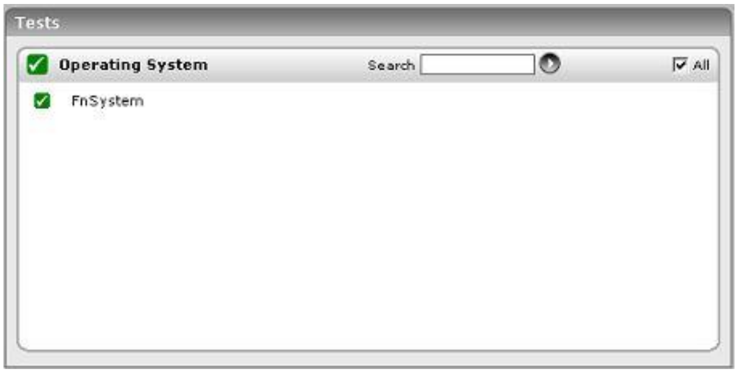


Figure 5.3: The test associated with the FnSystemTest

5.1.1.1 FnSystem Test

The FnSystem test monitors the resource utilization of a FortiGate firewall.

Purpose	Monitors the resource utlilization of a FortiGate Firewall
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

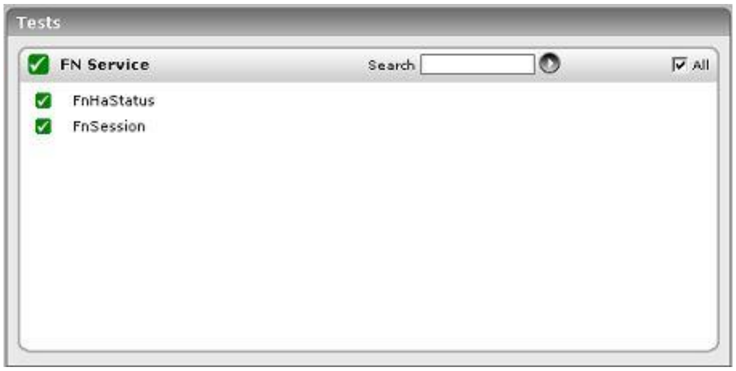
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **SNMPVERSION** – By 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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each firewall monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Fortinet CPU usage: This metric represents the current CPU usage of a FortiGate Firewall.	Percent	A value close to 100% indicates a CPU bottleneck on the firewall.
	Fortinet memory usage: This metric represents the current memory usage of the firewall.	MB	
	Hard disk capacity: This metric denote the hard disk capacity of the firewall.	MB	
	Hard disk usage: This metric denotes the current hard disk usage of the firewall.	MB	
	Percent of hard disk utilized: This value is the ratio of the disk usage of the firewall to the total disk capacity, expressed as a percentage**.**	Percent	A value close to 100% indicates that the hard disk is close to filling up and needs immediate attention.

5.1.2 The FN Service Layer

The tests mapped to this layer (see Figure 5.4), monitor:

- the session activity on the firewall
- the resource utilization, network traffic, session activity, and the extent of protection delivered by the firewall cluster unit



Tests

☑ FN Service

Search

☑ All

☑ FnHaStatus

☑ FnSession

Figure 5.4: The tests associated with the FN Service layer

5.1.2.1 FnSession Test

The FnSession test monitors the session activity to a FortiGate firewall.

Purpose	Monitors the session activity to FortiGate Firewall
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each firewall monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current sessions for Fortinet service: Indicates the number of sessions currently supported by the firewall.	Number	

5.1.2.2 FnHaStatus Test

The FnHaStatus test monitors the various statistics of interest regarding a high availability FortiGate firewall.

Purpose	Monitors the session various statistics of interest regarding a high availability FortiGate firewall.
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each firewall monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Cpu usage of cluster unit: This metric represents the current CPU usage of a unit of the firewall cluster.	Percent	
	Memory usage of cluster unit: This metric represents the current memory usage of the firewall cluster unit.	MB	
	Network usage of cluster unit: This metric indicates the current network utilization of the firewall cluster unit.	KB/Sec	
	Network traffic handled by cluster unit: This metric is the rate of packets processed by the firewall cluster unit during the last measurement period.	Packets/sec	

	Data traffic through cluster unit: This metric is the data traffic handled by the firewall cluster unit during the last measurement period, expressed in KB.	KB	
	Active sessions to cluster unit: This metric is the current active sessions to the firewall cluster unit.	Number	
	Virus attacks detected: This value is the number of attacks that the IPS detected in the last 20 hours.	Number	
	Viruses detected by cluster unit: This value is the number of viruses the antivirus system detected in the last 20 hours.	Number	

5.2 Monitoring the Fortigate Firewall v4 (and above)

Figure 5.2 below depicts the *Fortigate Firewall* monitoring model offered out-of-the-box by the eG Enterprise Suite. As stated earlier, this model focuses on the overall health of the FortiGate Firewall v3 (and its variants).

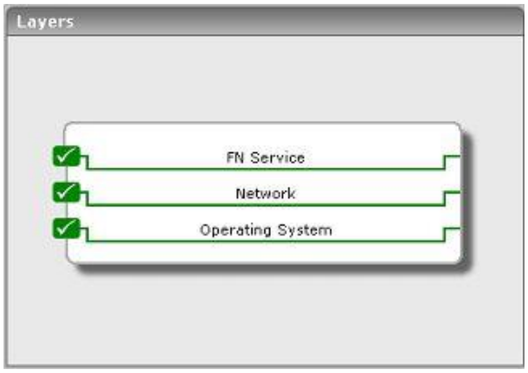


Figure 5.5: Layer model of the FortiGate Firewall

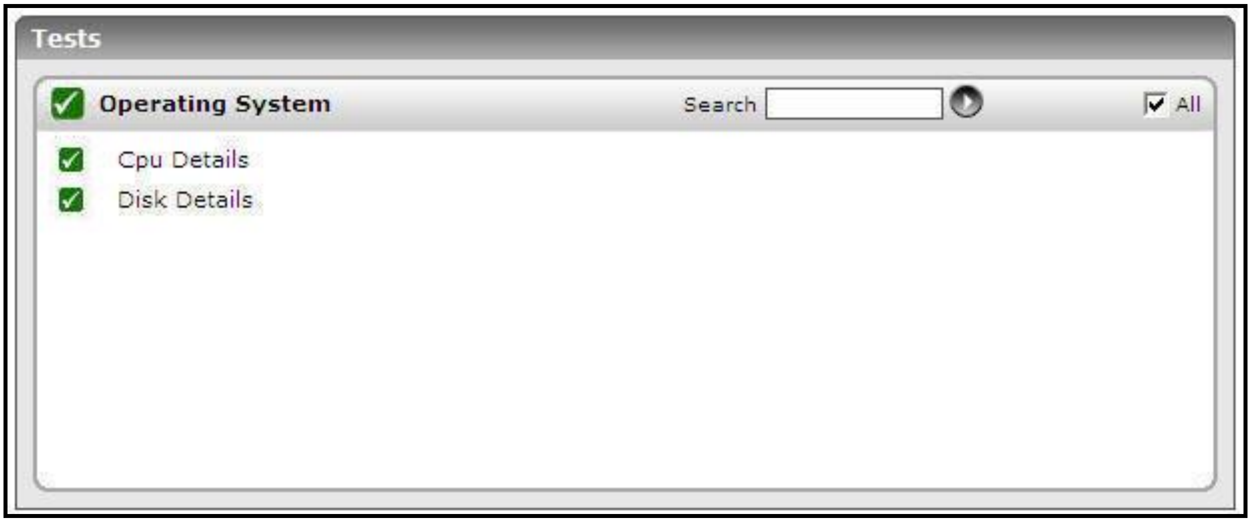
Every layer displayed by Figure 5.2 is mapped to a series of tests, which when executed on the firewall reveals a wealth of performance information pertaining to the firewall. These statistics provide quick and accurate answers to the following frequently asked performance-oriented questions:

- Has the firewall been consuming excessive CPU, memory, and disk resources?
- Are too many sessions currently active on the firewall?
- Is the network and data traffic on the firewall cluster unit very heavy?
- How effective are the anti-virus and IPS mechanisms configured on the firewall cluster unit? Have they been able to detect and prevent all attempted attacks?

The sections that follow discuss in detail the first and the last layer of Figure 5.2, and the tests mapped to these layers. The second layer, which is the **Network** layer, has already been discussed in the previous chapters.

5.2.1 The Operating System Layer

Using the tests mapped to this layer, you can receive a heads-up on potential CPU and/or memory contentions on the firewall.


Tests

☑ Operating System Search ☑ All

☑ Cpu Details

☑ Disk Details

Figure 5.6: The tests mapped to the Operating System layer of the Fortigate Firewall component

5.2.1.1 Disk Details Test

This test monitors the disk space usage of each disk partition supported by the firewall, points you to partitions that are over-utilizing disk space, and thus proactively alerts you to potential space contentions.

Purpose	Monitors the disk space usage of each disk partition supported by the firewall, points you to partitions that are over-utilizing disk space, and thus proactively alerts you to potential space contentions
Target of the test	A FortiGate Firewall

Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each disk partition on the firewall being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total capacity: This metric represents the total capacity of this disk partition.	MB	
	Disk space usage: This metric represents the current usage of space in this disk partition.	MB	A consistent increase in the value of this measure could indicate that the disk space is getting slowly but steadily eroded. Compare the value of this measure across partitions to identify the partitions that are utiilizing disk space excessively.
	Disk space used: Indicates the percentage of space in this disk partition that is currently utilized.	Percent	A consistent increase in the value of this measure could indicate that the disk space is getting slowly but steadily eroded. Compare the value of this measure across partitions to identify the partitions that are utiilizing disk space excessively.
	Free disk space: Indicates the percentage space in this disk partition that is currently free.	Percent	A high value is typically desired for this measure. A very low often is indicative of abnormal space utilization.

5.2.1.2 Cpu Details Test

This test monitors the CPU and memory usage of the firewall and proactively alerts you to potential resource contentions.

Purpose	Monitors the CPU and memory usage of the firewall and proactively alerts you to potential resource contentions
Target of the test	A FortiGate Firewall

Agent deploying the test	An external agent

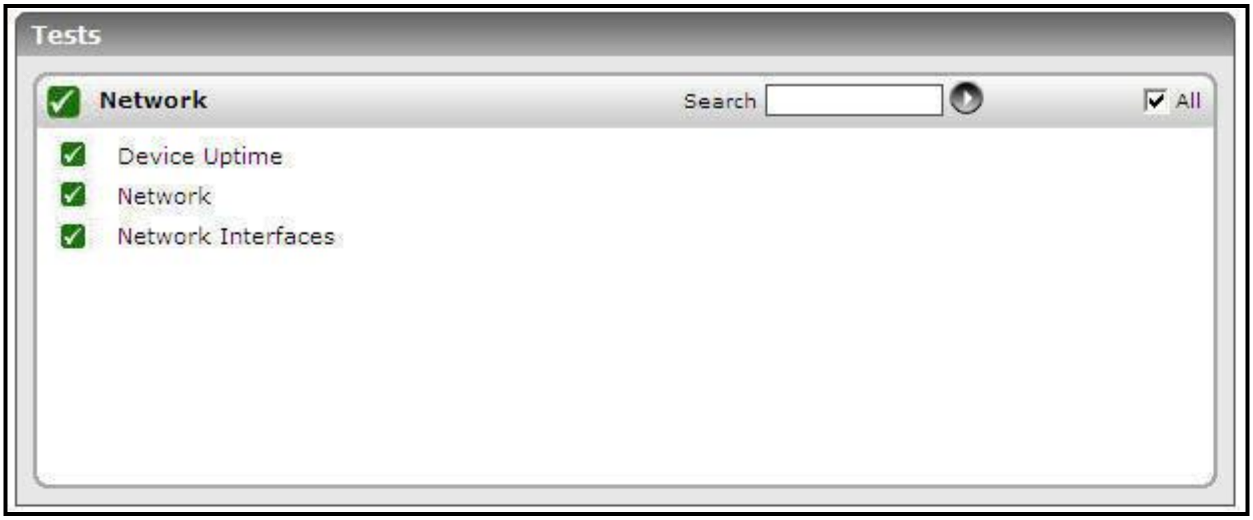
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **SNMPVERSION** – By 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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results the firewall being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	CPU utilization: Indicates the current CPU usage of the firewall.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the CPU usage of the firewall. A consistent increase however could indicate a gradual, yet steady erosion of CPU resources, and is hence a cause for concern.
	Current memory utilization: Indicates the current memory usage of the firewall.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the memory usage of the firewall. A consistent increase however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
	Total memory: Indicates the current memory capacity of the firewall.	KB	

5.2.2 The Network Layer

The tests mapped to this layer reveal the following anomalies:

- Unscheduled reboots of the firewall
- Non-availability of the firewall over the network
- Latencies when connecting to the firewall over the network
- Abnormal speed of and unusual bandwidth usage by the network interfaces supported by the firewall



Tests

☑ Network Search ☑ All

- ☑ Device Uptime
- ☑ Network
- ☑ Network Interfaces

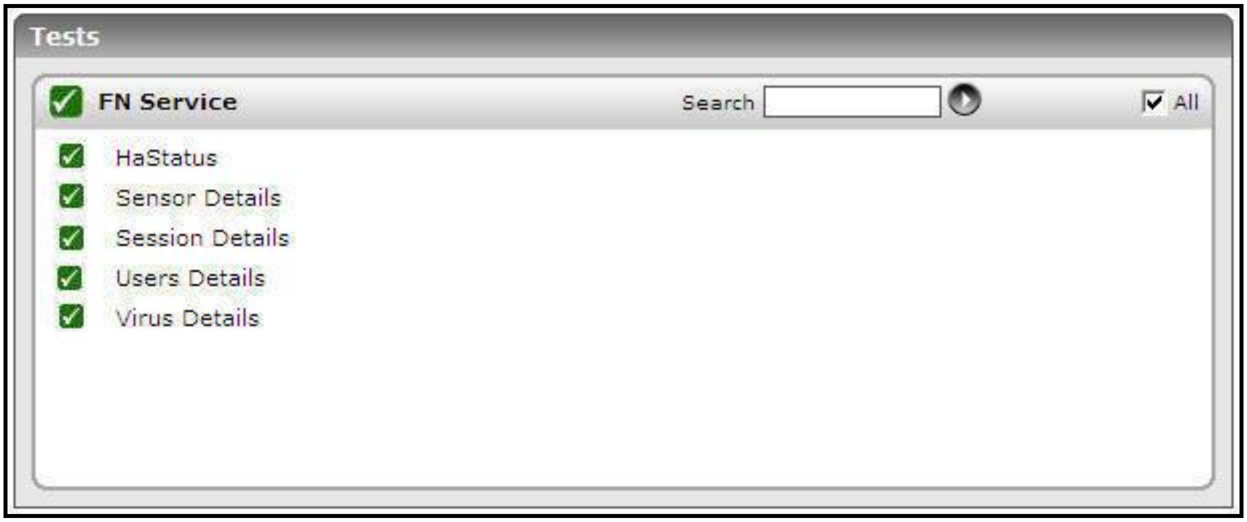
Figure 5.7: The tests mapped to the Network layer of the Fortigate Firewall component

Since the tests depicted by Figure 5.7 have already been dealt with in great detail in the previous chapters, let us proceed to look at the next layer.

5.2.3 The FN Service Layer

The tests mapped to this layer monitor the following:

- The resource usage of, the network traffic handled by, and the session load on each Fortigate unit in an High Availability Fortigate cluster;
- The current state of user accounts on the firewall;
- The current state of the sensors on the firewall;
- The count of viruses detected and blocked by the firewall



Tests

☑ FN Service Search ☑ All

- ☑ HaStatus
- ☑ Sensor Details
- ☑ Session Details
- ☑ Users Details
- ☑ Virus Details

Figure 5.8: The tests mapped to the FN Service layer

5.2.3.1 HaStatus Test

FortiGate high availability (HA) provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance. FortiGate HA consists of two or more FortiGate units operating as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewall, VPN, IPS, virus scanning, web filtering, and spam filtering services.

Inside the cluster the individual FortiGate units are called cluster units. These cluster units share state and configuration information. If one cluster unit fails, the other units in the cluster automatically replace that unit, taking over the work that the failed unit was doing. The cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption. The ability of an HA cluster to continue providing firewall services after a failure, is called failover.

A second HA feature, called load balancing, can be used to increase firewall performance. A cluster of FortiGate units can increase overall network performance by sharing the load of processing network traffic and providing security services. Periodically, you may want to check the network traffic processed by each cluster unit, so as to assess the efficiency with which the HA cluster balances load, isolate overloaded units, and thereby spot load balancing irregularities (if any) early. The **HaStatus** test enables you to achieve this end. This test monitors each Fortigate unit in an HA cluster, reports the resource usage of each unit, and also tracks the network traffic processed by every unit, so that resource-hungry and overloaded units can be quickly identified.

Purpose	Monitors each Fortigate unit in an HA cluster, reports the resource usage of each unit, and also tracks the network traffic processed by every unit, so that resource-hungry and overloaded units can be quickly identified
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each cluster unit monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Cpu usage: This metric represents the current CPU usage of this unit of the firewall cluster.	Percent	A value close to 100% indicates a CPU bottleneck on a cluster unit. Compare the value of this measure across cluster units to identify the CPU-hungry unit.
	Memory usage: This metric represents the current memory usage of this firewall cluster unit.	MB	A consistent increase in the value of this measure could indicate that a cluster unit is experiencing a memory drain. Compare the value of this measure across cluster units to identify the memory-hungry unit.
	Network usage: This metric indicates the current network utilization of this firewall cluster unit.	KB/Sec	By comparing the value of this measure across cluster units you can accurately isolate overloaded units, and in the process proactively detect load-balancing irregularities in the cluster.
	Network traffic: This metric is the rate of packets processed by the firewall cluster unit during the last measurement period.	Packets/sec	
	Data traffic: This metric is the data traffic handled by the firewall cluster unit during the last measurement period, expressed in KB.	KB	

	Sessions: This metric is the current active sessions to the firewall cluster unit.	Number	A high value of this measure could indicate a session overload on a cluster unit.
	Virus detected: This value is the number of viruses the antivirus system detected in the last measurement period.	Number	
	Ids events detected: This value is the number of attacks that the IDS/IPS detected during the last measurement period	Number	An IPS is an Intrusion Prevention System for networks. While early systems focused on intrusion detection, the continuing rapid growth of the Internet, and the potential for the theft of sensitive data, has resulted in the need for not only detection, but prevention. The FortiGate IPS detects intrusions by using attack signatures for known intrusion methods, and detects anomalies in network traffic to identify new or unknown intrusions. Not only can the IPS detect and log attacks, but users can choose actions to take on the session when an attack is detected. Using sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets.

5.2.3.2 Session Details Test

By reporting the number of sessions that are active on the firewall, this test provides us with pointers to the current session load handled by the firewall.

Purpose	Reports the number of sessions that are active on the firewall
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results the firewall being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Sessions: Indicates the number of sessions that are currently active on the firewall.	Number	A high value of this measure could indicate a session overload on the firewall.

5.2.3.3 Users Details Test

A user is a user account that consists of a user name, password and in some cases, other information that can be configured on the unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

When configuring a user account on the firewall, you can indicate whether the user is to be allowed to authenticate (i.e., enabled) or blocked from authenticating (i.e., disabled). This test auto-discovers the user accounts configured on the firewall, and reports which user accounts are allowed to authenticate and which are not.

Purpose	Auto-discovers the user accounts configured on the firewall, and reports which user accounts are allowed to authenticate and which are not
Target of the test	A FortiGate Firewall
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">15. <b>TIMEOUT</b> - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
16. <b>DATA OVER TCP –</b> 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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each user account configured on the firewall being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status of user account:</b>
Indicates the current authentication status of this user account.</td><td></td><td>If this measure reports the value <i>Enabled</i>, it indicates that the user account is allowed to authenticate. The value <i>Disabled</i> for a user account indicates that the user account is not allowed to authenticate.
The numeric values that correspond to the measure values discussed above have been listed 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>
Typically, this measure will report one of the <b>Measure Value</b>s listed in the table above to indicate the authentication status of a user account. However, in the graph of this measure, the authentication status will be depicted using the corresponding numeric equivalents only.</td></tr>
</table>

5.2.3.4 Sensor Details Test

This test reports the current state of each sensor on the Fortigate firewall.

Purpose	Reports the current state of each sensor on the Fortigate firewall
Target of the test	A FortiGate Firewall
Agent	An external agent

deploying the test	
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">15. <b>TIMEOUT</b> - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
16. <b>DATA OVER TCP –</b> 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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each sensor on the firewall being monitored</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Sensor status:</b>
Indicates the current status of this sensor.</td><td></td><td>If this measure reports the value <i>Enabled</i>, it indicates that the sensor is allowed to enabled. The value <i>Disabled</i> for a sensor indicates that the sensor is disabled.
The numeric values that correspond to the measure values discussed above have been listed 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>
Typically, this measure will report one of the <b>Measure Value</b>s listed in the table above to indicate the current sensor state. However, in the graph of this measure, the sensor state will be depicted using the corresponding numeric equivalents only.</td></tr>
</table>

5.2.3.5 Virus Details Test

The true test of the effectiveness of a firewall lies in its ability to detect and protect the system from malicious virus attacks. Using the metrics reported by the **Virus Details** test, you can assess the efficiency of the Fortigate firewall, as it reports the number of viruses detected and blocked by the firewall per protocol it supports.

Purpose	Helps assess the efficiency of the Fortigate firewall by reporting the number of viruses detected by the firewall per protocol it supports
Target of the test	A FortiGate Firewall
Agent	An external agent

deploying the test	
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the FortiGate firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the FortiGate firewall 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the firewall being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	HTTP Virus Detected: Indicates the number of virus transmissions over HTTP detected in the virtual domain in the last measurement period.	Number	
	HTTP Virus Blocked: Indicates the number of virus transmissions over HTTP blocked in the virtual domain in the last measurement period.	Number	
	SMTP Virus Detected: Indicates the number of virus transmissions over SMTP detected in the virtual domain in the last measurement period.	Number	
	SMTP Virus Blocked: Indicates the number of virus transmissions over SMTP detected in the virtual domain in the last measurement period.	Number	
	POP3 Virus Detected: Indicates the number of virus transmissions over POP3 detected in the virtual domain in the last measurement period.	Number	

	POP3 Virus Blocked: Indicates the number of virus transmissions over POP3 blocked in the virtual domain in the last measurement period.	Number	
	IMAP Virus Detected: Indicates the number of virus transmissions over IMAP detected in the virtual domain in the last measurement period.	Number	
	IMAP Virus Blocked: Indicates the number of virus transmissions over IMAP blocked in the virtual domain in the last measurement protocol.	Number	
	FTP Virus Detected: Indicates the number of virus transmissions over FTP detected in the virtual domain in the last measurement period.	Number	
	FTP Virus Blocked: Indicates the number of virus transmissions over FTP blocked in the virtual domain in the last measurement period.	Number	
	IM Virus Detected: Indicates the number of virus transmissions over IM protocols detected in the virtual domain in the last measurement period.	Number	
	IM Virus Blocked: Indicates the number of virus transmissions over IM protocols blocked in the virtual domain in the last measurement period.	Number	

	NNTP Virus Detected: Indicates the number of virus transmissions over NNTP detected in the virtual domain in the last measurement period.	Number	
	NNTP Virus Blocked: Indicates the number of virus transmissions over NNTP blocked in the virtual domain in the last measurement period.	Number	
	Total Virus Detected: Indicates the total number of virus transmissions detected in the virtual domain in the last measurement period.	Number	
	Total Virus Blocked: Indicates the total number of virus transmissions blocked in the virtual domain in the last measurement period.	Number	

Chapter

6

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **firewalls**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.