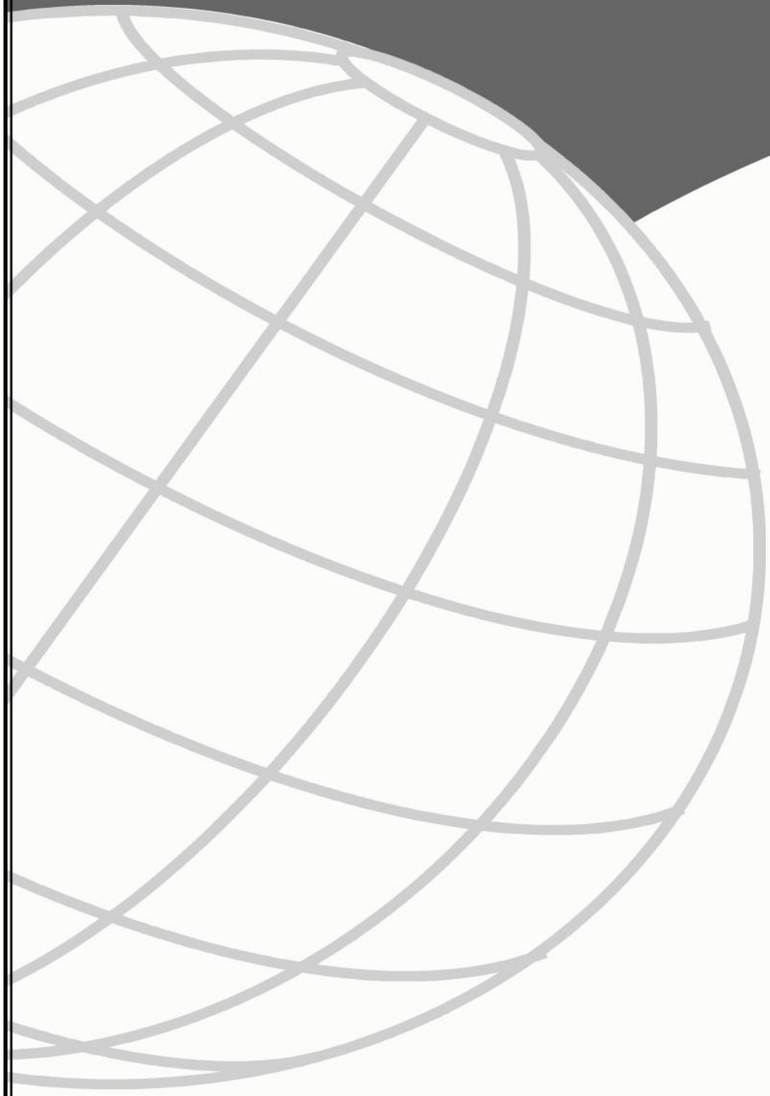


Enabling Service Excellence

Monitoring Sonic Firewall

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

MONITORING SONIC FIREWALL **1**

1.1 The Firewall Service Layer 1

1.1.1 SFW Connections Test 2

1.1.2 SFW VPN Details Test 4

1.2 The Operating System Layer 8

1.2.1 SFW CPU usage Test 8

1.2.2 SFW Memory Usage Test 10

CONCLUSION **13**

Table of Figures

Figure 1: The layer model of the Sonic Firewall 1
Figure 2: The tests mapped to the Firewall Service layer 2
Figure 2: The tests mapped to the Operating System layer 8

1

Monitoring Sonic Firewall

Sonic Firewall is the most secure Unified Threat Management (UTM) firewall for small businesses, retail deployments, government organizations, remote sites and branch offices. The Sonic Firewall delivers enterprise-class, high speed threat protection, reliable communications and flexible connectivity.

Uninterrupted firewall operations are imperative to keep hackers and harmful viruses at bay. Any issue in the configuration, state, or resource usage of the firewall can bring its operations to a halt, leaving your network and all mission-critical applications operating within defenceless against malicious viruses and unscrupulous users! It is hence important that the performance of the firewall is monitored 24x7.

eG Enterprise provides a specialized *Sonic Firewall* monitoring model (see Figure 1), which periodically polls the SNMP MIB of the firewall to measure the availability, responsiveness, resource usage, and VPN tunnel traffic of the firewall, and notifies administrators of potential resource crunches or configuration issues with the firewall.

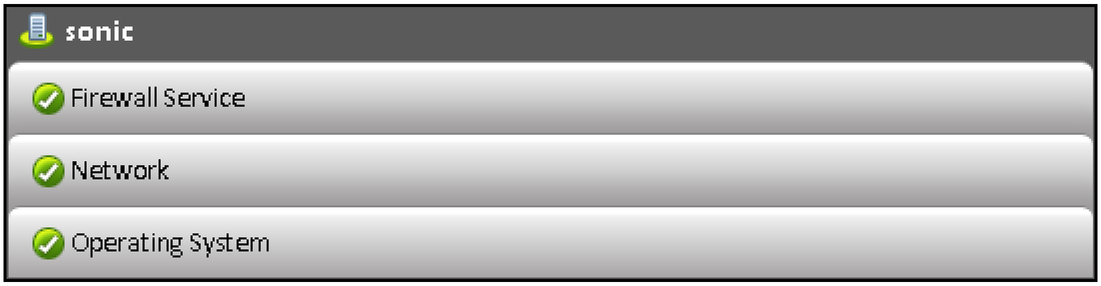


Figure 1: The layer model of the Sonic Firewall

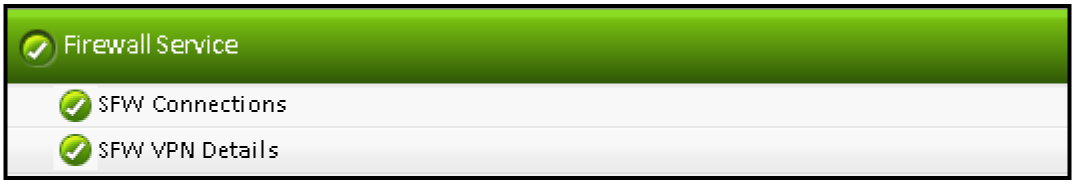
Using the metrics reported , administrators can find quick and accurate answers for the following performance questions:

- Is the firewall available over the network? How is the network connectivity to the firewall – solid or flaky?
- Is there a resource contention on the firewall device? Which resource is bottlenecked – CPU or memory?
- How many connections can the firewall service? Is the number of connections currently handled by the firewall unusually high?
- Is any VPN tunnel hogging the bandwidth resources? If so, which one is it?
- Are too many fragmented packets flowing through the firewall? If so, why? Is it because of an incorrect configuration?

The **Network** layer of the *Sonic Firewall* model is similar to that of a *Windows Generic* server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, Section 1.1 focuses on the **Firewall Service** layer.

1.1 The Firewall Service Layer

This layer tracks the simultaneous connections of the firewall and the numerical statistics of each VPN tunnel such as the number of fragmented packets that were transmitted/received; the number of data packets that were encrypted/decrypted etc.



Firewall Service

SFW Connections

SFW VPN Details

Figure 2: The tests mapped to the Firewall Service layer

1.1.1 SFW Connections Test

The Sonic firewall is typically pre-configured with the maximum number of connections it can handle – a limit that is pre-set based on the size of the network the firewall is designed to support. If the number of connections flowing through the firewall suddenly grows close to this limit, it could signal a problem condition that may require the immediate attention of the administrator! Such problems may be anything from an excessive spam to a mail server or a malicious virus attack on any application inside the network! To help administrators quickly capture such anomalous conditions and promptly investigate their reasons, the eG agent periodically runs the **SFW Connections** test. This test not only reports the maximum connection configuration of the firewall, but also continuously tracks the connections currently flowing through the firewall, so that administrators can rapidly detect an abnormal increase in the number of connections and determine what is causing it. This way, administrators can be proactively alerted to probable virus attacks/spams and initiate measures to protect their network from harm!

Purpose	Not only reports the maximum connection configuration of the firewall, but also continuously tracks the connections currently flowing through the firewall, so that administrators can rapidly detect an abnormal increase in the number of connections and determine what is causing it
Target of the test	A Sonic Firewall device
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 Sonic firewall 3. **PORT** – The port at which the specified host listens 4. **SNMPPORT** – The SNMP Port number of the Sonic 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 Sonic firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. 17. **ISPASSIVE** – If the value chosen is **Yes**, then the Sonic Firewall under consideration is a passive device in a firewall cluster. No alerts will be generated if the firewall is not running. Measures will be reported as "Not applicable' by the agent if the firewall is not up.		
II Outputs of the test	One set of results for the Sonic Firewall device that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Max connections: Indicates the maximum number of simultaneous connections that can be handled by this firewall.	Number	The value of this measure varies according to the model of the firewall device.
	Active connections: Indicates the number of connections that are currently active or open on this firewall.	Number	An abnormally high value for this measure could indicate a probable virus attack or spam to a mail server in the network.

1.1.2 SFW VPN Details Test

Virtual private network technology is based on the idea of tunneling. A Tunnel is nothing but a logical network connection in the internet cloud through which the send and receive data requests travel. When you initiate communication or send data over VPN network, the Tunneling protocol(s) used by the VPN network (like PPTP, L2TP, IPSec etc.) wraps up the data packets into another data packet and encrypts the package that is to be sent through the tunnel. At receiver's end, the tunneling device/protocol deciphers the package and then strips the wrapped data packet to read and access the original message and reveal the source of packet and other classified information.

Using the Sonic firewall, administrators can configure multiple VPN tunnels based on the volume of data traffic handled by their network and the security/privacy requirements of the network. Access policies and QoS rules can be configured for VPN tunnels, and bandwidth management can be enabled on these configurations to prevent unauthorized access to the network and to optimize the usage of network resources. Improper firewall configurations can therefore result in a few VPN tunnels hogging the bandwidth resources and choking the network! To avoid this, administrators should periodically check the efficacy of the firewall configuration, spot holes in the settings, and plug the holes! This is where the **SFW VPN Details** test helps! This test auto discovers the VPN tunnels configured using the Sonic firewall and closely monitors the amount of data and packets sent and received via every tunnel. In the process, the test accurately points to that tunnel that is handling an abnormally high volume of traffic and is hence hogging the bandwidth resources available to the network! This way, the test enables administrators to understand whether/not their firewall configurations are effective, and if not, initiate measures to fine-tune them.

Purpose	Auto discovers the VPN tunnels configured using the Sonic firewall and closely monitors the amount of data and packets sent and received via every tunnel. In the process, the test

	accurately points to that tunnel that is handling an abnormally high volume of traffic and is hence hogging the bandwidth resources available to the network
Target of the test	A Sonic Firewall device
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 Sonic firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Sonic 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 Sonic firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. 17. **ISPASSIVE** – If the value chosen is **Yes**, then the Sonic Firewall under consideration is a passive device in a firewall cluster. No alerts will be generated if the firewall is not running. Measures will be reported as “Not applicable' by the agent if the firewall is not up.		
Outputs of the test	One set of results for each VPN tunnel that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Fragmented received packets: Indicates the number of fragmented packets that are received through this VPN tunnel.	Number	
	Fragmented transmitted packets: Indicates the number of fragmented packets that are transmitted through this VPN tunnel.	Number	Comparing the value of this measure across the VPN tunnels helps you in identifying the VPN tunnel that is transmitting the highest number of fragmented packets. A very high value for this measure could imply that the MTU (Maximum Transmission Unit) set for the WAN interface is very low, causing many packets to be unnecessarily fragmented. To reduce the load on the network link, you may want to consider resetting the MTU.
	Encrypted data: Indicates the total amount of data that was encrypted by this VPN tunnel.	KB	Comparing the values of these measures across the VPN tunnels helps you in identifying the VPN tunnel that has encrypted/decrypted the maximum amount of data – i.e., the VPN tunnel that has consumed the maximum bandwidth over the network link. If the gap between the top and the least bandwidth consumers is very wide, it could indicate that one/more tunnels are hogging the bandwidth resources. You may then have to consider enabling bandwidth management on these VPN tunnels, reconfigure access policies, or fine-tune QoS settings, so as to minimize bandwidth usage.
	Decrypted data: Indicates the total amount of data that was decrypted by this VPN tunnel.	KB	

	Encrypted packets: Indicates the number of packets that were encrypted on this tunnel.	Number	Comparing the values of these measures across the VPN tunnels helps you in identifying the VPN tunnel that has encrypted/decrypted the maximum number of packets – i.e., the VPN tunnel that has consumed the maximum bandwidth over the network link. If the gap between the top and the least bandwidth consumers is very wide, it could indicate that one/more tunnels are hogging the bandwidth resources. You may then have to consider enabling bandwidth management on these VPN tunnels, reconfigure access policies, or fine-tune QoS settings, so as to minimize bandwidth usage.
	Decrypted packets: Indicates the number of packets that were decrypted by this tunnel.	Number	

1.2 The Operating System Layer

This layer tracks the CPU and memory utilization of the Sonic Firewall device.

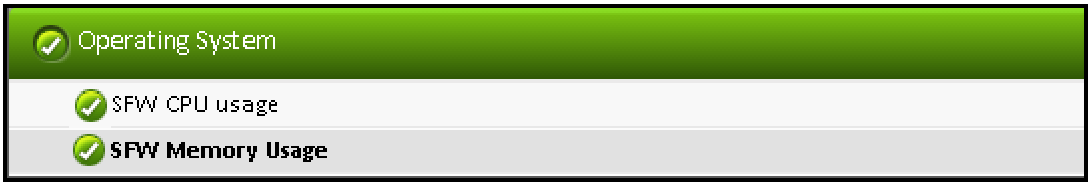


Figure 3: The tests mapped to the Operating System layer

1.2.1 SFW CPU usage Test

This test monitors the current CPU utilization of the firewall and reports whether/not the firewall is consuming too much CPU resources.

Purpose	Monitors the current CPU utilization of this firewall
Target of the test	A Sonic Firewall device
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 Sonic 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 Sonic firewall 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>.
17. <b>ISPASSIVE</b> – If the value chosen is <b>Yes</b>, then the Sonic Firewall under consideration is a passive device in a firewall cluster. No alerts will be generated if the firewall is not running. Measures will be reported as “Not applicable’ by the agent if the firewall is not up.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the Sonic Firewall device that is to be 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>Cpu utilization:</b>
Indicates the current CPU utilization of this firewall.</td><td>Percent</td><td>A value close to 100% is a cause of concern.</td></tr>
</table>

1.2.2 SFW Memory Usage Test

This test monitors the current memory utilization of the firewall and promptly alerts administrators to a potential memory contention on the firewall.

Purpose	Monitors the current memory utilization of this firewall device
Target of the test	A Sonic Firewall device
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 Sonic firewall 3. **PORT** – The port at which the specified **HOST** listens 4. **SNMPPORT** – The SNMP Port number of the Sonic 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 Sonic firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. 17. **ISPASSIVE** – If the value chosen is **Yes**, then the Sonic Firewall under consideration is a passive device in a firewall cluster. No alerts will be generated if the firewall is not running. Measures will be reported as "Not applicable' by the agent if the firewall is not up.		
Outputs of the test	One set of results for the Sonic Firewall device that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Memory utilization: Indicates the current memory utilization of this firewall device.	Percent	A value close to 100% could indicate a probable memory bottleneck.

2

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 the **Sonic Firewall**. 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.