Monitoring SonicWall Firewall

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

SonicWall Firewall is the most secure Unified Threat Management (UTM) firewall for small businesses, retail deployments, government organizations, remote sites and branch offices. The SonicWall 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. This is exactly eG Enterprise offers.

Chapter 2: How to Monitor SonicWall Firewall Using eG Enterprise?

eG Enterprise is capable of monitoring the SonicWall Firewall in an agentless manner. The eG external agent periodically polls the SNMP-MIB of the SonicWall Firewall and fetches the metrics pertaining to the performance of the SonicWall Firewall.

2.1 Managing the SonicWall Firewall

The eG Enterprise cannot automatically discover the SonicWall Firewall so that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a SonicWall Firewall component, do the following:

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

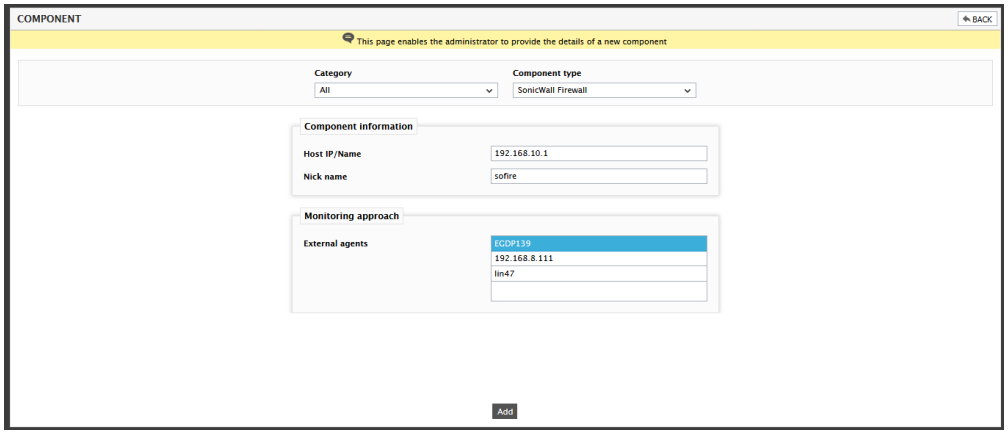

Figure 2.1: Adding a SonicWall Firewall component

4. Specify the **Host IP** and the **Nick name** of the SonicWall Firewall in Figure 2.1. Then, click the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

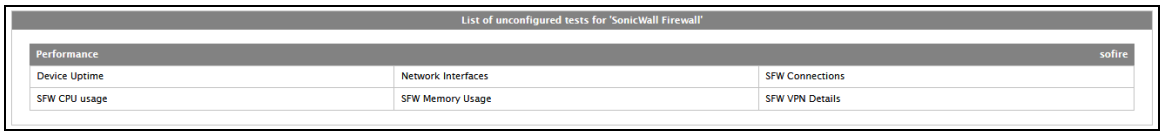

Figure 2.2: List of Unconfigured tests to be configured for the SonicWall Firewall

5. Click on any test in the list of unconfigured tests. For instance, click on the **SFW Connections** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

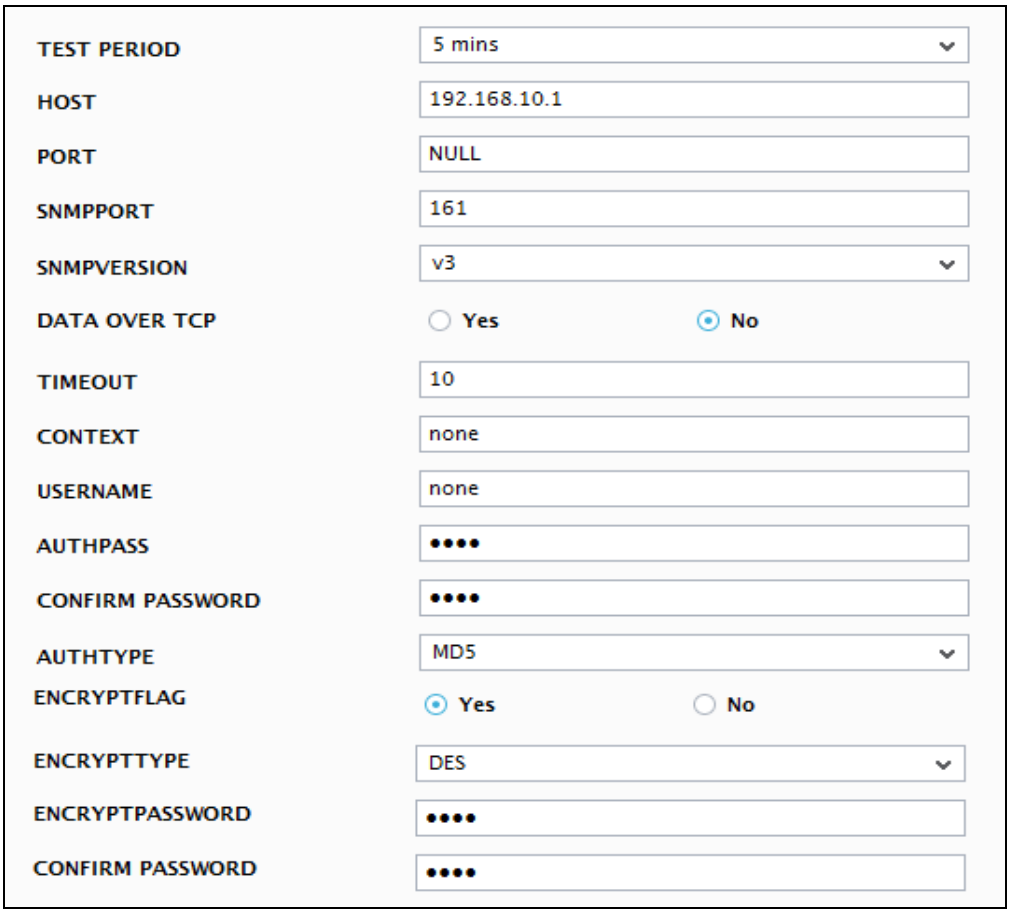

Figure 2.3: Configuring the SFW Connections test

6. To know how to configure parameters, refer to **Monitoring SonicWall Firewall**.
7. Finally signout of the eG administrative interface.

Chapter 3: Monitoring SonicWall Firewall

eG Enterprise provides a specialized SonicWall Firewall monitoring model (see Figure 4.1), 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.

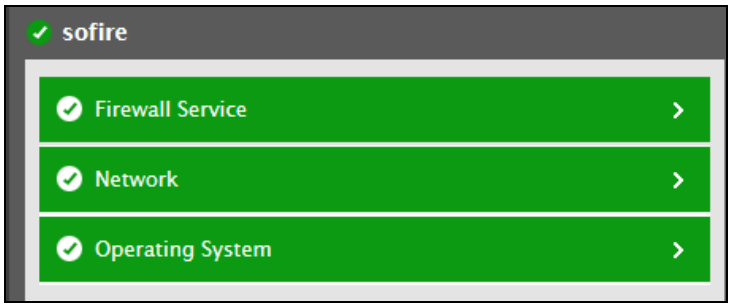

Figure 3.1: The layer model of the SonicWall Firewall

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 SonicWall Firewall model is similar to that of a *Windows Generic server model*. Therefore, you can refer to the *Monitoring Unix and Windows Servers* document in which the tests mapped to the **Network** layer have been discussed briefly. The upcoming section will focuses only on the **Firewall Service** layer.

3.1 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.

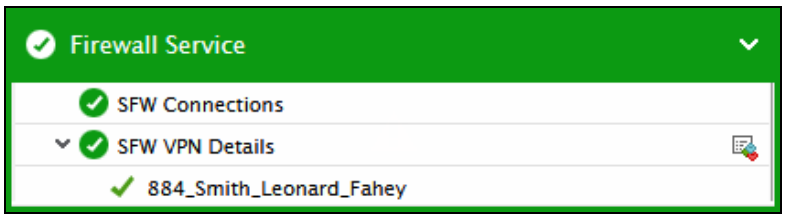

Figure 3.2: The tests mapped to the Firewall Service layer

3.1.1 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!

Target of the test : A SonicWall Firewall device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the SonicWall Firewall device that is to be monitored.

Configurable parameters for the test

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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.

3.1.2 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.

Target of the test : A SonicWall Firewall device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Sonic firewall for which this test is to be configured.
Port	Refers to the port at which the Sonic firewall listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			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

Measurement	Description	Measurement Unit	Interpretation
Decrypted packets	Indicates the number of packets that were decrypted by this tunnel.	Number	these VPN tunnels, reconfigure access policies, or fine-tune QoS settings, so as to minimize bandwidth usage.

3.2 The Operating System Layer

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

Figure 3.3: The tests mapped to the Operating System layer

3.2.1 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.

Target of the test : A SonicWall Firewall device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the SonicWall Firewall device that is to be monitored.

Configurable parameters for the test

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Cpu utilization	Indicates the current CPU utilization of this firewall.	Percent	A value close to 100% is a cause of concern.

3.2.2 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.

Target of the test : A SonicWall Firewall device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the SonicWall Firewall device that is to be monitored.

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Memory utilization	Indicates the current memory utilization of this firewall device.	Percent	A value close to 100% could indicate a probable memory bottleneck.

About eG Innovations

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

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

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

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