Monitoring WatchGuard Firewall

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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 where eG Enterprise helps administrators.

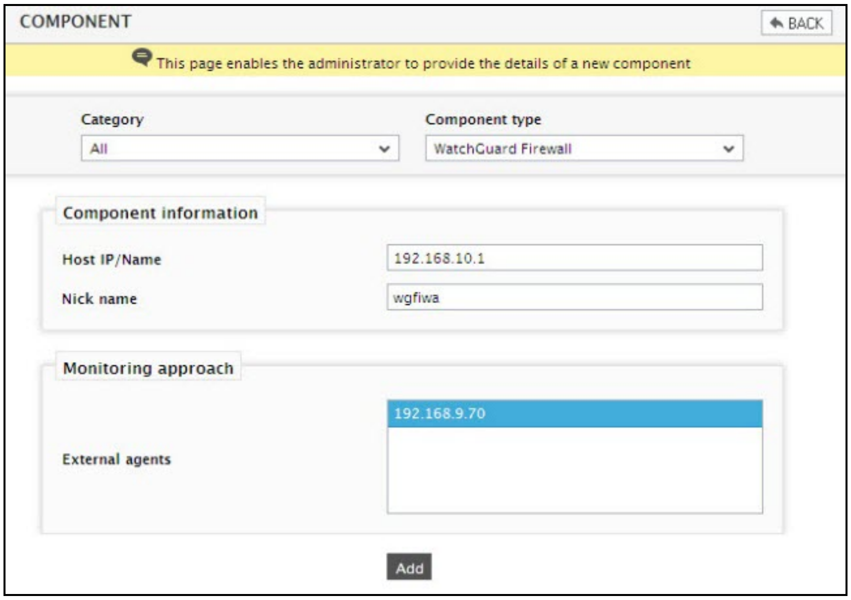
Chapter 2: How to Monitor WatchGuard Firewall Using the eG Enterprise?

eG Enterprise monitors the WatchGuard Firewall in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of monitoring the performance of the firewall by periodically polling the SNMP MIB of the firewall.

2.1 Managing the WatchGuard Firewall

The eG Enterprise cannot automatically discover the WatchGuard Firewall. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a WatchGuard 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 WatchGuard Firewall as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: WatchGuard Firewall

Component information

Host IP/Name: 192.168.10.1

Nick name: wgfiwa

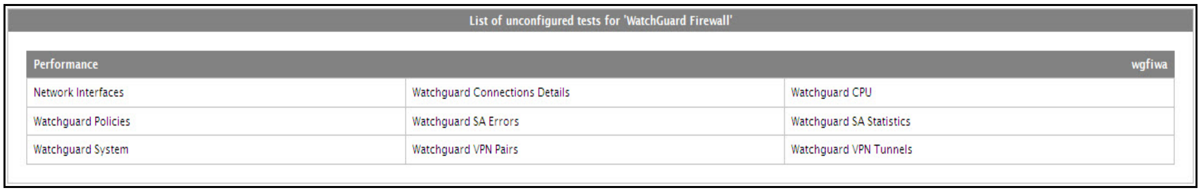
Monitoring approach

External agents: 192.168.9.70

Figure 2.1: Adding a WatchGuard Firewall server

4. Specify the **Host IP** and the **Nick name** of the WatchGuard Firewall component 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.

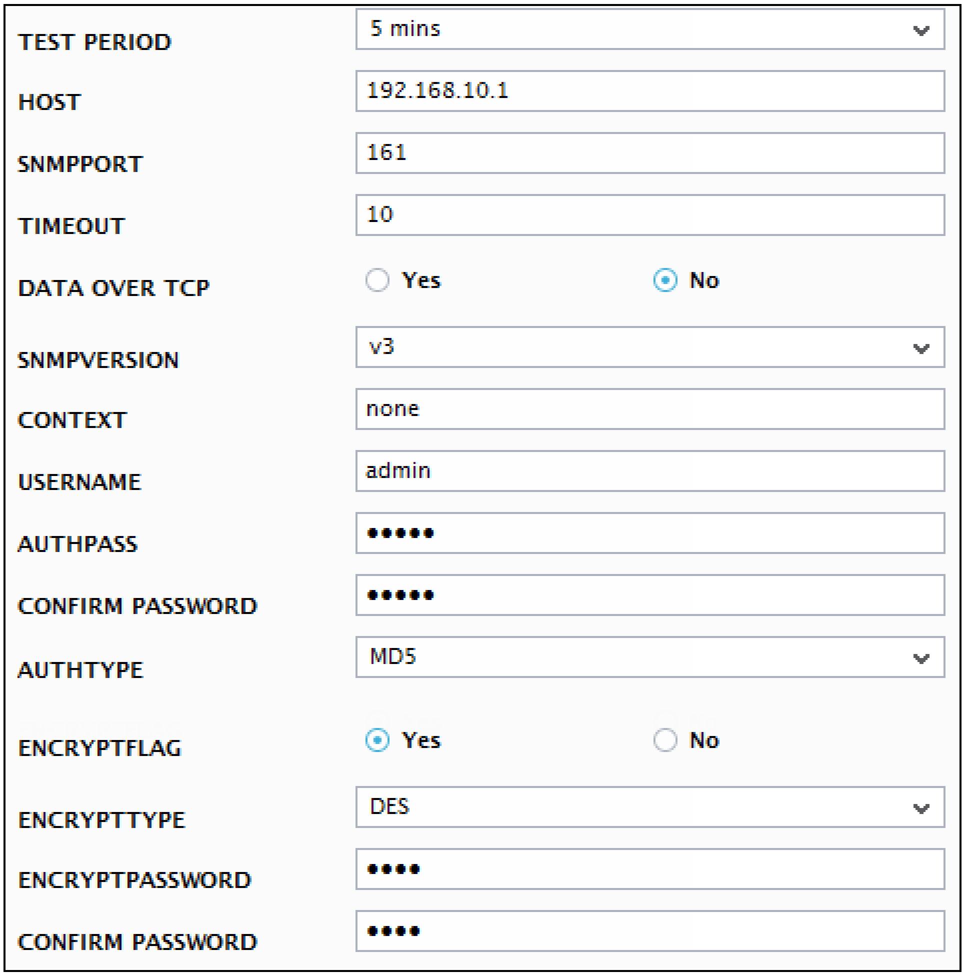


List of unconfigured tests for 'WatchGuard Firewall'

Performance		wgfiwa
Network Interfaces	Watchguard Connections Details	Watchguard CPU
Watchguard Policies	Watchguard SA Errors	Watchguard SA Statistics
Watchguard System	Watchguard VPN Pairs	Watchguard VPN Tunnels

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

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



TEST PERIOD	5 mins	
HOST	192.168.10.1	
SNMPPORT	161	
TIMEOUT	10	
DATA OVER TCP	○ Yes	● No
SNMPVERSION	v3	
CONTEXT	none	
USERNAME	admin	
AUTHPASS	•••••	
CONFIRM PASSWORD	•••••	
AUTHTYPE	MD5	
ENCRYPTFLAG	● Yes	○ No
ENCRYPTTYPE	DES	
ENCRYPTPASSWORD	••••	
CONFIRM PASSWORD	••••	

Figure 2.3: Configuring the WatchGuard Connections Details test

7. To know how to configure these parameters, refer to **Monitoring the WatchGuard Firewall** .

8. Next, try to signout of the eG administrative interface, now you will be prompted to configure the **Network Interfaces** test. To know how to configure the **Network Interfaces** test, refer to *Monitoring Cisco Router* document.

9. Finally signout of the eG administrative interface.

Chapter 3: Monitoring the WatchGuard Firewall

eG Enterprise provides a specialized WatchGuard Firewall monitoring model (see Figure 3.1), which periodically polls the SNMP MIBs of the firewall to measure the connections, responsiveness, resource usage, and VPN tunnel traffic of the firewall, and notifies administrators of potential resource crunches or configuration issues with the firewall.

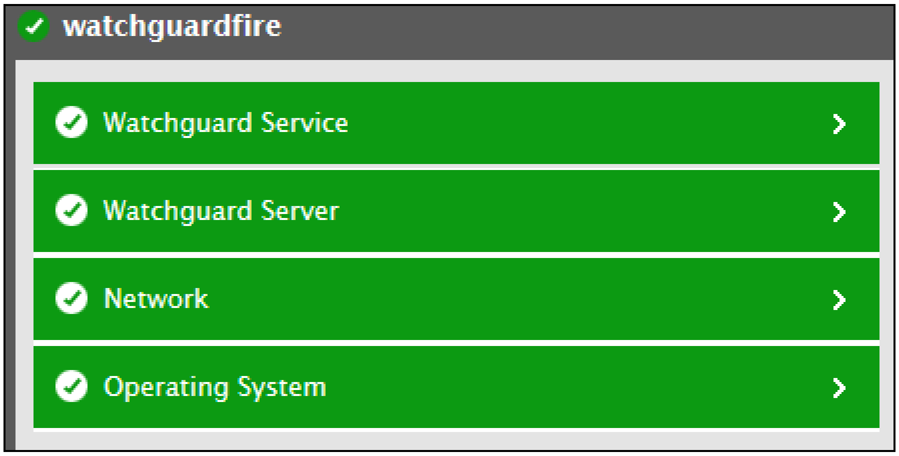


Figure 3.1: The layer model of the WatchGuard Firewall

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

- What is the current CPU utilization of the firewall?
- How many connections are active on the firewall? Are the connection dropped frequently? If so, how many connections are dropped?
- How well the data and packets are transmitted through the firewall?
- How well the data and packets are transmitted for each firewall policy? How many different error prone packets are discarded for each firewall policy?
- How well the data is transmitted through each VPN pair and VPN tunnel? How many different error prone packets were discarded?
- How well data is transmitted through each protocol for a security association and how many different error prone packets were discarded?

The **Network** layer of the **WatchGuard 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, this document focuses on all the other layers.

3.1 The Operating System Layer

This layer tracks the current CPU utilization of the firewall and reports administrators of any abnormalities detected in the utilization of the CPU.

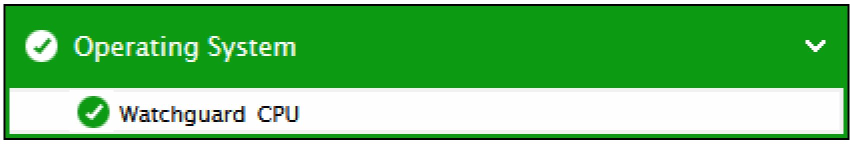


Figure 3.2: The tests mapped to the Operating System layer

3.1.1 Watchguard CPU Test

This test monitors the current CPU utilization of the firewall. If the device is found to consume CPU resources excessively, then, this test will also help administrators determine when exactly during the last 5 minutes did CPU utilization peak; this revelation will help them troubleshoot CPU spikes better.

Target of the test : A WatchGuard Firewall server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the WatchGuard 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 WatchGuard Firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this

Parameter	Description
	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 default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.

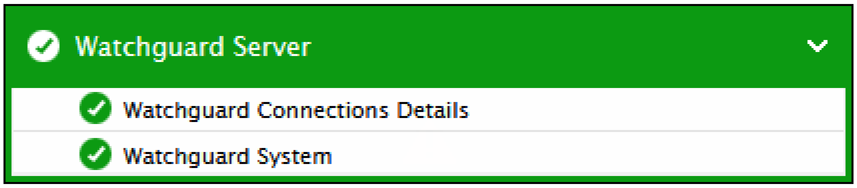
Parameter	Description
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	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 - 1 min	Indicates the percentage of CPU utilized by this firewall during the last 1 minute.	Percent	A value close to 100% is a cause of concern which requires further investigation. Comparing the value of this measure with that of CPU utilization – 5 mins measure will help you identify the abnormalities in the CPU utilization, if any.
CPU utilization - 5mins	Indicates the percentage of CPU utilized by this firewall during the last 5 minutes.	Percent	A value close to 100% is a cause of concern.

3.2 The Watchguard Server Layer

This layer tracks the simulataneous connections of the firewall and the amount of data/packets transmitted through the firewall. Figure 3.3 lists the tests that are currently mapped to the WatchguardServer layer.



✓ Watchguard Server

✓ Watchguard Connections Details

✓ Watchguard System

Figure 3.3: The tests mapped to the WatchGuard Server layer

3.2.1 Watchguard Connections Details Test

In computing, a stateful firewall (any firewall that performs stateful packet inspection (SPI) or stateful inspection) keeps track of the state of network connections (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. The firewall will allow packets matching a known active connection only and all other connections will either be dropped or rejected. Connections may also be dropped when the firewall is not able to handle a huge volume of traffic. This is where the **Watchguard Connections Details** test helps!

This test not only reports the total connections requested to the firewall, but also continuously tracks the connections that are currently active and enumerates the number of dropped connections, so that administrators can rapidly detect an abnormal increase in the number of dropped 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 WatchGuard Firewall server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the WatchGuard Firewall server 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 WatchGuard Firewall for which this test is to be configured.

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total connections	Indicates the total number of connections that were requested to this firewall since startup.	Number	This measure is a good indicator of the load on the firewall.
Active connections	Indicates the number of connections that were	Number	An abnormally high value for this measure could indicate a probable

Measurement	Description	Measurement Unit	Interpretation
	active or open on this firewall.		virus attack or spam to a mail server in the network.
Connections dropped	Indicates the number of connections that were dropped by this firewall.	Number	Ideally, the value of this measure should be zero. If there is a consistent increase in the value of this measure, then it clearly indicates that the firewall is either processing a lot of malicious traffic or is under attack.

3.2.2 Watchguard System Test

In environments where traffic flow is consistently on a higher side, it is always necessary to monitor the flow of traffic through the firewall so that malicious attacks may be identified and removed immediately. This test helps you in analyzing the amont of data that is transmitted/received through the firewall and the packets that are transmitted/received by the firewall. Using this test, administrators may figure out the amount of data and packets that are transmitted/received through the firewall and analyze the efficiency of the firewall constantly.

Target of the test : A WatchGuard Firewall server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the WatchGuard Firewall server 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 WatchGuard Firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

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

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

Measurements made by the test

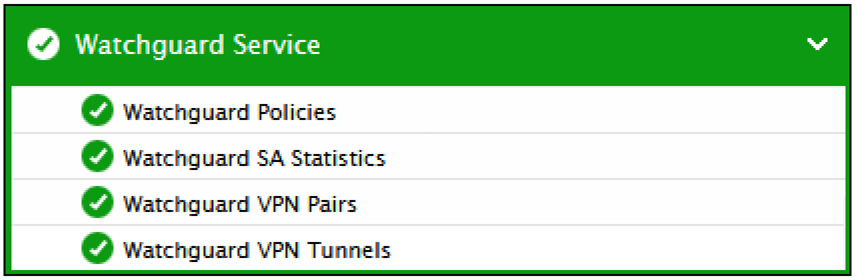
Measurement	Description	Measurement Unit	Interpretation
Data transmitted	Indicates the amount of data transmitted through this firewall.	KB	An abnormal increase in the value of this measure indicates a problem condition that needs to be investigated immediately.
Data Received	Indicates the amount of data received through this firewall.	KB	
Packets transmitted	Indicates the number of packets that were transmitted through this firewall.	Number	A continuously steady value for these measures clearly indicates that the firewall is performing efficiently without any abnormalities.
Packets received	Indicates the number of packets that were received by this firewall.	Number	

3.3 The Watchguard Service Layer

This layer helps the administrator in understanding the following capabilities of the firewall such as:

- Packet traffic through each firewall policy
- Numerical statistics relating to the packets discarded due to various errors for each firewall policy
- For each VPN pair and VPN tunnel, you can identify the traffic flow, packets sent/received statistics, error packets discarded etc.
- Inbound and Outbound data transmission through each protocol of the security association and error packets discared for the security association

Figure 3.4 lists the tests that are currently mapped to the Watchguard Service layer.



✓ Watchguard Service

✓ Watchguard Policies

✓ Watchguard SA Statistics

✓ Watchguard VPN Pairs

✓ Watchguard VPN Tunnels

Figure 3.4: The tests mapped to the Watchguard Service layer

3.3.1 Watchguard Policies Test

The security policy of your organization is a set of definitions to protect your computer network and the information that goes through it. The XTM device denies all packets that are not specifically allowed. When you add a policy to your XTM device configuration file, you add a set of rules that tell the XTM device to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

A policy can also give the XTM device more instructions on how to handle the packet. For example, you can define logging and notification settings that apply to the traffic, or use NAT (Network Address Translation) to change the source IP address and port of network traffic.

For each firewall policy that is configured, this test monitors the number of active connections and the amount of data/packet traffic through the firewall. In addition, this test helps the administrators in identifying the firewall policy through which the maximum number of packets were discarded due to various errors such as replay, authentication etc.

Target of the test : A WatchGuard Firewall server

Agent deploying the test : An external agent

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data traffic	Indicates the amount of data that was transmitted and received for this firewall policy.	KB	Comparing the values of these measures across the policies helps you in identifying the policy through which the data traffic was the maximum at any point of time.
Packet traffic	Indicates the number of packets that are transmitted and received for this firewall policy.	Number	
Packets discarded by decrypt errors	Indicates the number of packets that were discarded due to decrypt errors for this firewall policy.	Number	Ideally, the value of this measure should be zero.
Packets discarded by authenticate errors	Indicates the number of packets that were discarded due to authentication errors for this firewall policy.	Number	Ideally, the value of this measure should be zero.
Packets discarded by replay errors	Indicates the number of packets that were discarded due to replay errors for this firewall policy.	Number	Ideally, the value of this measure should be zero.
Total active connections	Indicates the total number of connections that are active for this firewall policy.	Number	
Current active connections	Indicates the total number of connections that are currently active for this firewall policy.	Number	

3.3.2 Watchguard VPN Pairs Test

This test auto discovers the VPN pairs configured using the WatchGuard Firewall and closely monitors the IPSEc traffic and the amount of packets sent and received via every VPN pair. In the process, the test accurately points to that VPN pair that is handling an abnormally high volume of traffic and is hence hogging the bandwidth resources available to the network! Also, this test reports the number of packets that were discarded due to various errors such as authentication, decrpt etc. 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 WatchGuard Firewall server

Agent deploying the test : An external agent

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Inbound IPSEC traffic	Indicates the amount of IPSec protocol traffic that was received through this VPN pair since the connection was established.	KB	Comparing the value of this measure across the VPN pairs will help you in identifying the VPN pair through which most of the IPSec traffic is flowing!
Outbound IPSEC traffic	Indicates the amount of IPSec protocol traffic that was transmitted through this VPN pair since the connection was established.	KB	
Inbound packets	Indicates the number of packets that were received through this VPN pair during the last measurement period.	Number	
Outbound packets	Indicates the number of packets that were transmitted through this VPN pair during the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
Packets discarded due to decrypt errors	Indicates the number of packets that were discarded due to decrypt errors by this VPN pair during the last measurement period.	Number	Ideally, the value of these measures should be zero. Comparing the value of these measures across the VPN Pairs will help you in identifying the VPN pair that is more error prone during packet transmission.
Packets discarded due to authentication errors	Indicates the number of packets flowing through this VPN pair that were discarded due to authentication errors during the last measurement period.	Number	
Packets discarded due to replay errors	Indicates the number of packets that were discarded due to replay errors by this VPN pair during the last measurement period.	Number	

3.3.3 Watchguard VPN Tunnels Test

A VPN (Virtual Private Network) creates secure connections between computers or networks in different locations. Each connection is known as a tunnel. When a VPN tunnel is created, the two tunnel endpoints authenticate with each other. Data in the tunnel is encrypted. Only the sender and the recipient of the traffic can read it.

Using the WatchGuard 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. Often bandwidth management can be enabled on the firewall 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, identify the issues in the firewall settings and rectify the same! This is where the **Watchguard VPN Tunnels** test helps! This test auto discovers the VPN tunnels configured using the WatchGuard Firewall and closely monitors the amount of data traffic and packets sent and received via every tunnel. In addition, this test clearly indicates the number of various error – prone packets that were sent and received through each VPN 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 WatchGuard Firewall server

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 WatchGuard Firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP

Parameter	Description
	entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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

Parameter	Description
	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**.
IsPassive	If the value chosen is **Yes**, then the WatchGuard 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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Inbound traffic over VPN tunnel	Indicates the amount of traffic that was received through this VPN tunnel since the connection was established.	KB	Comparing the value of these measures across the VPN tunnels helps you in identifying the VPN tunnel that is receiving/transmitting the highest amount of traffic.
Outbound traffic over VPN tunnel	Indicates the amount of traffic that was transmitted through this VPN tunnel since the connection was established.	KB	
Inbound packets over VPN tunnel	Indicates the number of packets that were received through this VPN tunnel during the last measurement period.	Number	Comparing the values of these measures across the VPN tunnels helps you in identifying the VPN tunnel that has received/transmitted the maximum number of packets.
Outbound packets over VPN tunnel	Indicates the number of packets that were transmitted through this VPN tunnel during the last measurement period.	Number	
Inbound packets discarded by decrypt	Indicates the number of packets that were	Number	Ideally, the value of this measure should be zero.

Measurement	Description	Measurement Unit	Interpretation
errors	discarded due to decrypt errors when received by this VPN tunnel during the last measurement period.		
Outbound packets discarded by decrypt error	Indicates the number of packets that were discarded due to decrypt errors when transmitted through this VPN tunnel during the last measurement period.	Number	Ideally, the value of this measure should be zero.
Inbound packets discarded by auth errors	Indicates the number of packets that were discarded due to authentication errors during the last measurement period while being received by this VPN tunnel.	Number	Ideally, the value of this measure should be zero.
Outbound packets discarded by auth errors	Indicates the number of packets that were discarded due to authentication errors during the last measurement period while being transmitted through this VPN tunnel.	Number	Ideally, the value of this measure should be zero.
Inbound packets discarded by replay errors	Indicates the number of packets that were discarded due to replay errors during the last measurement period wile being received by this VPN tunnel.	Number	Ideally, the value of this measure should be zero.
Outbound packets discarded by replay errors	Indicates the number of packets that were discarded due to replay	Number	Ideally, the value of this measure should be zero.

Measurement	Description	Measurement Unit	Interpretation
	errors during the last measurement period while being transmitted through this VPN tunnel.		

3.3.4 Watchguard SA Statistics Test

In Internet Protocol Security (IPSec), settings that establish policy and encryption keys used to protect communication between two end points in a Virtual Private Network (VPN). Security associations are negotiated between two computers during the first phase of establishing an Internet key Exchange (IKE) connection. These security associations establish shared session secrets from which keys are derived for encryption of tunneled data.

This test monitors the security association of the firewall and provides you with the exact numerical statistics of the data packets that were transmitted/received through protocols such as ESP, Authentication Header and IPComp that are part of the IPSec. This way, administrators could identify the protocol that is transmitting/receiving the maximum number of data packets and channelize the packet traffic accordingly!

Target of the test : A WatchGuard Firewall server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the WatchGuard Firewall server 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 WatchGuard Firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this

Parameter	Description
	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 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
Inbound data via ESP	Indicates the amount of data that was received through the ESP protocol.	Number	ESP (Encapsulating Security Payload) provides authentication and encryption of data. ESP takes the original payload of a data packet and replaces it with encrypted data. It adds integrity checks to make sure that the data is not altered in transit, and that the data came from the proper source.
Outbound data via ESP	Indicates the amount of data that was transmitted through the ESP protocol.	Number	
Inbound data via AH	Indicates the amount of data that was received through the AH protocol.	Number	AH (Authentication Header) is a protocol that you can use in manual VPN negotiations. To provide security,

Measurement	Description	Measurement Unit	Interpretation
			AH adds authentication information to the IP datagram. Most VPN tunnels do not use AH because it does not provide encryption.
Outbound data via AH	Indicates the amount of data that was transmitted through the AH protocol.	Number	
Inbound data via Ipcomp	Indicates the amount of data that was received through the IPComp protocol.	Number	In networking IP Payload Compression Protocol, or IPComp, is a low level compression protocol for IPdatagrams. The intent is to reduce the size of data transmitted over congested or slow network connections, thereby increasing the speed of such networks without losing data. According to the RFC requirements, compression must be done before fragmenting or encrypting the packet. It further states that each datagram must be compressed independently so it can be decompressed even if received out of order. This is important because it allows IPComp to work with both TCP and UDP network communications.
Outbound data via Ipcomp	Indicates the amount of data that was transmitted through the IpComp protocol.	Number	

3.3.5 Watchguard SA Errors Test

Security associations are negotiated between two computers during the first phase of establishing an Internet key Exchange (IKE) connection. These security associations establish shared session secrets from which keys are derived for encryption of tunneled data. For an optimal encryption process to happen, the packets that are sent thorugh the security associations should be error free. If too many errors are spotted in the data packets, administrators may need to figure out the exact cause of the errors – whether is it due to a fault security association connection or due to a malicious attack? The Watchguard SA errors test helps you in identifying the errors in the data packets!

This test monitors the security association of the firewall and identifies the data packets that were received with errors such as decrypt errors, authenticate errors, replay errors etc. This way, administrators would be alerted if there are too may errors that need to be manipulated for the security association to encrypt tunneled data smoothly.

Target of the test : A WatchGuard Firewall server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the WatchGuard Firewall server 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 WatchGuard Firewall for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP

Parameter	Description
	context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the UserName provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the UserName in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some

Parameter	Description
	environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Packets received with decrypt errors	Indicates the number of packets that were received with decrypt errors.	Number	Ideally, the value of this measure should be zero. A high value for this measure is a cause of concern which requires the administrator to identify the errors and rectify them quickly.
Packets received with authenticate errors	Indicates the number of packets that were received with authentication errors.	Number	
Packets received with replay errors	Indicates the number of packets that were received with replay errors.	Number	
Packets received with policy errors	Indicates the number of packets that were received with errors relating to the security policy.	Number	
Packets received with other errors	Indicates the number of packets that were received with other type of errors i.e.,.packets received with miscellaneous errors.	Number	

About eG Innovations

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

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

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

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

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.