Monitoring Cisco ASA

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW DOES THE EG ENTERPRISE MONITOR THE CISCO ASA? 2

2.1 Managing the Cisco ASA 2

CHAPTER 3: MONITORING THE CISCO ASA 4

3.1 The ASA Hardware Layer 5

3.1.1 ASA Hardware Status Test 5

3.1.2 ASA CPU Details Test 9

3.1.3 ASA Memory Details Test 11

3.2 The Network Layer 14

3.3 The ASA Sessions Layer 15

3.3.1 ASA Remote Access Sessions Test 15

3.3.2 ASA Sessions Test 18

3.4 The ASA Tunnels Layer 20

3.4.1 Ike Global Tunnels Test 21

3.4.2 Ike Secondary Tunnels Test 24

ABOUT EG INNOVATIONS 28

Table of Figures

Figure 2.1: Adding a Cisco ASA component 2
Figure 2.2: List of unconfigured tests to be configured for the Cisco ASA 3
Figure 2.3: Configuring the ASA CPU Details test 3
Figure 3.1: The Cisco ASA layer model 4
Figure 3.2: The tests mapped to the ASA Hardware Layer 5
Figure 3.3: The tests mapped to the Network layer 14
Figure 3.4: The tests associated with the ASA Sessions layer 15
Figure 3.5: The tests mapped to the ASA Tunnels layer 21

Chapter 1: Introduction

In computer networking, Cisco ASA 5500 Series Adaptive Security Appliances, or simply Cisco ASA 5500 Series, is Cisco's line of network security devices.

In an era that abounds in network security threats, the continuous availability and error-free operation of the Cisco ASA device is of utmost importance in order to protect mission-critical IT infrastructures from malicious virus attacks, and thus ensure the continuous availability of these infrastructures.

To continuously monitor the Cisco ASA device and promptly alert administrators to issues in its performance, eG Enterprise provides the Cisco ASA monitoring model.

This document describes the eG-developed custom monitor for the Cisco ASA.

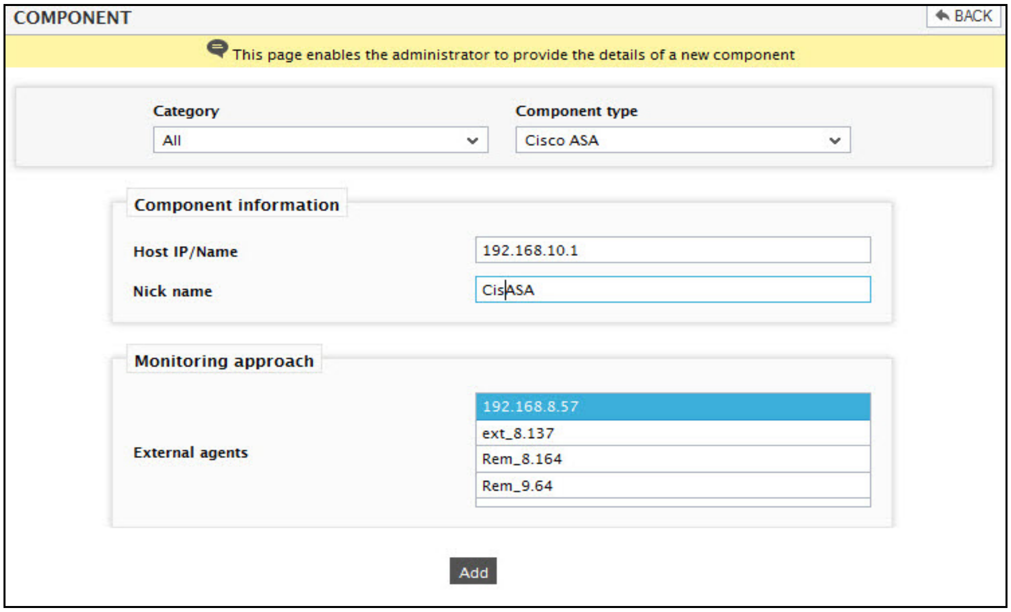
Chapter 2: How does the eG Enterprise Monitor the Cisco ASA?

The eG Enterprise is capable of monitoring the Cisco ASA using an eG external agent on any remote host. The eG external agent periodically checks the SNMP MIB of the Cisco ASA for fetching the metrics related to the performance of the Cisco ASA device. The sections that follow describe how to manage and monitor the Cisco ASA device.

2.1 Managing the Cisco ASA

The eG Enterprise cannot automatically discover a Cisco ASA device. This implies that you need to manually add the component for monitoring. To manage a Cisco ASA 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 Cisco ASA 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: Cisco ASA

Component information

Host IP/Name: 192.168.10.1

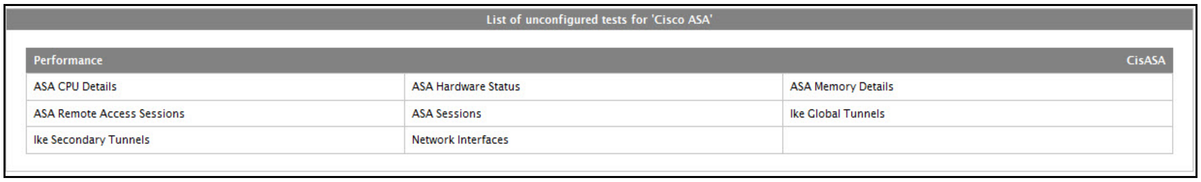
Nick name: CisASA

Monitoring approach

External agents: 192.168.8.57, ext_8.137, Rem_8.164, Rem_9.64

Figure 2.1: Adding a Cisco ASA component

4. Specify the **Host IP/Name** and **Nick name** of the Cisco ASA component to be monitored as shown in . Then, click **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

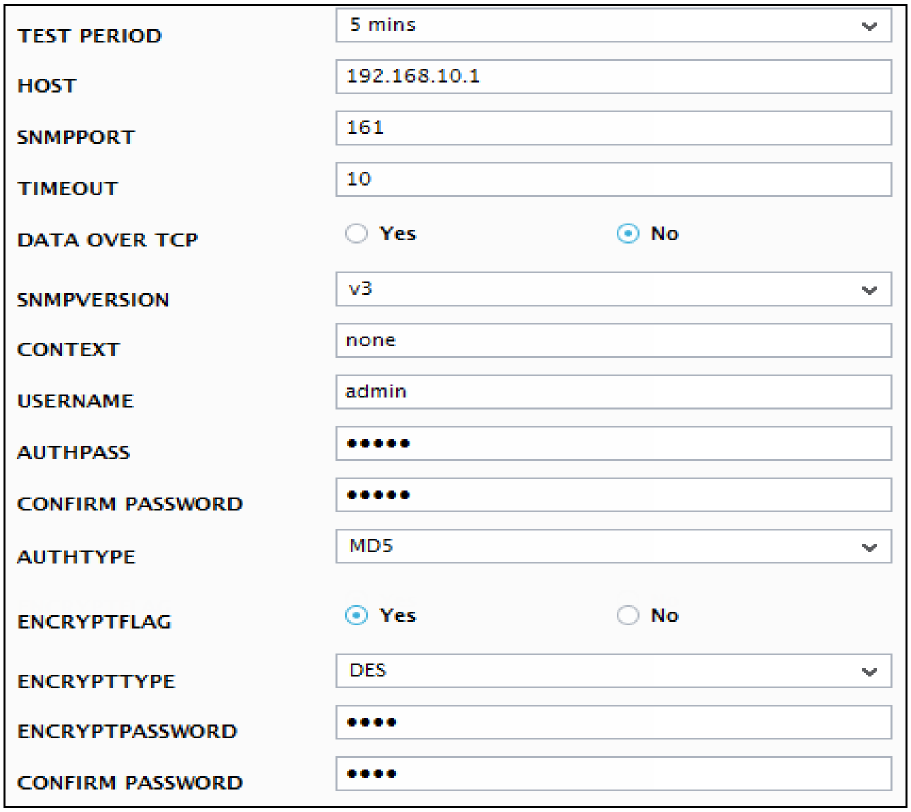


List of unconfigured tests for 'Cisco ASA'

Performance		CisASA
ASA CPU Details	ASA Hardware Status	ASA Memory Details
ASA Remote Access Sessions	ASA Sessions	Ike Global Tunnels
Ike Secondary Tunnels	Network Interfaces	

Figure 2.2: List of unconfigured tests to be configured for the Cisco ASA

6. Click on any test in the list of unconfigured tests. For instance, click on the **ASA CPU 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 ASA CPU Details test

7. To know how to configure the tests, refer to the **Monitoring the Cisco ASA** chapter.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Cisco ASA

eG Enterprise provides the Cisco ASA monitoring model.To continuously monitor the Cisco ASA device and promptly alert administrators to issues in its performance,

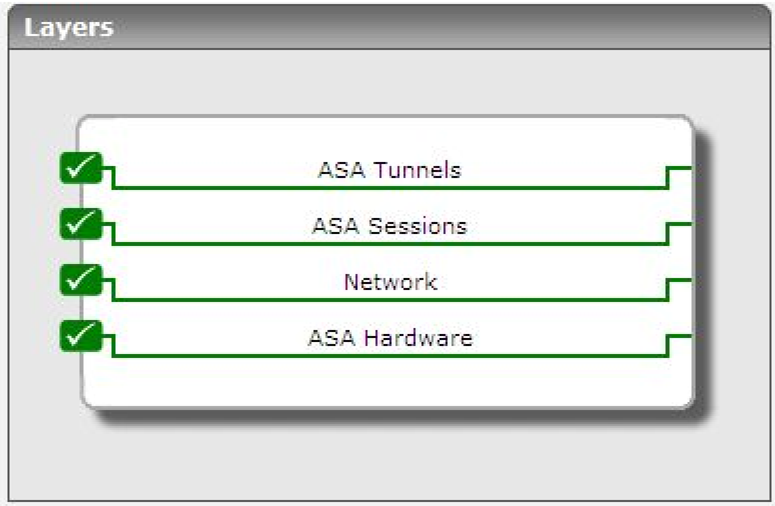


Figure 3.1: The Cisco ASA layer model

Using the metrics reported by this model, you can answer the following questions quickly and accurately:

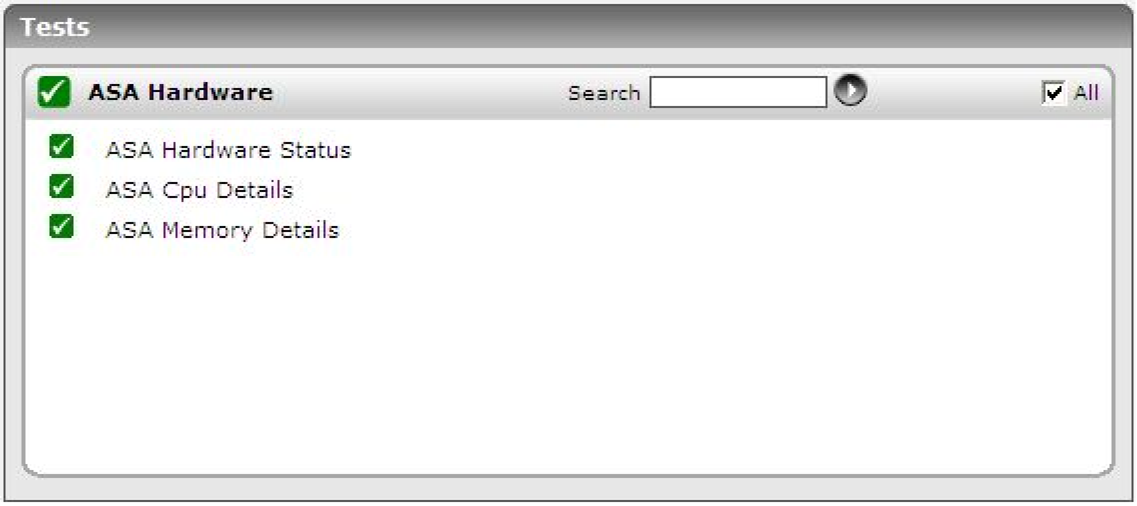
- Is any memory pool consuming memory excessively?
- Is the device utilizing its CPU resources optimally? When during the last 5 minutes did the CPU usage peak - during the last 1 second or the last 1 minute?
- What are the types of hardware that support the firewall unit of the device? What is the current state of each hardware type?
- Are too many remote access sessions active on the device? How many users are connected to the device via these sessions?
- Is the device overloaded with sessions? How many of these sessions are currently inactive? Can they be closed?
- Were too many packets dropped by the IPsec Phase-1 IKE global and secondary tunnels? When was packet drop the maximum - when the tunnels were receiving data or transmitting data?

The sections that will follow discuss each layer of the monitoring model depicted by Figure 3.1 above.

3.1 The ASA Hardware Layer

The tests mapped to this layer will enable you to instantly detect the following:

- Hardware failures and the type of hardware that has failed;
- Abnormal CPU usage by the ASA device;
- Excessive memory usage by the device, and the memory pool from which maximum memory resoures have been drained;



Tests

☑ ASA Hardware Search ☑ All

☑ ASA Hardware Status
☑ ASA Cpu Details
☑ ASA Memory Details

Figure 3.2: The tests mapped to the ASA Hardware Layer

3.1.1 ASA Hardware Status Test

This test auto-discovers the various types of hardware that support the firewall unit of the ASA device, and reports the current status of each hardware.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of hardware auto-discovered from the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed

Parameter	Description
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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
Status	Indicates the current status of hardware of this type.		The values that this measure can report and the states they indicate are available in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Down</td></tr>
<tr><td>1</td><td>Error</td></tr>
<tr><td>2</td><td>Over Temperature</td></tr>
<tr><td>3</td><td>Busy</td></tr>
<tr><td>4</td><td>Nomedia</td></tr>
<tr><td>5</td><td>Backup</td></tr>
<tr><td>6</td><td>Active</td></tr>
<tr><td>7</td><td>Standby</td></tr>
<tr><td>8</td><td>Other</td></tr>
<tr><td>9</td><td>Up</td></tr>
</table>
The above listed status are given for each of the hardware type. The Hardware type would be any of the following :
• memory,
• disk,
• power,
• netInterface,
• cpu,
• primaryUnit, secondaryUnit and other hardware types.
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the resource. The graph of this measure however, represents the measure values using the numeric equivalents only.
</td></tr>
</table>

3.1.2 ASA CPU Details Test

This test enables administrators to figure out how CPU hungry the ASA device is. 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 usage peak; this revelation will help them troubleshoot CPU spikes better.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU busy (5sec)	Indicates the percentage of time during the last 5 seconds the device was using the CPU.	Percent	By comparing the values of all the 3 measures, you can quickly figure out when CPU usage was maximum so that, you can investigate why CPU usage peaked during that time.
CPU busy (1min)	Indicates the percentage of time during the last 1 minute the device was using the CPU.	Percent	
CPU busy (5min)	Indicates the percentage of time during the last 5 minutes the device was using the CPU.	Percent	

3.1.3 ASA Memory Details Test

To evaluate the memory efficiency of an ASA device, you need to know how each memory pool configured for the device is consuming the available memory resources. This test provides this information. For every memory pool, this test reports the percentage of unused memory in the pool. By comparing the memory usage statistics reported by this test across all memory pools, you can quickly identify which pool is under-sized or is currently running out of memory.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameter	Description
	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**.

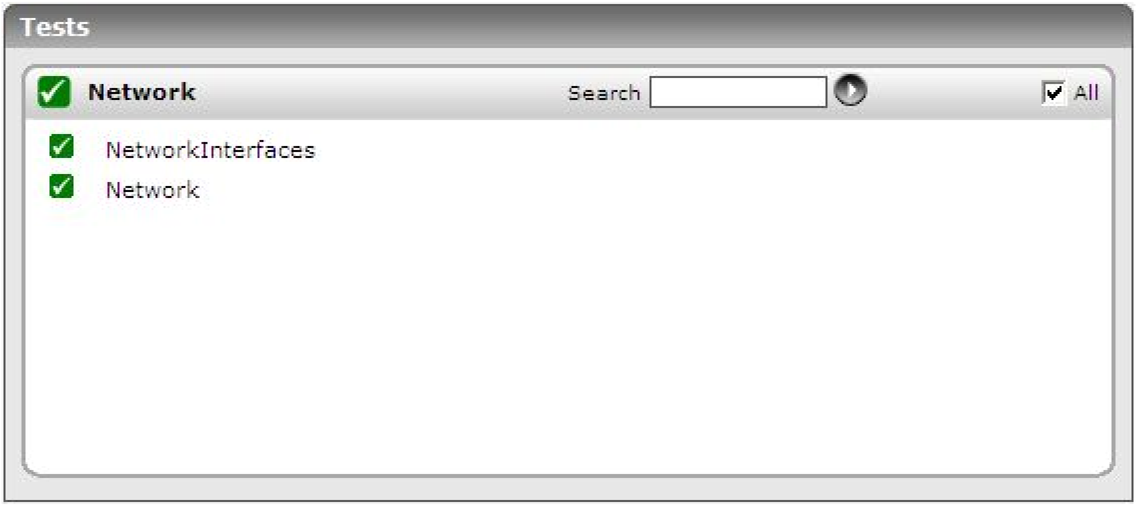
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total memory (in MB) available for this memory pool.	MB	
Used memory	Indicates the number of	MB	

Measurement	Description	Measurement Unit	Interpretation
	bytes from this pool that are currently used by applications on the managed device.		
Available memory	Indicates the number of bytes from this pool that are currently available for use by applications.	MB	
Available free memory	Indicates the percentage of unused memory in this pool.	Percent	Ideally, this value should be high. A low value or a value that consistently decreases could be a cause for concern, as it could indicate the gradual erosion of memory resources from the pool. Under such circumstances, you may either want to resize the pool or investigate what is causing the memory drain and curb it.

3.2 The Network Layer

The quality of network connections to and from the device, and the overall health, speed, and bandwidth usage of the network interfaces supported by the device can easily assess using the tests mapped to this layer.



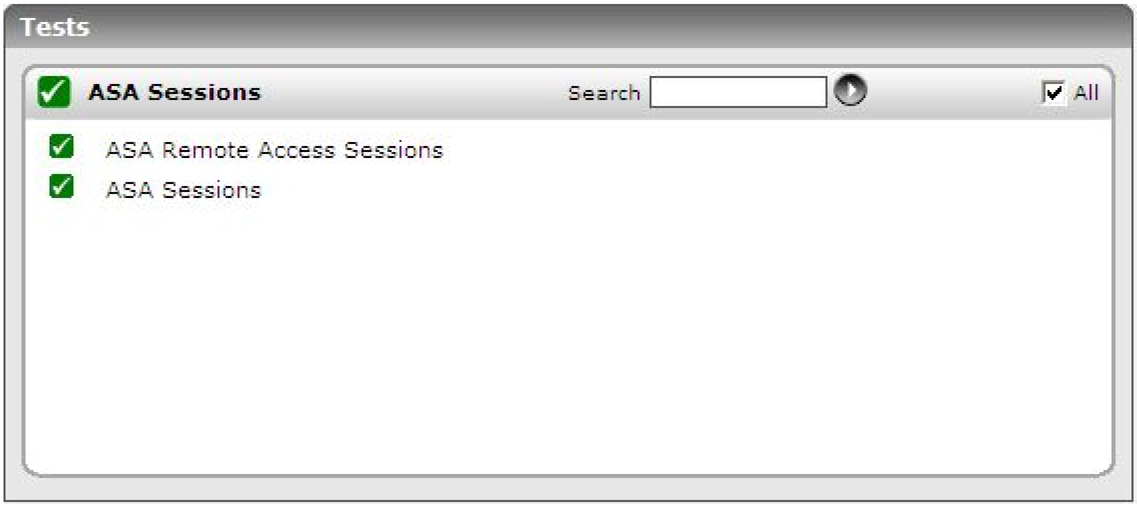
☑ NetworkInterfaces
☑ Network

Figure 3.3: The tests mapped to the Network layer

Since all the tests depicted by Figure 3.3 have been elaborately discussed in the *Monitoring Cisco Router* document, let us proceed to the next layer.

3.3 The ASA Sessions Layer

This layer monitors the session load on the device.



☑ ASA Remote Access Sessions

☑ ASA Sessions

Figure 3.4: The tests associated with the ASA Sessions layer

3.3.1 ASA Remote Access Sessions Test

This test reveals the load generated by remote access sessions by reporting the number of remote access sessions that are currently active on the device, and the number of users connecting to those sessions.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.

Parameter	Description
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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
Remote sessions	Indicates the number of sessions that are currently active on the device.	Number	
Active users	Indicates the number of users who have active remote access sessions.	Number	

3.3.2 ASA Sessions Test

This test serves as a good indicator of the session load on the device.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameter	Description
	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 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 sessions	Indicates the total number of sessions to the device.	Number	
Active sessions	Indicates the total number of sessions to the device.	Number	

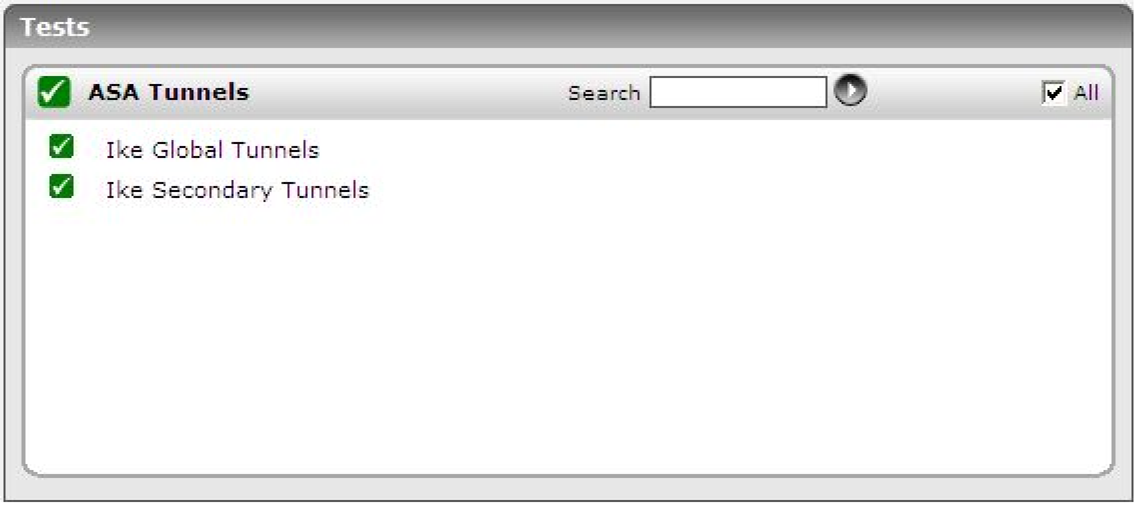
3.4 The ASA Tunnels Layer

Tunneling makes it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network. Each secure connection is called a tunnel. The adaptive security appliance uses the ISAKMP and IPsec tunneling standards to build and manage tunnels. ISAKMP and IPsec accomplish the following:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users and data
- Manage security keys
- Encrypt and decrypt data
- Manage data transfer across the tunnel
- Manage data transfer inbound and outbound as a tunnel endpoint or router

The adaptive security appliance functions as a bidirectional tunnel endpoint. It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The tests mapped to this layer monitor the Ike global and secondary tunnels.



Tests

☑ ASA Tunnels Search ☑ All

☑ Ike Global Tunnels

☑ Ike Secondary Tunnels

Figure 3.5: The tests mapped to the ASA Tunnels layer

3.4.1 Ike Global Tunnels Test

This test measures the level of traffic to and from the IKE global tunnels.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active tunnels	Indicates the number of IPsec Phase-1 IKE Tunnels that are currently active.	Number	IKE (Internet Key Exchange), also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. ISAKMP separates negotiation into two phases: Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. This measure reports the number of such tunnels that are currently active.
In packets	Indicates the number of packets received by all IPsec Phase-1 IKE tunnels.	Number	
Out packets	Indicates the number of packets sent by all IPsec Phase-1 IKE tunnels.	Number	

Measurement	Description	Measurement Unit	Interpretation
In packets dropped	Indicates the number of packets that were dropped by all IPsec Phase-1 IKE tunnels while receiving data.	Number	Ideally, this value should be low.
Out packets dropped	Indicates the number of packets that were dropped by all IPsec Phase-1 IKE tunnels while sending data.	Number	Ideally, this value should be low.

3.4.2 Ike Secondary Tunnels Test

This test measures the level of traffic to and from the IKE secondary tunnels.

Target of the test : A Cisco ASA Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cisco ASA device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco ASA device.
Port	The port at which the Cisco ASA device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

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

Parameter	Description
	• **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
Active tunnels	Indicates the number of IPsec Phase-2 IKE Tunnels that are currently active.	Number	IKE (Internet Key Exchange), also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. ISAKMP separates negotiation into two phases: Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. This measure reports the number of tunnels that protect data.
In packets	Indicates the number of packets received by all IPsec Phase-2 IKE tunnels.	Number	
Out packets	Indicates the number of packets sent by all IPsec Phase-2 IKE tunnels.	Number	

Measurement	Description	Measurement Unit	Interpretation
In packets dropped	Indicates the number of packets that were dropped by all IPsec Phase-2 IKE tunnels while receiving data.	Number	Ideally, this value should be low.
Out packets dropped	Indicates the number of packets that were dropped by all IPsec Phase-2 IKE tunnels while sending data.	Number	Ideally, this value should be low.

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.

Copyright © 2020 eG Innovations Inc. All rights reserved.

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.