Monitoring Cyberoam Firewall

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Cyberoam Firewall is available as a Next-Generation Firewall and UTM firewall. It offers stateful and deep packet inspection for network, application and user identity-based security. Cyberoam's Layer 8 Human Identity-based firewall appliance enables work-profile based policies and a single interface for policy creation across all features, providing ease of management and high security with flexibility. Cyberoam Firewall thus protects organizations from DoS, DDoS and IP Spoofing attacks.

Cyberoam offers advanced network security features to deliver business continuity, faster uptimes, higher network throughput, rapid network growth, meeting the security and regulatory compliance requirements through the following capabilities:

- High Availability with stateful failover
- Dynamic routing
- Multiple VLAN zones to create work-profile based groups across distributed locations
- Virtual host capability, enabling secure hosting of services inside the LAN and DMZ
- Centralized management and logging-reporting

These capabilities enable administrators to 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 Cyberoam Firewall using eG Enterprise?

eG enterprise monitors the Cyberoam Firewall in an agentless manner. For this purpose, deploy a single eG agent on a remote Windows host. This agent executes various tests that connect to the SNMP MIB of the firewall to be monitored, and collects critical statistics of interest. To enable the eG agent to access the SNMP MIB, specify the following while configuring the tests:

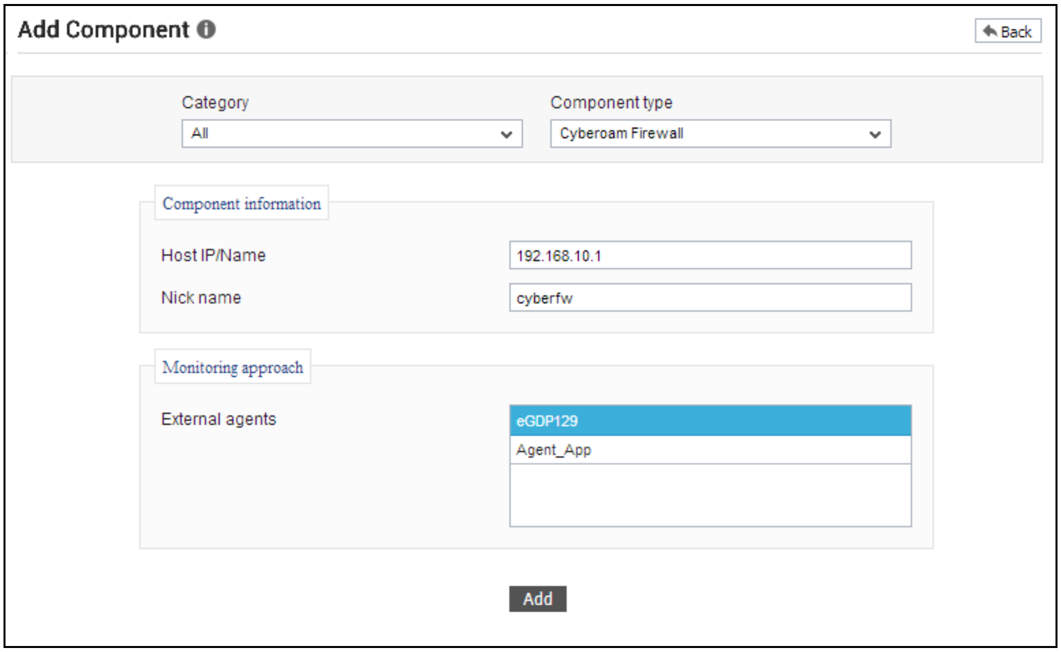
- port number on which the target firewall exposes its MIB
- SNMP community to be used for accessing the MIB

To start monitoring the target firewall, first manage the Cyberoam Firewall component using the steps explained in the section below.

2.1 Managing the Cyberoam Firewall

Using eG Enterprise, you can auto-discover the Cyberoam Firewall as well as manually add the component for monitoring. To manage a Cyberoam Firewall component, do the following:

1. Log into the eG admin interface.
2. If the Cyberoam Firewall is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if the target firewall is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **COMPONENTS** page. Remember that components manually added are managed automatically.
4. In the **COMPONENT** page that appears next, select *Cyberoam Firewall* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



Add Component

Category: All

Component type: Cyberoam Firewall

Component information

Host IP/Name: 192.168.10.1

Nick name: cyberfw

Monitoring approach

External agents: eGDP129, Agent_App

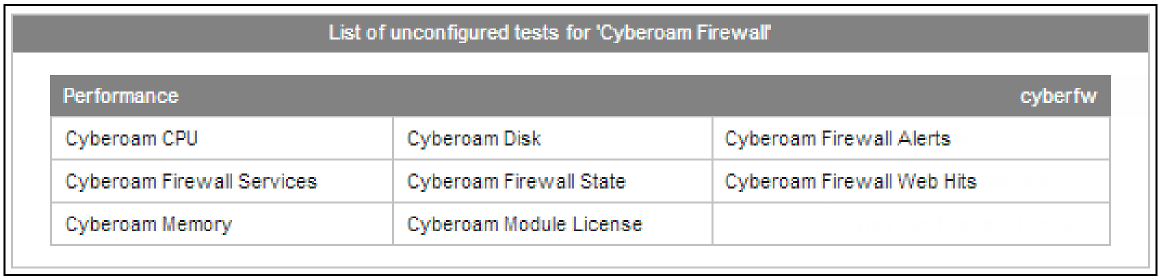
Figure 2.1: Adding the Cyberoam Firewall component

5. Specify the **Host IP/Name** and the **Nick name** for the Cyberoam Firewall component.

6. Choose an external agent for the target firewall by picking an option from the **External agents** list box.

7. Then, click the **Add** button to register the changes (see Figure 2.1).

8. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.



List of unconfigured tests for 'Cyberoam Firewall'

Performance		cyberfw
Cyberoam CPU	Cyberoam Disk	Cyberoam Firewall Alerts
Cyberoam Firewall Services	Cyberoam Firewall State	Cyberoam Firewall Web Hits
Cyberoam Memory	Cyberoam Module License	

Figure 2.2: A list of tests that need to be configured for the Cyberoam Firewall

9. Click on any test in the list of unconfigured tests. For instance, click on the **Cyberoam CPU** test to configure it. To know how to configure the tests, refer to **Monitoring Cyberoam Firewall**.

10. Finally, signout of the eG admin interface.

Chapter 3: Monitoring Cyberoam Firewall

eG Enterprise provides a specialized Cyberoam Firewall monitoring model (see Figure 3.1), which periodically polls the SNMP MIBs of the firewall to measure the connections, responsiveness, resource usage, service state and module licenses of the firewall, and notifies administrators of potential resource crunches or subscriptions issues with the firewall.

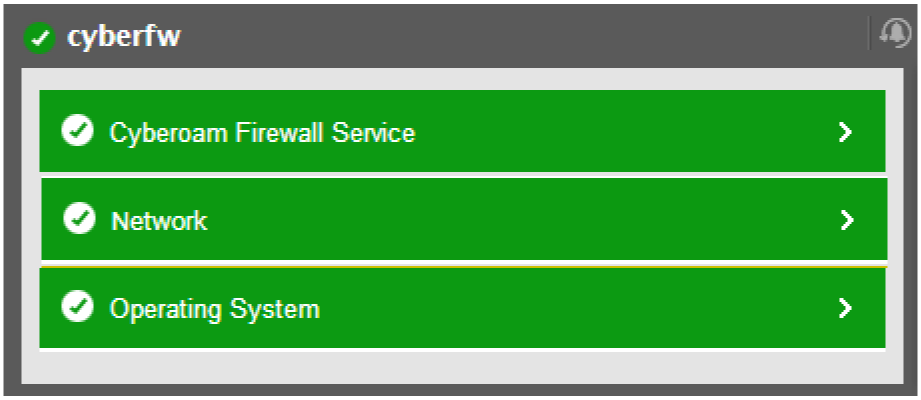


Figure 3.1: The layer model of the Cyberoam Firewall

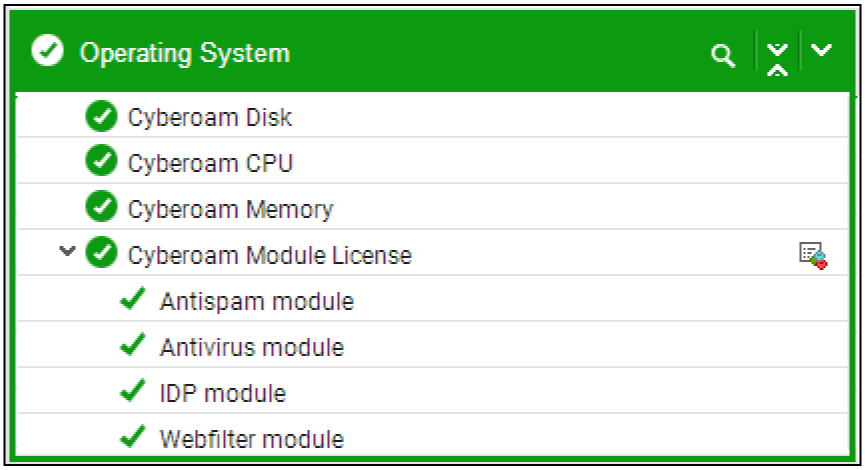
Using the metrics reported, administrators can find quick and accurate answers for the following performance questions:

- What is the current CPU utilization of the firewall?
- How well the memory of the firewall is utilized?
- What is the swap memory utilization on the firewall?
- What is the current state of the firewall services?
- How many hits were received by each protocol?
- What is the subscription status of the modules?
- How many anti-virus events were triggered during the last measurement period?

The **Network** layer of the **Cyberoam 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 potential space crunch. In addition, this layer also tracks the subscription status of the modules on the firewall.



Operating System

- ✓ Cyberoam Disk
- ✓ Cyberoam CPU
- ✓ Cyberoam Memory
- ✓ Cyberoam Module License
  - ✓ Antispam module
  - ✓ Antivirus module
  - ✓ IDP module
  - ✓ Webfilter module

Figure 3.2: The tests mapped to the Operating System layer

3.1.1 Cyberoam CPU Test

This test helps administrators to figure out how CPU hungry the Cyberoam firewall is, and also enables them to quickly troubleshoot the issues (if any) in the CPU resource usage.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cyberoam Firewall that is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU usage	Indicates the percentage of CPU utilized by the firewall.	Percent	If the value of this measure is close to 100, it is a cause for concern.

3.1.2 Cyberoam Disk Test

This test monitors the space utilization of each disk in the Cyberoam Firewall and proactively alerts administrators to potential space crunches, if any.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk on the Cyberoam Firewall being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host for which this test is to be configured.
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

Parameter	Description
	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
Disk space	Indicates the total space of this disk.	GB	
Used space	Indicates the space that is currently in use on this disk.	GB	Compare the value of this measure across the disks to find out the disk that is over utilized.

Measurement	Description	Measurement Unit	Interpretation
Free space	Indicates the space that is currently available for use in this disk.	GB	A high value is desired for this measure. If the value of this measure is decreasing alarmingly, then it indicates that the disk is running out of space. Administrators may either need to free up the space or add additional resources to the disk.
Space utilization	Indicates the percentage of space utilized on this disk.	Percent	A low value is desired for this measure. If the value of this measure is greater than 80, it indicates that the disk is running out of space.

3.1.3 Cyberoam Memory Test

This test reveals the statistics related to the utilization of the main memory and swap memory of the Cyberoam firewall. Using this test, administrators may be proactively alerted to memory resource contention, if any.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cyberoam Firewall that is 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 Nexus Switch to be monitored.
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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total memory of the Cybreoam firewall.	GB	
Used memory	Indicates the amount of memory currently utilized by the firewall.	GB	A high value for this measure indicates that the memory resources are depleting drastically. Administrators may be alerted to add additional resources before memory resources are drained completely.
Free memory	Indicates the amount of memory that is currently available for use in the firewall.	GB	The value of this measure should be high.
Memory usage	Indicates the percentage of memory utilized by the firewall.	Percent	
Swap memory size	Indicates the total amount of memory that is allocated	GB	Swap memory is the temporary storage on the disk and used only

Measurement	Description	Measurement Unit	Interpretation
	as swap memory for the firewall.		when the main memory is unable to function properly or full.
Used swap memory	Indicates the amount of swap memory currently utilized by the firewall.	GB	A low value is desired for this measure.
Free swap memory	Indicates the amount of swap memory that is currently available for use in the firewall.	GB	The value of this measure should be high.
Swap memory usage	Indicates the percentage of swap memory utilized by the firewall.	Percent	

3.1.4 Cyberoam Module License Test

To apply improved anti-virus protection and spam filtering, the Cyberoam Firewall includes the following subscription modules, which are not included in basic package:

- Intrusion Detection and Prevention
- Gateway Anti Virus
- Gateway Anti Spam
- Web and Application Filter
- 8 x 5 Support
- 24 x 7 Support

These modules when subscribed provide higher levels of security and protect the environment from unknown threats and malicious attacks. Administrators can subscribe these modules either for free trial or for longer period with registered license. Monitoring the current status of these subscriptions helps administrators to find out whether the modules are in trial period, subscribed with license, unsubscribed or expired. This is where the **Cyberoam Module License** test helps administrators!

This test auto-discovers the modules available on the target firewall, and for each module, it reveals the subscription status.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk on the Cyberoam Firewall being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the target host for which this test is to be configured.
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.

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Module subscribe status	Indicates the subscription status of this module on		The values that this measure reports and their corresponding numeric values

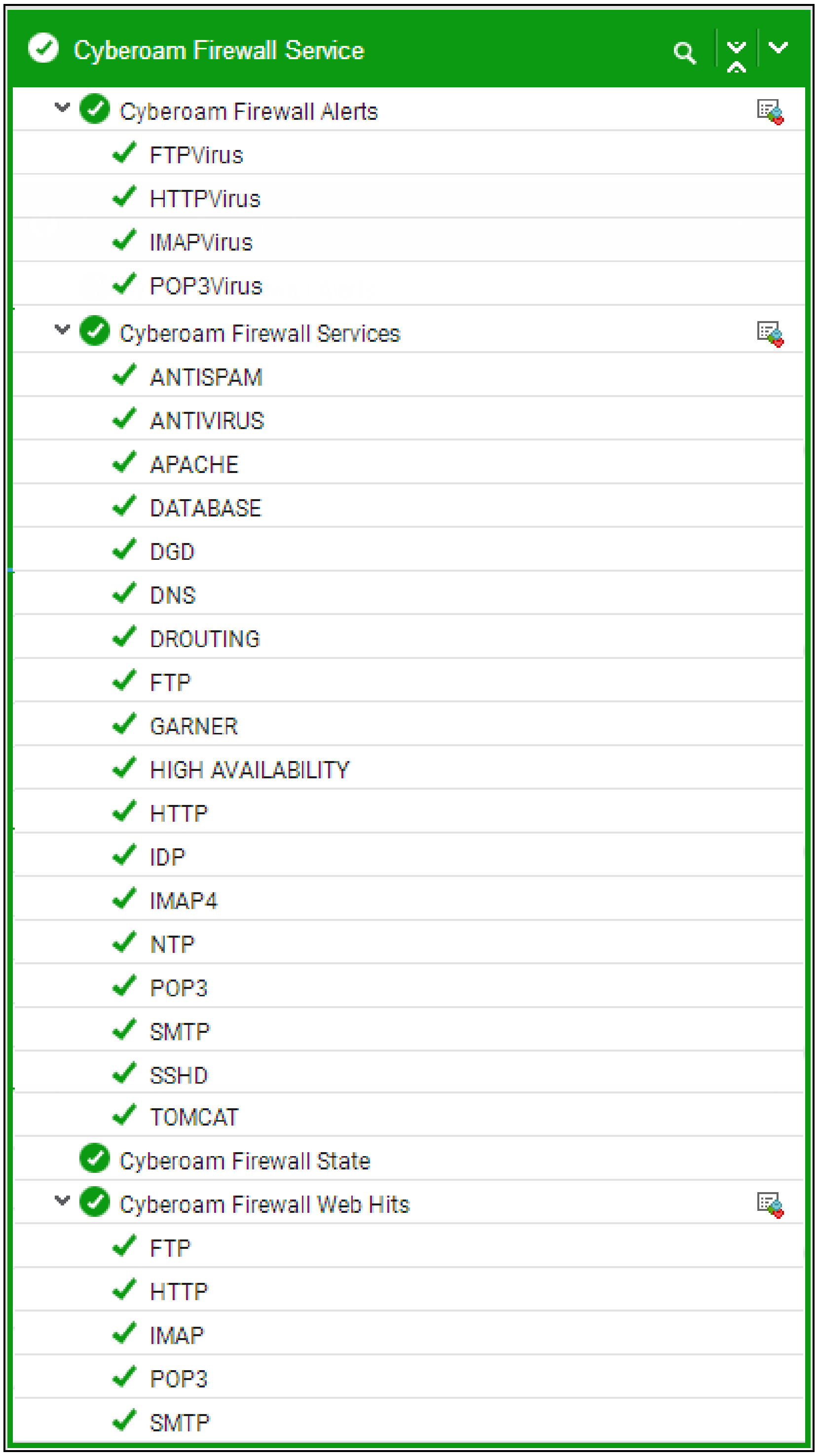
<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>the firewall.</td><td></td><td>are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Trial</td><td>1</td></tr><tr><td>Unsubscribed</td><td>2</td></tr><tr><td>Subscribed</td><td>3</td></tr><tr><td>Expired</td><td>4</td></tr></table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s discussed in the table above. However, in the graph of this measure, the subscription status of the each module is indicated using the numeric equivalents only.</td></tr>
</table>

3.2 The Cyberoam Firewall Service Layer

This layer helps the administrator to figure out the following statistics:

- High-availability status of the firewall
- Status of each service on the firewall
- Alerts generated by the protocol based anti-virus
- Number of hits transferred through the firewall by different protocols

Figure 3.3 lists the tests that are currently mapped to the Cyberoam Firewall Service layer.



Cyberoam Firewall Service

- Cyberoam Firewall Alerts
  - ✓ FTPVirus
  - ✓ HTTPVirus
  - ✓ IMAPVirus
  - ✓ POP3Virus
- Cyberoam Firewall Services
  - ✓ ANTISPAM
  - ✓ ANTIVIRUS
  - ✓ APACHE
  - ✓ DATABASE
  - ✓ DGD
  - ✓ DNS
  - ✓ DROUTING
  - ✓ FTP
  - ✓ GARNER
  - ✓ HIGH AVAILABILITY
  - ✓ HTTP
  - ✓ IDP
  - ✓ IMAP4
  - ✓ NTP
  - ✓ POP3
  - ✓ SMTP
  - ✓ SSHD
  - ✓ TOMCAT
- Cyberoam Firewall State
- Cyberoam Firewall Web Hits
  - ✓ FTP
  - ✓ HTTP
  - ✓ IMAP
  - ✓ POP3
  - ✓ SMTP

Figure 3.3: The tests mapped to the Cyberoam Firewall Service layer

3.2.1 Cyberoam Firewall State Test

Cyberoam uses clustering technology to ensure high availability. In a cluster, two Cyberoam firewall appliances are grouped together and instructed to work as a single entity. In the cluster setup, one of the firewall appliances acts as primary whereas the other one acts as secondary. The high availability configuration always ensures that one of the two firewall appliances is available for maintaining the network traffic so that the downtime of the network is reduced considerably. The firewall appliances can be configured in Active/Passive or Active/Active mode.

If the high availability of the firewall is challenged, the environment may become vulnerable to unknown virus attacks and unauthorized access, both of which can put the environment's security at risk. Hence, to make sure that the environment stays protected around the year from network threats, it is necessary to monitor the high availability status of the Cyberoam firewall. This is where the **Cyberoam Firewall State** test helps administrators!

By continuously monitoring the target firewall, this test reveals whether the firewall is in standalone configuration or high availability configuration. In addition, this test also reports the number of VPN users who are currently accessing the firewall. Analyzing these metrics, administrators can figure out the mode in which the firewall is currently operating and the workload.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Cyberoam Firewall being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host for which this test is to be configured.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>HA mode</td><td>Indicates whether the firewall is configured in standalone mode or high-availability mode, and the mode on which the firewall is configured for high availability.</td><td></td><td>The values that this measure reports and their corresponding numeric values are listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Standalone</td><td>1</td></tr>
<tr><td>Active-passive</td><td>2</td></tr>
<tr><td>Active-active</td><td>3</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s discussed in the table above. However, in the graph of this measure, the high availability status of the firewall is indicated</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			using the numeric equivalents only.
Firewall live users	Indicates the number of users who are currently connected to the firewall.	Number	This measure is a good indicator of the current workload on the firewall.

3.2.2 Cyberoam Firewall Alerts Test

This test intercepts the traps sent by the protocols based on anti-virus detection, extracts relevant information related to the errors from the traps, and reports the count of anti-virus events to the eG manager. This information enables administrators to detect the failures if any, understand the nature of failures, and accordingly decide on the remedial measures.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each protocol communicating with the target Cyberoam Firewall.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified host listens. By default, this is NULL.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
<p>In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.</p>
<p>An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.</p>
<p>Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be Host and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:</p>
<p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p>
<p>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:</p>
<p>Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.</p>
<p>Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.</p>
</td></tr>
<tr><td>ShowOID</td><td>Specifying True against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.</td></tr>
<tr><td>TrapOIDs</td><td>By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be</td></tr>
</table>

Parameters	Description
	specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Antivirus alerts	Indicates the number of times the anti-virus alert was triggered through this protocol during the last measurement period.	Number	Ideally, the value of this measure should be zero. A high value is an indication of security risk in your environment. The detailed diagnosis of this measure reveals the host which sent the traps, the time stamp at which the trap was received, type of the trap and the trap message

3.2.3 Cyberoam Firewall Services Test

This test auto-discovers the services on the Cyberoam firewall, and reports the current status of each service. Using this test, administrators can instantly find out the services that are currently running, stopped or dead. This way, administrators can quickly take necessary actions if any of the services is in the stopped or dead state for long time.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each service on the Cyberoam Firewall being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the target host for which this test is to be configured.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Service status</td><td>Indicates the current status of this service.</td><td></td><td>The values that this measure reports and their corresponding numeric values are listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Dead</td><td>1</td></tr>
<tr><td>Stopped</td><td>2</td></tr>
<tr><td>Initializing</td><td>3</td></tr>
<tr><td>Running</td><td>4</td></tr>
<tr><td>Exiting</td><td>5</td></tr>
<tr><td>Untouched</td><td>6</td></tr>
<tr><td>Unregistered</td><td>7</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s discussed in the table above. However, in the graph of this measure, the status of the each service is indicated using the numeric equivalents only.</td></tr>
</table>

3.2.4 Cyberoam Firewall Web Hits Test

The Cyberoam firewall is capable of handling traffic generated by various protocols such as HTTP, HTTPs, SMTP, FTP, etc. In large environments, administrators may want to identify the protocol that transfers maximum number of requests to the infrastructure through the target firewall. This can be easily achieved using the **Cyberoam Firewall Web Hits** test!

This test auto-discovers the protocols that are communicating with the IT infrastructure through the Cyberoam firewall and for each protocol, reports the number of hits transferred by each protocol. This way, administrators can easily figure out the protocol through which the maximum amount of traffic is ported to the firewall and block the requests from that protocol, if necessary.

Target of the test : A Cyberoam Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each protocol communicating with the Cyberoam Firewall being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the target host for which this test is to be configured.
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

Parameter	Description
	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 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

Parameter	Description
	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
Web hits	Indicates the number of hits transferred through the firewall by this protocol during the last measurement period.	Number	Compare the value of this measure across the protocols to find out the protocol that ported the maximum number of requests through the firewall.

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 © 2019 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.