Monitoring FortiGate Firewall

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

FortiGate's firewall series of ASIC accelerated antivirus firewalls are the new generation of real time protection systems for LAN, VPN, WAN and wireless network security. Capable of providing anitvirus/worm protection for emails, network inrusion detection, web content filtering based on URLS and keywords and traffic shaping, the FortiGate Antivirus Firewall products secure the network without degrading its performance.

High availability of the firewall is therefore imperative to ensure the safety of the mission-critical environment it protects. If the availability of the firewall is challenged, then the IT environment is rendered defenceless against unsavory virus attacks and unauthorized access, both of which can cause irreparable damage. Hence, to make sure that an IT environment stays protected 24X7X365 from network threats, the availability and performance of the firewall should be continuously monitored. eG Enterprise helps administrators in this regard.

eG Enterprise offers two specialized monitoring models to monitor different versions of the FortiGate Firewall - the Fortigate Firewall 3x model that performs a thorough, top-down monitoring of the various aspects of performance of FortiGate Firewall v3 (and its variants), and the Fortigate Firewall model that provides indepth insights into the performance of the FortiGate Firewall v4 (and above) .

With the help of both these models, you can keep track of the variations in a wide range of critical performance parameters - from the session activity on the firewall to its resource utilization and its ability to detect attacks. Analysis of the statistics collected enable administrators to proactively detect performance anomalies at the firewall, and promptly initiate remedial measures, so as to ensure continuous firewall availability.

Chapter 2: How does eG Enterprise Monitor Fortigate Firewalls?

To gather the statistics of interest, the eG agent polls the SNMP-MIB of the firewall. To facilitate this data retrieval, SNMP should be enabled on the FortiGate firewall. In order to enable SNMP on FortiGate firewall, do the following:

1. Follow the menu sequence: System>Config> SNMP v1/v2c on the firewall.
2. Select the check box **Enable SNMP** (see Figure 2.1).

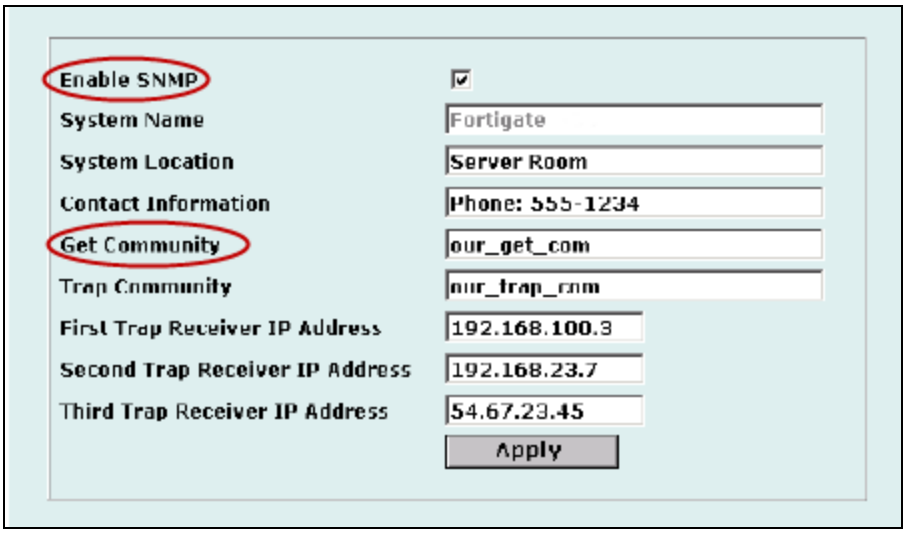

Figure 2.1: Enabling SNMP

3. To retrieve information from SNMP MIB, ensure that you specify a **Get Community** string, which is a password to identify SNMP get requests sent to the FortiGate unit. The default get community string is “public”. You can change the default **Get Community** string if need be (see Figure 2.1).
4. In the Figure 2.1, click the **Apply** button to save the details.

Also, before the eG agent connects to the FortiGate agent, an administrator must configure one or more FortiGate interfaces to accept SNMP connections. The configuration depends upon whether the FortiGate unit is operating in NAT/Route mode or Transparent mode.

In order to configure SNMP access to an interface in **NAT/Route** mode, do the following:

a. Follow the menu sequence: Systems>Network>Interface.

b. Choose an interface that eG agents connect to and select **Modify**.

c. For Administrative Access, select SNMP.

d. Select **OK**.

In order to configure SNMP access to an interface in **Transparent** mode:

a. Follow the menu sequence: System> Network>Management.

b. Select the interface that the SNMP manager connects to and select SNMP.

c. Select **Apply**.

Having enabled the SNMP agent to extract the performance measures from FortiGate Firewall, you can now proceed to configure the eG agent to pull out statistics from the SNMP MIB. The metrics collected by the agent are then presented in the eG monitor interface using the unique Fortigate Firewall or Fortigate Firewall 3x layer model (depending upon the version being monitored).

2.1 Managing the FortiGate Firewall

The eG Enterprise is capable of automatically discovering the FortiGate Firewall. The discovered firewall needs to be managed for monitoring. This can be achieved using the following steps;

1. Log into the eG administrative interface.
2. If a FortiGate Firewall is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page (Infrastructure - > Components - > Manage/Unmanage).
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **COMPONENTS** page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS – MANAGE / UNMANAGE** page. Figure 2.2 and Figure 2.3 clearly illustrate the process of managing the *FortiGate Firewall.*

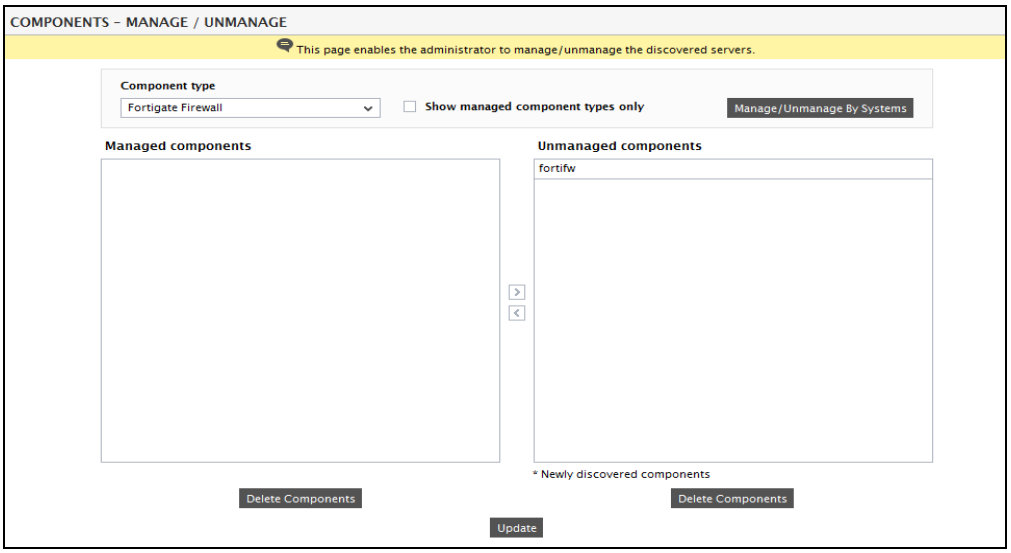

Figure 2.2: Selecting the FortiGate Firewall to be monitored

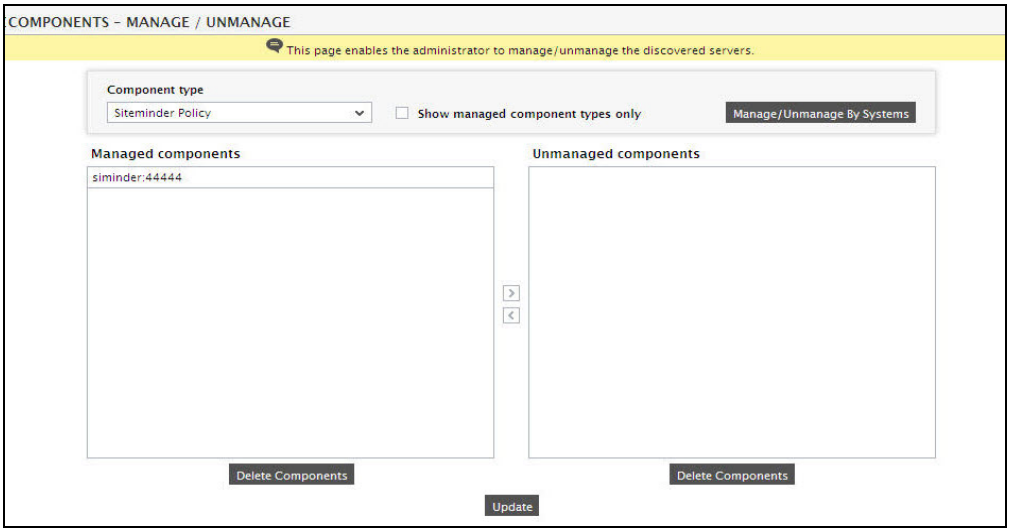

Figure 2.3: Managing the selected FortiGate Firewall

4. Once you managed the FortiGate firewall that is auto- discovered, sign out of the eG administrative interface.

Chapter 3: Monitoring the FortiGate Firewall v3x

Figure 3.1 below depicts the Fortigate Firewall 3x monitoring model offered out-of-the-box by the eG Enterprise Suite. As stated earlier, this model focuses on the overall health of the FortiGate Firewall v3 (and its variants).

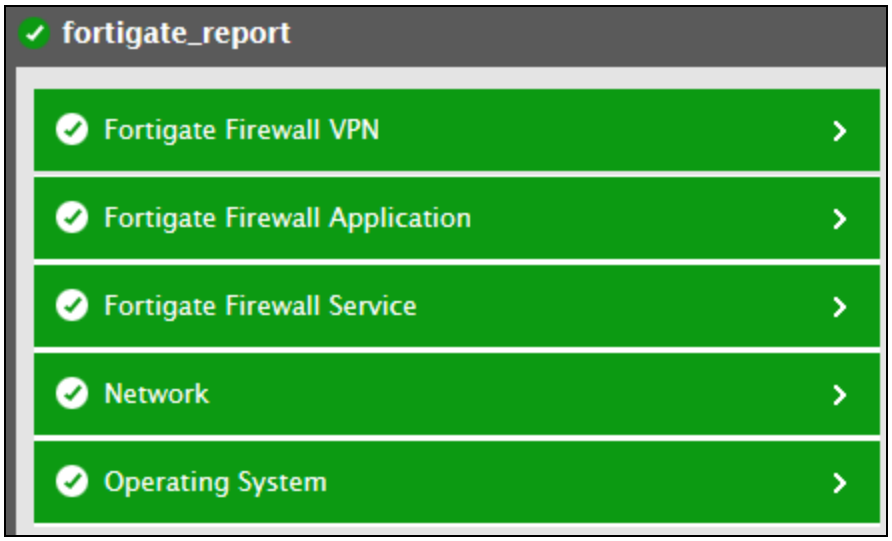

Figure 3.1: Layer model of the FortiGate Firewall

Every layer displayed by Figure 3.1 is mapped to a series of tests, which when executed on the firewall reveals a wealth of performance information pertaining to the firewall. These statistics provide quick and accurate answers to the following frequently asked performance- oriented questions:

- Has the firewall been consuming excessive CPU, memory, and disk resources?
- Are too many sessions currently active on the firewall?
- Is the network and data traffic on the firewall cluster unit very heavy?
- How effective are the anti-virus and IPS mechanisms configured on the firewall cluster unit? Have they been able to detect and prevent all attempted attacks?
- How many packets and data was transmitted/received (processed) for each firewall policy configured on the FortiGate firewall?
- How many intrusions were detected and blocked by the firewall?

- Were signature intrusions detected? If so, how many signature intrusions were detected by the firewall?
- How many HTTP/HTTPS URLs were blocked?
- How many cookies were blocked altogether?
- How many HTTP/HTTPS requests were examined and sent through the web content filter?
- How many HTTP/HTTPS requests were blocked by the web content filter of the firewall?
- What is the current state of each VPN tunnel?
- How well data was transmitted/received through each VPN tunnel?
- What is the current state of each SSL VPN tunnel?
- How many users were logged in through the SSL VPN?
- How many users are currently active on each SSL VPN tunnel?
- How many sessions are currently active on each SSL VPN tunnel?
- What is the rate at which data was transmitted/received for each user through the SSL VPN using the tunnel mode?
- How many users are currently logged in through the SSL VPN using tunnel mode?
- How many users actually logged out of the SSL VPN?
- How many users were registered on the firewall?
- How many users were enabled on the firewall and how many users were actually disabled on the firewall?
- How well memory was utilized by each proxy server on the firewall?
- How many connections were utilized by each proxy server connection?
- What is the maximum number of connection supported by each proxy server?
- How many files were scanned by each scan unit of the firewall?
- How many peer-to-peer connections were blocked and how well data was transmitted using peer-to-peer protocol?
- How well the CPU was utilized by each processor of the firewall?
- How many messages were processed for the Instant Messenger protocol?

- How many files were transferred using the Instant Messenger protocol and how many files were blocked?
- How many connections were blocked while using the Instant messenger protocol?
- How many VOIP connections were currently active on the firewall and how many VOIP connections were blocked?

The sections that follow discuss in detail all other layers except the **Network** layer which has been extensively dealt in the *Monitoring Unix and Windows Servers* document.

3.1 The Operating System Layer

Using the tests mapped to this layer, administrators can monitor the following:

- the CPU, memory, and disk utilization of the FortiGate firewall;
- the CPU utilization of each processor of the firewall;
- the total capacity of each disk partition and the space utilization of each disk partition;

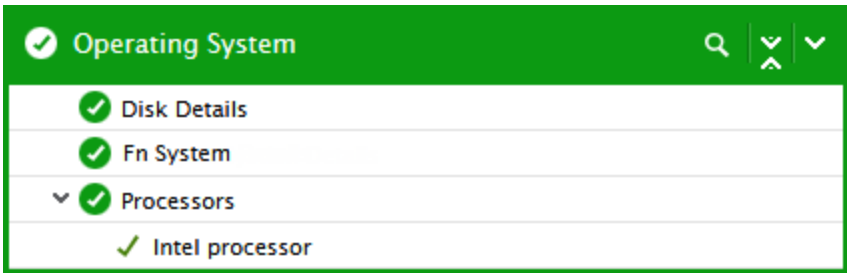

Figure 3.2: The test associated with the Operating System layer

3.1.1 Fn System Test

This test monitors the resource utilization of a FortiGate firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each firewall 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
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
Fortinet CPU usage	This metric represents the current CPU usage of a FortiGate Firewall.	Percent	A value close to 100% indicates a CPU bottleneck on the firewall.
Fortinet memory usage	This metric represents the current memory usage of the firewall.	MB	

Measurement	Description	Measurement Unit	Interpretation
Hard disk capacity	This metric denote the hard disk capacity of the firewall.	MB	
Hard disk usage	This metric denotes the current hard disk usage of the firewall.	MB	
Percent of hard disk utilized	This value is the ratio of the disk usage of the firewall to the total disk capacity, expressed as a percentage.	Percent	A value close to 100% indicates that the hard disk is close to filling up and needs immediate attention.

3.1.2 Processors Test

For each processor of the firewall, this test monitors the current CPU utilization and reports whether/not the firewall is consuming too much CPU resources.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the desired **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each processor of the target 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
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 • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percentage of CPU utilized by this processor of the firewall.	Percentage	A value close to 100% is a cause of concern.

3.2 The Fortigate Firewall Service Layer

The tests mapped to this layer (see Figure 3.3), monitor:

- the session activity on the firewall;
- the resource utilization, network traffic, session activity, and the extent of protection delivered by the firewall cluster unit;

- the number of files scanned by the scan unit of the firewall;
- the number of virus transmissions detected over HTTP;
- the number of virus transmissions blocked over HTTP and SMTP;
- the number of virus transmissions blocked over FTP and Instant Messsenger protocol;
- the total number of virus transmissions blocked;
- the status of each sensor on the firewall;

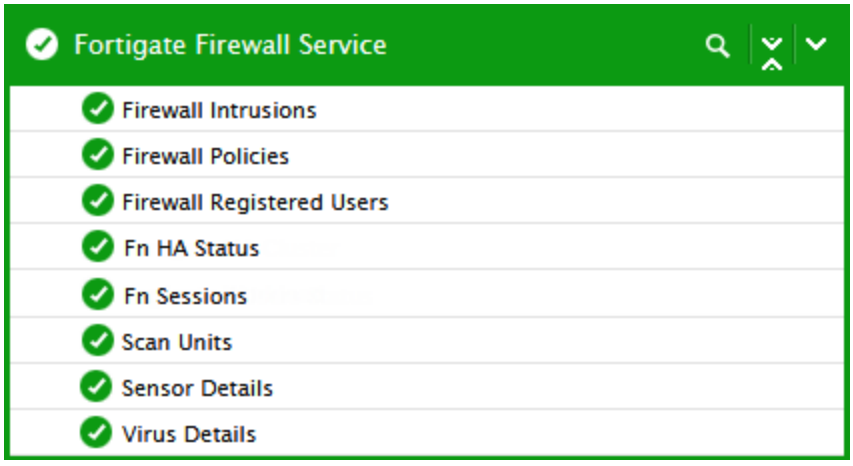

Figure 3.3: The tests associated with the Fortigate Firewall Service layer

3.2.1 Fn HA Status Test

This test monitors the various statistics of interest regarding a high availability FortiGate firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each firewall monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is

Parameter	Description
	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 • **SHA** – Secure Hash Algorithm

Parameter	Description
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
Cpu usage of cluster unit	This metric represents the current CPU usage of a unit of the firewall cluster.	Percent	
Memory usage of cluster unit	This metric represents the current memory usage of the firewall cluster unit.	MB	
Network usage of cluster unit	This metric indicates the current network utilization of the firewall cluster unit.	KB/Sec	

Measurement	Description	Measurement Unit	Interpretation
Network traffic handled by cluster unit	This metric is the rate of packets processed by the firewall cluster unit during the last measurement period.	Packets/sec	
Data traffic through cluster unit	This metric is the data traffic handled by the firewall cluster unit during the last measurement period, expressed in KB.	KB	
Active sessions to cluster unit	This metric is the current active sessions to the firewall cluster unit.	Number	
Virus attacks detected	This value is the number of attacks that the IPS detected in the last 20 hours.	Number	
Viruses detected by cluster unit	This value is the number of viruses the anti-virus system detected in the last 20 hours.	Number	

3.2.2 Sensor Details Test

This test reports the current state of each sensor on the Fortigate firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor on the 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 host for which this test is to be configured.

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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>
Note:
Typically, this measure will report one of the Measure Values listed in the table above to indicate the current sensor state. However, in the graph of this measure, the sensor state will be depicted using the corresponding numeric equivalents only.</td></tr>
</table>

3.2.3 Virus Details Test

The true test of the effectiveness of a firewall lies in its ability to detect and protect the system from malicious virus attacks. Using the metrics reported by the **Virus Details** test, you can assess the efficiency of the Fortigate firewall, as it reports the number of viruses detected and blocked by the firewall per protocol it supports.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.

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

Parameter	Description
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
HTTP Virus Detected	Indicates the number of virus transmissions over HTTP detected in the virtual domain in the last measurement period.	Number	
HTTP Virus Blocked	Indicates the number of virus transmissions over HTTP blocked in the virtual domain in the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
SMTP Virus Detected	Indicates the number of virus transmissions over SMTP detected in the virtual domain in the last measurement period.	Number	
SMTP Virus Blocked	Indicates the number of virus transmissions over SMTP detected in the virtual domain in the last measurement period.	Number	
POP3 Virus Detected	Indicates the number of virus transmissions over POP3 detected in the virtual domain in the last measurement period.	Number	
POP3 Virus Blocked	Indicates the number of virus transmissions over POP3 blocked in the virtual domain in the last measurement period.	Number	
IMAP Virus Detected	Indicates the number of virus transmissions over IMAP detected in the virtual domain in the last measurement period.	Number	
IMAP Virus Blocked	Indicates the number of virus transmissions over IMAP blocked in the virtual domain in the last measurement protocol.	Number	
FTP Virus Detected	Indicates the number of virus transmissions over FTP detected in the virtual domain in the last measurement period.	Number	
FTP Virus Blocked	Indicates the number of virus transmissions over	Number	

Measurement	Description	Measurement Unit	Interpretation
	FTP blocked in the virtual domain in the last measurement period.		
IM Virus Detected	Indicates the number of virus transmissions over IM protocols detected in the virtual domain in the last measurement period.	Number	
IM Virus Blocked	Indicates the number of virus transmissions over IM protocols blocked in the virtual domain in the last measurement period.	Number	
NNTP Virus Detected	Indicates the number of virus transmissions over NNTP detected in the virtual domain in the last measurement period.	Number	
NNTP Virus Blocked	Indicates the number of virus transmissions over NNTP blocked in the virtual domain in the last measurement period.	Number	
Total Virus Detected	Indicates the total number of virus transmissions detected in the virtual domain in the last measurement period.	Number	
Total Virus Blocked	Indicates the total number of virus transmissions blocked in the virtual domain in the last measurement period.	Number	

3.2.4 Fn Sessions Test

This test monitors the session activity to a FortiGate firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each firewall monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current sessions for Fortinet service	Indicates the number of sessions currently supported by the firewall.	Number	

3.2.5 Firewall Registered Users Test

This test reports the number of users registered on the firewall and the users who are enabled/disabled on the firewall. Using this test, administrators can figure out the users who are disabled on the firewall i.e., the users who are prohibited from accessing the target environment. This way, the firewall helps in securing the target environment from unauthorized accesses.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
	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 • **AES** – Advanced Encryption Standard

Parameter	Description
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**.
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
Registered users	Indicates the total number of users registered on the firewall.	Number	Registered users are alone allowed to initiate VPN tunneling activities.
Enabled users	Indicates the number of users currently enabled on the firewall during the last measurement period.	Number	The detailed diagnosis of this measure lists the name of the users who are currently enabled on the firewall.
Disabled users	Indicates the number of	Number	The detailed diagnosis of this measure

Measurement	Description	Measurement Unit	Interpretation
	users currently disabled on the firewall during the last measurement period.		lists the name of the users who are currently disabled on the firewall.

3.2.6 Scan Units Test

Using an *antivirus* profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unit supports SSL/SSH content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions. Antivirus scanning is configured in an AntiVirus profile, but it is enabled in a firewall policy. Once the use of an AntiVirus profile is enabled and selected in one or more firewall policies, all the traffic controlled by those firewall policies will be scanned according to the settings in that profile. Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action. Multiple scan units can be configured for antiviru scanning. If the antivirus scanning is not performed or if the scan unit is not configured for antivirus scanning, then there may be a chance for the target environment to be exposed to malware/trojans. Critical information in the target environment when exposed to malware/trojans may lead to loss of confidential data resulting in greater losses. Therefore it is essential to monitor the scan units of the FortiGate firewall round the clock. The **Scan Units** test helps administrators in this regard!

This test auto-discovers the scan units of the target FortiGate firewall and for each scan unit, this test reports the number of files scanned. This way, administrators can keep track on the number of files scanned in the target environment.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each scan unit of the target 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 host for which this test is to be configured.

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

3.2.7 Firewall Policies Test

The security policy of your organization is a set of definitions to protect your computer network and the information that goes through it. The Fortigate firewall denies all packets that are not specifically

allowed. When you add a policy to your firewall device configuration file, you add a set of rules that tell the firewall device to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

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

For each firewall policy that is configured, this test monitors the number of packets and the amount of data traffic through the firewall. This way, this test helps the administrators in identifying the firewall policy through which the maximum number of packets/data was transmitted/received.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each security policy created on the target firewall monitored.

Configurable parameters for the test

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Packets processed	Indicates the number of packets processed (transmitted/received) for this security policy.	Number	Comparing the values of these measures across the policies helps you in identifying the policy through which the number of packets transmitted/received was the maximum at any point of time.
Data processed	Indicates the amount of data processed (transmitted/received) for this security policy.	MB	Comparing the values of these measures across the policies helps you in identifying the policy through which the data traffic was the maximum at any point of time.

3.2.8 Firewall Intrusions Test

An IPS is an Intrusion Prevention System for networks. While early systems focused on intrusion detection, the continuing rapid growth of the Internet, and the potential for the theft of sensitive data, has resulted in the need for not only detection, but prevention. The FortiGate IPS detects intrusions by using attack signatures for known intrusion methods, and detects anomalies in network traffic to identify new or unknown intrusions. Not only can the IPS detect and log attacks, but users can choose actions to take on the session when an attack is detected. Often, administrators may want to keep close track on the intrusions and figure out the behavioral pattern of the intrusions so that attacks can be detected at the earliest. The Firewall Intrusions test helps administrators in this regard.

By closely monitoring the FortiGate IPS, administrators can keep track on the number of intrusions detected and blocked by the IPS, the number of intrusions detected based on severity (critical/high/medium) and the number of intrusions detected using attack signatures.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

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
Intrusions detected	Indicates the number of intrusions (malicious attacks) detected by the firewall.	Number	
Intrusions blocked	Indicates the number of intrusions blocked by the firewall.	Number	
Critical severity intrusions detected	Indicates the number of critical severity intrusions that were detected by the firewall.	Number	
High severity intrusions detected	Indicates the number of high severity intrusions that were detected by the firewall.	Number	
Medium severity intrusions detected	Indicates the number of medium severity intrusions that were detected by the firewall.	Number	
Signature intrusions detected	Indicates the number of signature intrusions that were detected by the firewall.	Number	

3.3 The FortiGate Firewall Application Layer

Using the tests mapped to this layer, administrators can figure out the following:

- the number of messages processed for the Instant Messenger protocol;
- the count of the files that were transferred using the Instant Messenger protocol the count of the files that were blocked;
- the count of the connections blocked while using the Instant messenger protocol;

- the number of VOIP connections that were currently active on the firewall and the number of VOIP connections that were blocked;
- the number of peer-to-peer connections that were blocked and the amount of data transmitted using peer-to-peer protocol;
- the memory utilized by each proxy server on the firewall;
- the number of connections utilized by each proxy server connection;
- the maximum number of connection supported by each proxy server;

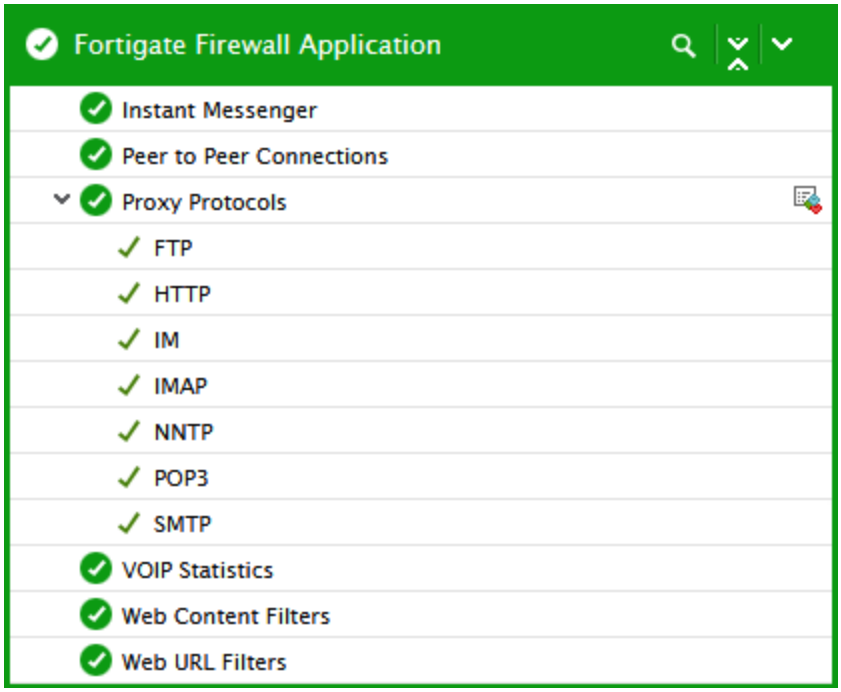

Figure 3.4: The tests associated with the FortiGate Firewall Application layer

3.3.1 Web URL Filters Test

Web filtering is a means of controlling the content that an Internet user is able to view. With the popularity of web applications, the need to monitor and control web access is becoming a key component of secure content management systems that employ antivirus, web filtering, and messaging security. Important reasons for controlling web content include:

- lost productivity because employees are accessing the web for non-business reasons
- network congestion — when valuable bandwidth is used for non-business purposes, legitimate business applications suffer

- loss or exposure of confidential information through chat sites, non-approved email systems, instant messaging, and peer-to-peer file sharing
- increased exposure to web-based threats as employees surf non-business-related web sites
- legal liability when employees access/download inappropriate and offensive material
- copyright infringement caused by employees downloading and/or distributing copyrighted material.

As the number and severity of threats increase on the World Wide Web, the risk potential increases within a company's network as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation as hostile environments have been created by employees who download and view offensive content. Web-based attacks and threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:

- spyware/grayware
- phishing
- pharming
- instant messaging
- peer-to-peer file sharing
- streaming media
- blended network attacks.

The methods available for monitoring and controlling Internet access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control web activity.

Common web access control mechanisms include:

- establishing and implementing a well-written usage policy in the organization on proper Internet, email, and computer conduct
- installing monitoring tools that record and report on Internet usage
- implementing policy-based tools that capture, rate, and block URLs.

The FortiGate unit applies web filters in a specific order:

- URL filter
- FortiGuard Web Filter

- web content filter
- web script filter
- antivirus scanning.

The FortiGate firewall blocks the URLs that are mentioned in the URL filter list. The firewall is not only capable of blocking the URLs but also blocks the applets, cookies and Activex controls of the URLs in an active manner. Administrators can keep track on the number of hits to the blocked URLs using the **Web URL Filters** test.

By closely monitoring the FortiGate firewall, administrators can figure out the number of HTTP/HTTPS URLs that were blocked by the firewall as well as the number of applets, cookies and ActiveX controls of the URLs. This way, unwanted URLs can be blocked and the bandwidth consumption can be kept under check thus helping administrators maintain a prudent infrastructure at ease!

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2

Parameter	Description
	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 • **AES** – Advanced Encryption Standard

Parameter	Description
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
HTTP URLs blocked	Indicates the number of HTTP URLs that were blocked by the firewall.	Number	
HTTPS URLs blocked	Indicates the number of SSL enabled HTTP URLs that were blocked by the firewall.	Number	
ActiveX objects blocked	Indicates the number of ActiveX objects that were blocked by the firewall.	Number	
Applets blocked	Indicates the number applets that were blocked by the firewall.	Number	
Cookies blocked	Indicates the number of cookies that were blocked by the firewall.	Number	

3.3.2 Instant Messenger Test

Using the Application Control Security Profile feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

Fortinet is constantly adding to the list of applications detected through maintenance of the FortiGuard Application Control Database. This database is part of the FortiGuard Intrusion Protection System Database because intrusion protection protocol decoders are used for application control and both of these databases have the same version number.

Enabling the application control security profile helps administrators to block messages communicated through the instant messenger protocol. To understand the pattern of messages sent through the instant messenger protocol and how well the files that were sent through the instant messenger protocol were blocked, administrators can use the **Instant Messenger** test offered by the eG Enterprise!

This test reports the number of messages that were processed through the instant messenger protocol and throws light on the files that were transferred using the instant messenger protocol. In addition, this test reports the number of files that were blocked by the firewall while being transferred and the connections that were blocked to the instant messenger. Using this test, administrators can figure out ho w well the firewall blocks the instant messages in the target environment.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
	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
Messages processed	Indicates the number of messages processed for the Instant Messenger	Number	

Measurement	Description	Measurement Unit	Interpretation
	protocol.		
Files transferred	Indicates the number of files transferred using the Instant Messenger protocol.	Number	
Blocked files transferred	Indicates the number of files that were blocked while being transferred using the Instant Messenger protocol.	Number	
Blocked connections	Indicates the number of connections that were blocked using the Instant Messenger protocol.	Number	

3.3.3 Web Content Filters Test

You can control web content by blocking access to web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can also add words, phrases, patterns, wild cards and Perl regular expressions to match content on web pages. You can add multiple web content filter lists and then select the best web content filter list for each web filter profile.

Enabling web content filtering involves three separate parts of the FortiGate configuration.

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day.
- The web filter profile specifies what sort of web filtering is applied.
- The web content filter list contains blocked and exempt patterns.

The web content filter feature scans the content of every web page that is accepted by a security policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than a threshold set in the web filter profile, the FortiGate unit blocks the page.

By closely monitoring the target environment guarded by the FortiGate firewall, administrators can actually figure out the health of the web content filter of the firewall. The number of HTTP/HTTPS requests examined, allowed and blocked helps administrators figure out the efficiency of the web content filter. The higher the ratio of the HTTP requests blocked indicates that the firewall is put to the maximum use in the target environment by the administrators to prevent malicious attacks, unwanted browsing under check and maintain optimal utilization of the resources in the target environment.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
HTTP requests examined	Indicates the number of HTTP requests that were examined by the web content filter of the firewall.	Number	
HTTPS requests examined	Indicates the number of SSL enabled HTTPS request that were examined by the web content filter of the firewall.	Number	
HTTP requests allowed	Indicates the number of HTTP requests that were allowed by the web content filter of the firewall.	Number	
HTTPS requests allowed	Indicates the number of SSL enabled HTTP requests that were allowed by the web content filter of the firewall.	Number	
HTTP requests blocked	Indicates the number of HTTP requests that were blocked by the web content filter of the firewall.	Number	
HTTPS requests blocked	Indicates the number of SSL enabled HTTP requests that were blocked by the web content filter of the firewall.	Number	

Measurement	Description	Measurement Unit	Interpretation
HTTP requests blocked ratio	Indicates the ratio of HTTP requests that were blocked to the HTTP requests that were examined, in percentage.	Percentage	This measure is obtained using the formulae: (HTTP requests blocked/HTTP requests examined)*100
HTTPS requests blocked ratio	Indicates the ratio of SSL enabled HTTP requests that were blocked to the SSL enabled HTTP requests that were examined, in percentage.	Percentage	This measure is obtained using the formulae: (HTTPS requests blocked/HTTPS requests examined)*100

3.3.4 Peer to Peer Connections Test

In large environment where thousands of employees access the internet at the same time, administrators may want to keep a check on the utilization of the internet bandwidth. Therefore, administrators may use a security policy on the FortiGate firewall to block peer to peer connections that are considered as one of the primary reasons for the depleting internet bandwidth. P2P traffic can be blocked via Web filtering, URL filtering and app control, or any combination of all three. Administrators may want to keep track on the data transmitted through peer to peer connections so that they can learn the bandwidth usage pattern of the employees and provide optimal resources to all the employees of the organization. This is where the **Peer to Peer Connections** test helps!

This test reports the number of peer to peer connections blocked and the amount of data transmitted over the network using the peer to peer protocol. Using this test administrators can determine the pattern of data traffic over the peer to peer protocol and take remedial measures to optimize the internet bandwidth consumption.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target firewall 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
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
Blocked P2P connections	Indicates the number of peer to peer connections that were blocked by the firewall.	Number	
Data transmitted on P2P protocol	Indicates the amount of data transmitted on the	KB	By analyzing the pattern of this measure over a period of time helps

Measurement	Description	Measurement Unit	Interpretation
	peer to peer protocol of the firewall.		administrators to optimize the internet bandwidth consumption in the target environment.

3.3.5 VOIP Statistics Test

To enhance the security of the target environment, security policies can be applied to the FortiGate firewall to block VoIP connections. The VOIP Statistics test helps administrators to keep track on the VoIP calls that were blocked by the firewall.

This test monitors the VoIP connections through the firewall and reports the number of VoIP connections to the firewall and the number of VoIP calls that were blocked by the firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2

Parameter	Description
	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 • **AES** – Advanced Encryption Standard

Parameter	Description
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
Current VOIP connections	Indicates the number of VOIP connections that are currently active on the firewall.	Number	
Blocked VOIP calls	Indicates the number of VOIP calls that were blocked by the firewall.	Number	

3.3.6 Proxy Protocols Test

The FortiGate firewall can explicitly block specific traffic generated through various proxy protocols such as HTTP, HTTPS, FTP etc. Often administrators of large environments may want to figure out the protocol that is transferring the maximum number of requests through the firewall to the target environment. This analysis may help the administrators to figure out the protocol and block requests from that protocol. The Proxy Protocols test helps administrators in this regard!

This test auto-discovers the proxy protocols that are communicating with the target environment though the firewall and for each protocol, reports the memory utilization and the number of requests processed by the protocol. In addition, this test throws light on the maximum connections that can be handled by each protocol and the percentage of connections that were utilized by the protocol. This

way, administrators can figure out the protocol that is responsible for the abnormal traffic through the firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
	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 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
Proxy memory usage	Indicates the percentage of memory utilized by this proxy server.	Percentage	Comparing the value of this measure across the protocol servers helps administrators to identify the proxy protocol server that is utilizing the maximum amount of memory.
Requests processed by proxy	Indicates the number of requests processed by this proxy server.	Number	
Current proxy connections	Indicates the number of proxy connections created by this proxy server.	Number	
Maximum connections supported by proxy	Indicates the maximum number of connections that can be supported by this proxy server.	Number	
Proxy connections usage	Indicates the percentage of connections that were utilized by this proxy server.	Percent	

3.4 The FortiGate Firewall VPN Layer

The tests mapped to this layer (see Figure 3.5), monitor:

- the current state of each VPN tunnel;
- the amount of data transmitted/received through each VPN tunnel;
- the current state of each SSL VPN tunnel;
- the count of the users logged in through the SSL VPN;
- the number of users currently active on each SSL VPN tunnel;
- the number of sessions currently active on each SSL VPN tunnel;
- the rate at which data was transmitted/received for each user through the SSL VPN using the tunnel mode;

- the number of users are currently logged in through the SSL VPN using tunnel mode;
- the number of users actually logged out of the SSL VPN;

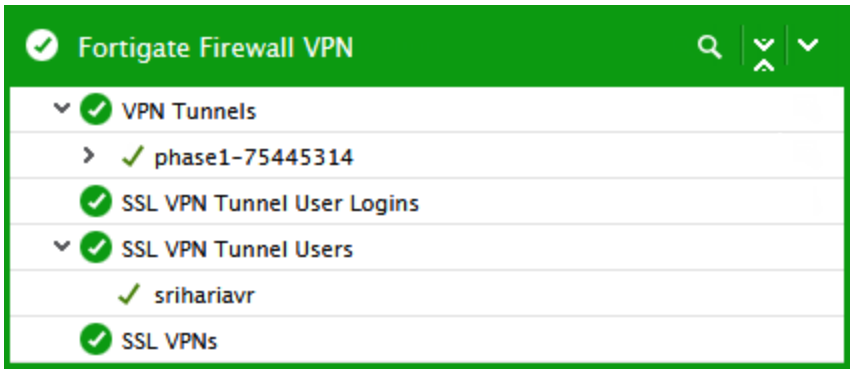

Figure 3.5: The tests associated with the Fortigate Firewall VPN layer

3.4.1 SSL VPN Tunnel Users Test

For each user logging into the corporate network through the SSL VPN using the tunnel mode, this test monitors the data traffic flowing through the FortiGate firewall. This way, administrators can figure out the user who is transmitting/receiving the maximum amount of data and further analyze if the traffic to the user is malicious or genuine.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each user connecting through the SSL VPN using the tunnel mode on the target 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data received	Indicates the rate at which data was received for this user through the SSL VPN using the tunnel mode.	KB/sec	Comparing the value of this measure across the users helps in identifying the user who is receiving the maximum data.
Data transmitted	Indicates the rate at which data was transmitted for this user through the SSL VPN using the tunnel mode.	KB/sec	Comparing the value of this measure across the users helps in identifying the user who is transmitting the maximum data.

3.4.2 SSL VPN Tunnel User Logins Test

In large high secure environments, administrators may want to check if remote users could login to their network in a hassle free manner. Sometimes, users may not be able to login to the target

environment due to connectivity issues in the firewall. This may in turn affect the productivity of the users. Therefore, it is important for the administrators to monitor the user logins to the corporate network through the SSL VPN using the FortiNet client i.e., tunnel mode. The **SSL VPN Tunnel User Logins** test helps administrators in this regard!

Using this test, administrators can figure out the number of users who have recently logged in to the SSL VPN through the tunnel mode, the users who have logged in from the start of the firewall and the users who have recently logged out of the network. The detailed diagnosis of this test helps administrators to track session level information of the users and the time duration for which the users have logged in through the firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

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

Parameter	Description
	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**.
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
Users currently loggedin	Indicates the number of users currently logged into the SSL VPN through the tunnel mode.	Number	The detailed diagnosis of this measure lists the name of the users, the login time for each user and the session duration of each user.
New users	Indicates the number of new users logged into the SSL VPN through the tunnel mode during the last measurement period.	Number	The detailed diagnosis of this measure lists the names of the users who were recently logged into the firewall.
Recently loggedout users	Indicates the number of user logged out of the SSL VPN during the last measurement period.	Number	The detailed diagnosis of this measure lists the name of the users, the login time of the user, the logout time of the user and the session duration of the user.

3.4.3 VPN Tunnels Test

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

Using the FortiGate Firewall, administrators can configure multiple VPN tunnels based on the volume of data traffic handled by their network and the security/privacy requirements of the network. Often bandwidth management can be enabled on the firewall configurations to prevent unauthorized access to the network and to optimize the usage of network resources. Improper firewall configurations can therefore result in a few VPN tunnels hogging the bandwidth resources and choking the network! To avoid this, administrators should periodically check the efficacy of the firewall configuration, identify the issues in the firewall settings and rectify the same! This is where the VPN Tunnels test helps! This test auto discovers the VPN tunnels configured using the FortiGate Firewall and reports the status of each tunnel. This test also closely monitors the amount of data traffic sent and received via every tunnel. In the process, the test accurately points to that tunnel that is handling an abnormally high volume of traffic and is hence hogging the bandwidth resources available to the network! This way, the test enables administrators to understand whether/not their firewall configurations are effective, and if not, initiate measures to fine-tune them.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each VPN tunnel created on the target 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
VPN tunnel status	Indicates the current state of this VPN tunnel.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Up – 2 Down – 1 **Note:** By default, this measure reports the Measure Values listed in the table

Measurement	Description	Measurement Unit	Interpretation
			above to indicate the current state of this VPN tunnel. The graph of this measure however is represented using the numeric equivalents only - 0 or 1.
Data transmitted	Indicates the amount of data transmitted through this VPN tunnel.	KB	Comparing the value of this measure across tunnels helps you to identify the tunnel that is transmitting the maximum amount of data.
Data received	Indicates the amount of data received through this VPN tunnel.	KB	Comparing the value of this measure across tunnels helps you to identify the tunnel that is receiving the maximum amount of data.

3.4.4 SSL VPNs Test

Remote users access the corporate network using an SSL VPN, connecting either by web mode using a web browser or tunnel mode using FortiClient.

Web mode allows users to access network resources, such as the Internal Segmentation Firewall (ISFW). For users connecting via tunnel mode, traffic to the internet will flow through the FortiGate so that security scanning can be applied to this traffic. During the connecting phase, the FortiGate also verifies whether the remote user's antivirus software is installed and up-to-date.

If the SSL VPN is misconfigured or does not function as expected, then, remote users could not login to the corporate network. This would in turn affect the productivity of the users who work from home, affect the users who would need critical information available only on the corporate network etc. Therefore it is necessary to monitor the SSL VPN of the FortiGate firewall round the clock. The **SSL VPNs** test helps administrators on this regard!

Using this test administrators can figure out the current status of the SSL VPN. In addition, administrators can also figure out the users who are active on the SSL VPN using the web mode and tunnel mode. The sessions that were initiated by the users on the SSL VPN through the web mode and tunnel mode can also be tracked besides tracking the maximum number of users and sessions on the SSL VPN. This way, abnormalities can be detected and preemptive measures can be initiated before users face issuesin accessing the corporate network.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
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
SSL VPN status	Indicates the current state		The values reported by this measure

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>of the SSL VPN.</td><td></td><td>and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>Disabled</td><td>1</td></tr><tr><td>Enabled</td><td>2</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the SSL VPN. The graph of this measure however is represented using the numeric equivalents only - 1 or 2.</td></tr>
<tr><td>Users logged</td><td>Indicates the number of users logged in through the SSL VPN.</td><td>Number</td><td></td></tr>
<tr><td>Active tunnel users</td><td>Indicates the number of users currently active on the SSL VPN through the tunnel mode.</td><td>Number</td><td></td></tr>
<tr><td>Active web users</td><td>Indicates the number of web users currently active on the SSL VPN through the web mode.</td><td>Number</td><td></td></tr>
<tr><td>Max users logged - High mark</td><td>Indicates the maximum number of users logged in using the SSL VPN since the start of the firewall.</td><td>Number</td><td></td></tr>
<tr><td>Total active sessions</td><td>Indicates the total number of sessions that are active on the SSL VPN.</td><td>Number</td><td></td></tr>
<tr><td>Active tunnel sessions</td><td>Indicates the number of sessions that are currently active on the SSL VPN using the tunnel</td><td>Number</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	mode.		
Active web sessions	Indicates the number of sessions that are currently active on the SSL VPN using the web mode.	Number	
Max sessions logged - High mark	Indicates the maximum number of sessions logged in using the SSL VPN since the start of the firewall.	Number	

Chapter 4: Monitoring the Fortigate Firewall v4 (and above)

Figure 4.1 below depicts the Fortigate Firewall monitoring model offered out-of-the-box by the eG Enterprise Suite. As stated earlier, this model focuses on the overall health of the FortiGate Firewall v4 (and its variants).

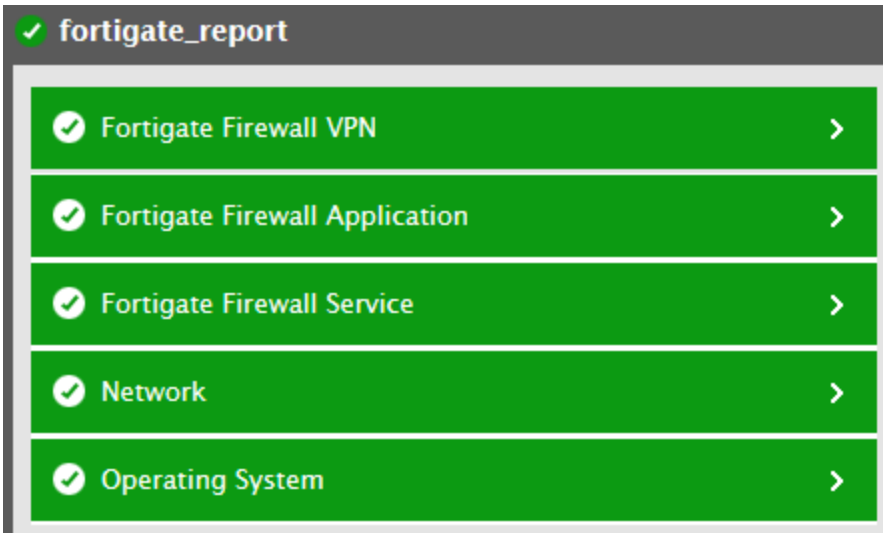

Figure 4.1: Layer model of the FortiGate Firewall

Every layer displayed by Figure 4.1 is mapped to a series of tests, which when executed on the firewall reveals a wealth of performance information pertaining to the firewall. These statistics provide quick and accurate answers to the following frequently asked performance-oriented questions:

- Has the firewall been consuming excessive CPU, memory, and disk resources?
- Are too many sessions currently active on the firewall?
- Is the network and data traffic on the firewall cluster unit very heavy?
- How effective are the anti-virus and IPS mechanisms configured on the firewall cluster unit? Have they been able to detect and prevent all attempted attacks?
- How many packets and data was transmitted/received (processed) for each firewall policy configured on the FortiGate firewall?
- How many intrusions were detected and blocked by the firewall?

- Were signature intrusions detected? If so, how many signature intrusions were detected by the firewall?
- How many HTTP/HTTPS URLs were blocked?
- How many cookies were blocked altogether?
- How many HTTP/HTTPS requests were examined and sent through the web content filter?
- How many HTTP/HTTPS requests were blocked by the web content filter of the firewall?
- What is the current state of each VPN tunnel?
- How well data was transmitted/received through each VPN tunnel?
- What is the current state of each SSL VPN tunnel?
- How many users were logged in through the SSL VPN?
- How many users are currently active on each SSL VPN tunnel?
- How many sessions are currently active on each SSL VPN tunnel?
- What is the rate at which data was transmitted/received for each user through the SSL VPN using the tunnel mode?
- How many users are currently logged in through the SSL VPN using tunnel mode?
- How many users actually logged out of the SSL VPN?
- How many users were registered on the firewall?
- How many users were enabled on the firewall and how many users were actually disabled on the firewall?
- How well memory was utilized by each proxy server on the firewall?
- How many connections were utilized by each proxy server connection?
- What is the maximum number of connection supported by each proxy server?
- How many files were scanned by each scan unit of the firewall?
- How many peer-to-peer connections were blocked and how well data was transmitted using peer-to-peer protocol?
- How well the CPU was utilized by each processor of the firewall?
- How many messages were processed for the Instant Messenger protocol?

- How many files were transferred using the Instant Messenger protocol and how many files were blocked?
- How many connections were blocked while using the Instant messenger protocol?
- How many VOIP connections were currently active on the firewall and how many VOIP connections were blocked?

Since most of the tests mapped to the Fortigate Firewall component have already been dealt with the Fortigate Firewall 3x component, let us now discuss the tests applicable for the Fortigate Firewall compoennt alone. This chapter will not cover the **Network** layer as this layer has been extensively dealt in the *Monitoring Unix and Windows Servers* document.

4.1 The Operating System Layer

Using the tests mapped to this layer, administrators can monitor the following:

- the CPU, memory, and disk utilization of the FortiGate firewall;
- the CPU utilization of each processor of the firewall;
- the total capacity of each disk partition and the space utilization of each disk partition;

Figure 4.2: The tests mapped to the Operating System layer

4.1.1 Disk Details Test

This test monitors the disk space usage of each disk partition supported by the firewall, points you to partitions that are over-utilizing disk space, and thus proactively alerts you to potential space contentions.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
	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 capacity	This metric represents the total capacity of this disk partition.	MB	

Measurement	Description	Measurement Unit	Interpretation
Disk space usage	This metric represents the current usage of space in this disk partition.	MB	A consistent increase in the value of this measure could indicate that the disk space is getting slowly but steadily eroded. Compare the value of this measure across partitions to identify the partitions that are utilizing disk space excessively.
Disk space used	Indicates the percentage of space in this disk partition that is currently utilized.	Percent	A consistent increase in the value of this measure could indicate that the disk space is getting slowly but steadily eroded. Compare the value of this measure across partitions to identify the partitions that are utilizing disk space excessively.
Free disk space	Indicates the percentage space in this disk partition that is currently free.	Percent	A high value is typically desired for this measure. A very low often is indicative of abnormal space utilization.

4.1.2 Fn System Test

This test monitors the resource utilization of a FortiGate firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each firewall monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.

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

Parameter	Description
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
CPU utilization	Indicates the current CPU usage of the FortiGate Firewall.	Percent	A value close to 100% indicates a CPU bottleneck on the firewall.
Memory utilization	Indicates the current memory usage of the firewall.	Percent	A value close to 100% indicates that the memory is close to filling up and needs immediate attention.
Total configured memory	This metric denote the hard disk capacity of the firewall.	GB	

Measurement	Description	Measurement Unit	Interpretation
Used memory	This metric denotes the current hard disk usage of the firewall.	GB	

4.1.3 CPU Details Test

This test monitors the CPU and memory usage of the firewall and proactively alerts you to potential resource contentions.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the current CPU usage of the firewall.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the CPU usage of the firewall. A consistent increase however could indicate a gradual, yet steady erosion of CPU resources, and is hence a cause for concern.
Current memory utilization	Indicates the current memory usage of the firewall.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the memory usage of the firewall. A consistent increase however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
Total memory	Indicates the current memory capacity of the firewall.	KB	

4.2 The Network Layer

The tests mapped to this layer reveal the following anomalies:

a. Unscheduled reboots of the firewall
b. Non-availability of the firewall over the network
c. Latencies when connecting to the firewall over the network

d. Abnormal speed of and unusual bandwidth usage by the network interfaces supported by the firewall

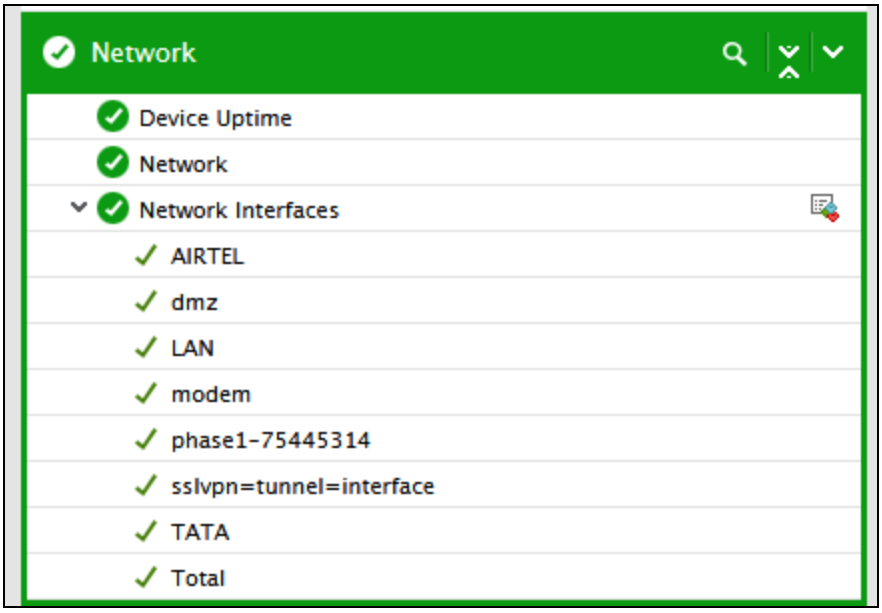

Figure 4.3: The tests mapped to the Network layer of the Fortigate Firewall component

The tests mapped to this layer are elaborately discussed in the *Monitoring Cisco Router* document, let us proceed to look at the next layer.

4.3 The FortiGate Firewall Service Layer

The tests mapped to this layer monitor the following:

- The resource usage of, the network traffic handled by, and the session load on each Fortigate unit in an High Availability Fortigate cluster;
- The current state of user accounts on the firewall;
- The current state of the sensors on the firewall;
- The count of viruses detected and blocked by the firewall
- the number of files scanned by the scan unit of the firewall;
- the statistics of the packets and data that were transmitted/received (processed) for each firewall policy configured on the FortiGate firewall;
- the count of the sessions currently active on the firewall;

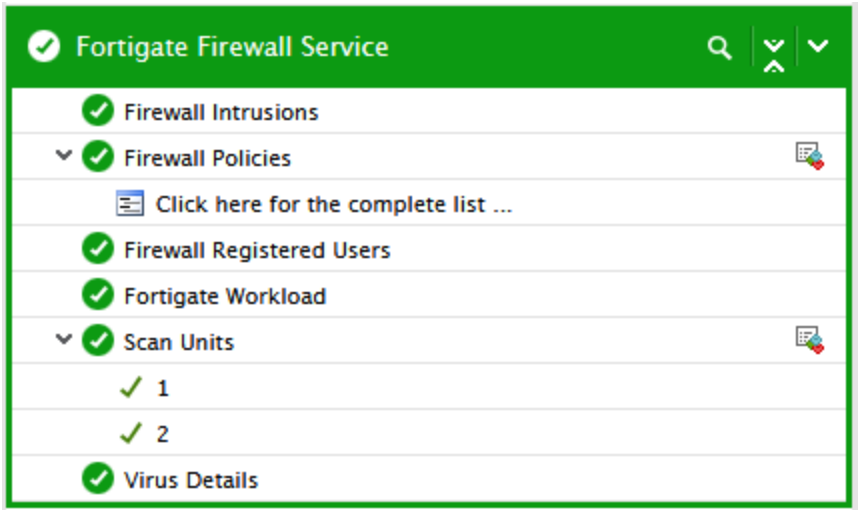

Figure 4.4: The tests mapped to the Fortigate Firewall Service layer

4.3.1 Fortigate HA Cluster Test

FortiGate high availability (HA) provides a solution for two key requirements of critical enterprise networking components: enhanced reliability and increased performance. FortiGate HA consists of two or more FortiGate units operating as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewall, VPN, IPS, virus scanning, web filtering, and spam filtering services.

Inside the cluster the individual FortiGate units are called cluster units. These cluster units share state and configuration information. If one cluster unit fails, the other units in the cluster automatically replace that unit, taking over the work that the failed unit was doing. The cluster continues to process network traffic and provide normal FortiGate services with virtually no interruption. The ability of an HA cluster to continue providing firewall services after a failure, is called failover.

A second HA feature, called load balancing, can be used to increase firewall performance. A cluster of FortiGate units can increase overall network performance by sharing the load of processing network traffic and providing security services. Periodically, you may want to check the network traffic processed by each cluster unit, so as to assess the efficiency with which the HA cluster balances load, isolate overloaded units, and thereby spot load balancing irregularities (if any) early.

The **Fortigate HA Cluster** test enables you to achieve this end. This test monitors each Fortigate unit in an HA cluster, reports the resource usage of each unit, and also tracks the network traffic processed by every unit, so that resource-hungry and overloaded units can be quickly identified.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each cluster unit monitored.

Configurable parameters for the test

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

Parameter	Description
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
Cpu utilization	This metric represents the current CPU usage of this unit of the firewall cluster.	Percent	A value close to 100% indicates a CPU bottleneck on a cluster unit. Compare the value of this measure across cluster units to identify the CPU-hungry unit.
Memory usage	This metric represents the current memory usage of this firewall cluster unit.	MB	A consistent increase in the value of this measure could indicate that a cluster unit is experiencing a memory drain. Compare the value of this measure across cluster units to identify the memory-hungry unit.
Network usage	This metric indicates the current network utilization of this firewall cluster unit.	KB/Sec	By comparing the value of this measure across cluster units you can accurately isolate overloaded units, and in the process proactively detect load-balancing irregularities in the cluster.
Packets processed	This metric is the rate of packets processed by the firewall cluster unit during the last measurement period.	Packets/sec	
Data processed	This metric is the data traffic handled by the firewall cluster unit during the last measurement period, expressed in KB.	KB	
Active session count	This metric is the current active sessions to the firewall cluster unit.	Number	A high value of this measure could indicate a session overload on a cluster unit.
Virus detected	This value is the number of viruses the antivirus system detected in the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
Intrusions blocked	This value is the number of attacks that the IDS/IPS detected during the last measurement period	Number	An IPS is an Intrusion Prevention System for networks. While early systems focused on intrusion detection, the continuing rapid growth of the Internet, and the potential for the theft of sensitive data, has resulted in the need for not only detection, but prevention. The FortiGate IPS detects intrusions by using attack signatures for known intrusion methods, and detects anomalies in network traffic to identify new or unknown intrusions. Not only can the IPS detect and log attacks, but users can choose actions to take on the session when an attack is detected. Using sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets.

4.3.2 Session Details Test

By reporting the number of sessions that are active on the firewall, this test provides us with pointers to the current session load handled by the firewall.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

Parameter	Description
	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
Sessions	Indicates the number of sessions that are currently active on the firewall.	Number	A high value of this measure could indicate a session overload on the firewall.

4.3.3 Users Details Test

A user is a user account that consists of a user name, password and in some cases, other information that can be configured on the unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

When configuring a user account on the firewall, you can indicate whether the user is to be allowed to authenticate (i.e., enabled) or blocked from authenticating (i.e., disabled). This test auto-discovers the user accounts configured on the firewall, and reports which user accounts are allowed to authenticate and which are not.

Target of the test : A FortiGate Firewall

Agent deploying the test : An external agent

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

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

Parameter	Description
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 of user account	Indicates the current authentication status of this user account.		If this measure reports the value *Enabled*, it indicates that the user account is allowed to authenticate. The value *Disabled* for a user account indicates that the user account is not allowed to authenticate. The numeric values that correspond to the measure values discussed above have been listed in the table below: **Measure Value** / **Numeric Value** Enabled – 1 Disabled – 0 **Note:** Typically, this measure will report one of the **Measure Value**s listed in the table above to indicate the authentication status of a user account. However, in the graph of this measure, the authentication status will be depicted using the corresponding numeric equivalents only.

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.