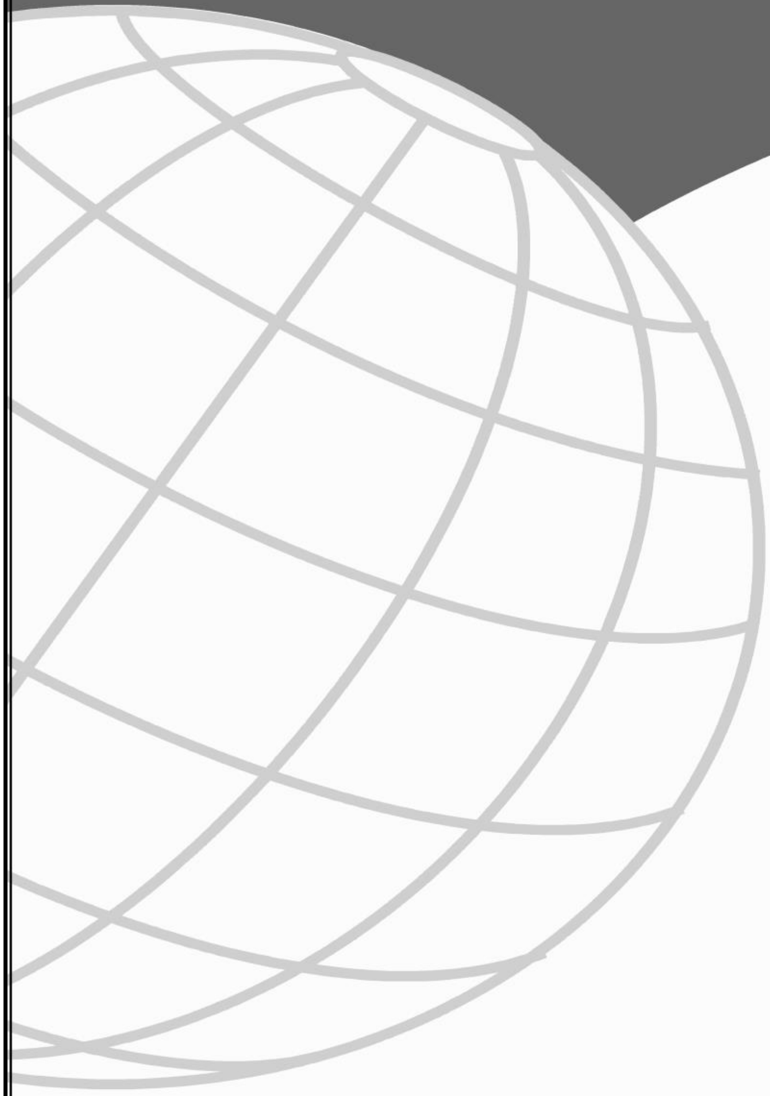


Monitoring Check Point Smart-1 Appliance

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

1

Monitoring the Check Point Smart-1 Appliance

Check Point Smart-1 appliances deliver cyber security management for the era of big data. Five Smart-1 Appliances enable organizations to consolidate security policy, log, and event management. Organizations can leverage Smart-1 Appliances to manage from 5 to 5000 gateways, segment the network into 200 independent domains, and detect threats in real-time. Smart-1 appliances offer the scalability to meet your needs today and in the future.

In order to keep your network safe and secure from malicious threats and attacks, it is imperative to operate the Check Point Smart-1 appliance continuously without any glitch. Any issue in the configuration, state, or resource usage of the appliance can bring its operations to a halt, leaving your network and all mission-critical applications operating within defenceless against malicious threats and unscrupulous users! It is hence important that the performance of the Check Point Smart-1 appliance is monitored 24x7.

eG Enterprise provides a specialized *Check Point Smart Appliance* monitoring model (see Figure 1) that enables administrators to keep an eye on the accesses to the protected environment and judge whether the smart appliance is capable in preventing unauthorized accesses.

To obtain statistics specific to a *CheckPoint Smart Appliance*, the eG agents rely on the SNMP interface supported by the Check Point Smart-1 appliance. Through the eG Enterprise's administrative interface, the port number on which the Check Point Smart-1 appliance exposes its MIB as well as the SNMP community to be used for accessing the MIB must be specified.

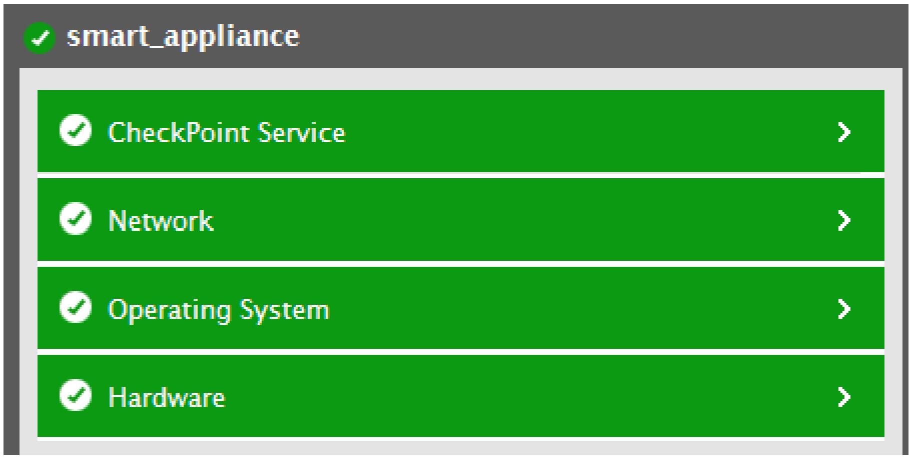


Figure 1: The layer model of a CheckPoint Smart Appliance

Every layer of Figure 1 is mapped to a variety of tests which reports a host of metrics using which administrators can easily find quick and accurate answers to the following performance questions:

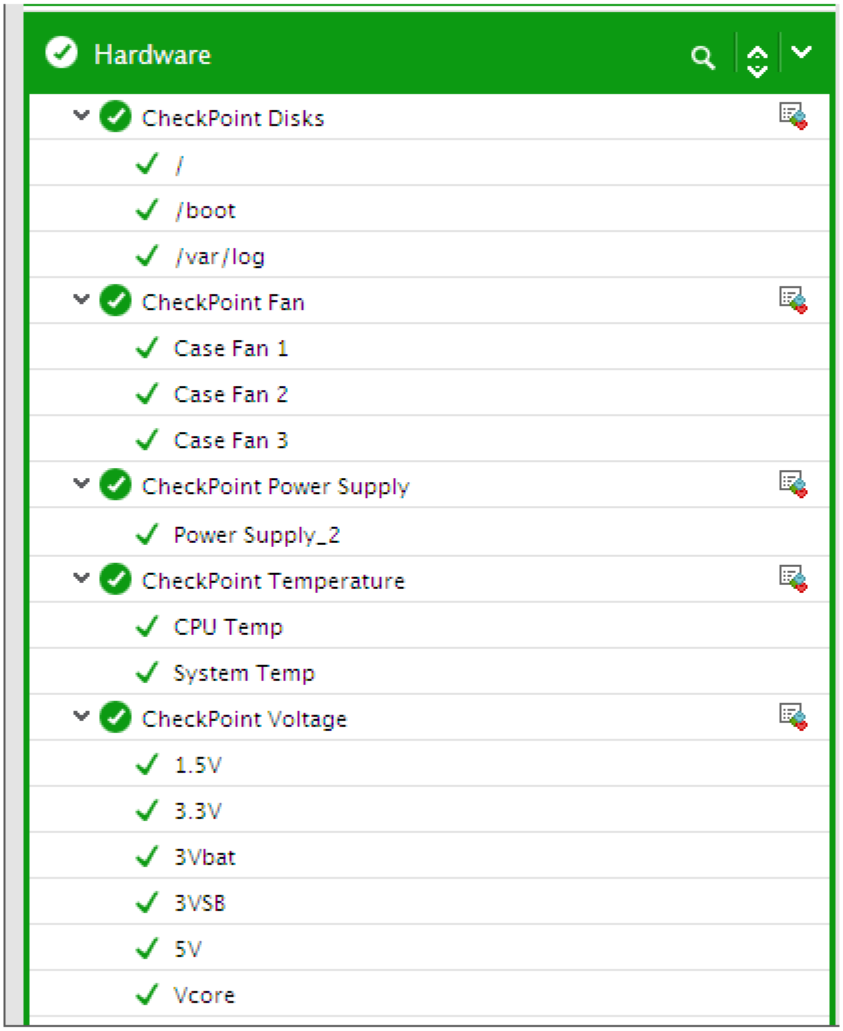
- What is the space utilization of each disk?
- What is the speed of each fan? Is the sensor of each fan out of range?
- Are the Power supply units up/down?

- What is the current voltage of each hardware element? Is the sensor of the hardware elements out of range?
- What is the current temperature of each hardware unit? Is the sensor of each hardware unit out of range?
- How well the CPU is utilized by the Check Point Smart-1 appliance? How much of CPU is utilized for system processes and user processes?
- What is the current memory utilization of the Check Point Smart-1 appliance?
- How well data and packets are processed by each virtual system of the CheckPoint Smart Appliance? How much of data/packets are dropped?

The **Network** layer of the *Check Point Smart-1 appliance* model is similar to that of a *Windows Generic* server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, Section 1.1 focuses on the **Hardware** layer.

1.1 The Hardware Layer

This layer helps administrators track the space utilization of each disk on the Check Point Smart-1 appliance, detect the speed of the fans in the appliance, the current voltage of each hardware element, the current temperature of each hardware unit etc.



Hardware

- ✓ CheckPoint Disks
  - ✓ /
  - ✓ /boot
  - ✓ /var/log
- ✓ CheckPoint Fan
  - ✓ Case Fan 1
  - ✓ Case Fan 2
  - ✓ Case Fan 3
- ✓ CheckPoint Power Supply
  - ✓ Power Supply_2
- ✓ CheckPoint Temperature
  - ✓ CPU Temp
  - ✓ System Temp
- ✓ CheckPoint Voltage
  - ✓ 1.5V
  - ✓ 3.3V
  - ✓ 3Vbat
  - ✓ 3VSB
  - ✓ 5V
  - ✓ Vcore

Figure 2: The tests mapped to the Hardware layer

1.1.1 CheckPoint Disks Test

This test monitors the space utilization of each disk in the Check Point Smart-1 appliance and proactively alerts administrators to potential space crunches, if any.

Purpose	Monitors the space utilization of each disk in the Check Point Smart-1 appliance and proactively alerts administrators to potential space crunches, if any.
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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.

	6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each disk on the Check Point Smart-1 Appliance being monitored

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

1.1.2 CheckPoint Fan Test

Fans ensure that the temperature of the core components of the Check Point Smart-1 appliance are well-within operable limits. If one/more fans fail, then the temperature of sensitive hardware may soar causing permanent hardware damage. With the help of this test, you can instantly detect the speed at which the fans operate and an out of range fan sensor, initiate remedial measures in order to prevent any irreparable damage to the hardware.

Purpose	Instantly detects the speed at which the fans operate and an out of range fan sensor, initiate remedial measures in order to prevent any irreparable damage to the hardware
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan operating on the Check Point Smart-1 appliance</td></tr>
<tr><td rowspan="3"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Speed:</b>
Indicates the speed at which this fan operates.</td><td>Rpm</td><td>The speed of the fan should be well within operable limits. A sudden/significant rise/fall in the value of this measure could be a cause of concern which warrants an investigation.</td></tr>
<tr><td><b>Is sensor out of range?:</b>
Indicates whether/not the sensor of this fan is out of range.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>100</td><td>No</td></tr>
<tr><td>1</td><td>Yes</td></tr>
<tr><td>2</td><td>Reading error</td></tr>
</table>
Note
By default, this measure reports the <b>Measure Values</b> discussed above to indicate whether/not the sensor of this fan is out of range. In the graph of this measure however, the <b>Measure Values</b> are represented using the numeric equivalents only.</td></tr>
</table>

1.1.3 CheckPoint Power Supply Test

This test auto-discovers the power supply units of the Check Point Smart-1 appliance and reports the current state of each power supply unit.

Purpose	Auto-discovers the power supply units of the Check Point Smart-1 appliance and reports the current state of each power supply unit.
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each Power supply unit in the Check Point Smart-1 appliance</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Power supply status:</b>
Indicates the current state of this power supply unit.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>100</td><td>Up</td></tr>
<tr><td>0</td><td>Down</td></tr>
</table>
Note
By default, this measure reports the <b>Measure Values</b> discussed above to indicate the current state of the power supply. In the graph of this measure however, the <b>Measure Values</b> are represented using the numeric equivalents only.</td></tr>
</table>

1.1.4 CheckPoint Voltage Test

This test auto-discovers the hardware elements in the Check Point Smart-1 appliance, reports the current voltage of each hardware element in addition to reporting whether/not the LED corresponding to each hardware element is out of range.

Purpose	Auto-discovers the hardware elements in the Check Point Smart-1 appliance, reports the current voltage of each hardware element in addition to reporting whether/not the LED corresponding to each hardware element is out of range.
Target of the	A Check Point Smart-1 appliance

test	
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each voltage unit in the Check Point Smart-1 appliance</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Voltage:</b>
Indicates the current voltage of this element.</td><td>Volts</td><td></td></tr>
<tr><td></td><td><b>Is sensor out of range?:</b>
Indicates whether/not the LED corresponding to this element is out of range.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>1</td><td>Yes</td></tr><tr><td>2</td><td>Reading error</td></tr><tr><td>100</td><td>No</td></tr></table>
Note
By default, this measure reports the <b>Measure Values</b> discussed above to indicate whether/not the LED corresponding to the element is out of range. In the graph of this measure however, the <b>Measure Values</b> are represented using the numeric equivalents only.</td></tr>
</table>

1.1.5 CheckPoint Temperature Test

This test auto-discovers the hardware units of the Check Point Smart-1 appliance, reports the current temperature of each hardware unit in addition to reporting whether/not the LED corresponding to each hardware unit is out of range. This test perfectly pin points the hardware units that are not operating in the admissible temperature limits thus forewarning administrators to potential failure of the hardware units.

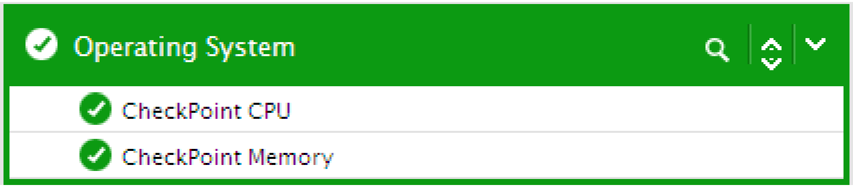
Purpose	Auto-discovers the hardware units of the Check Point Smart-1 appliance, reports the current temperature of each hardware unit in addition to reporting whether/not the LED corresponding to each hardware unit is out of range.
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** **-** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each voltage unit in the Check Point Smart-1 appliance</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Temperature:</b>
Indicates the current temperature of this hardware unit.</td><td>Celsius</td><td></td></tr>
<tr><td></td><td><b>Is sensor out of range?:</b>
Indicates whether/not the LED corresponding to this hardware unit is out of range.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>1</td><td>Yes</td></tr>
<tr><td>2</td><td>Reading error</td></tr>
<tr><td>100</td><td>No</td></tr>
</table>
Note
By default, this measure reports the <b>Measure Values</b> discussed above to indicate whether/not the LED corresponding to this hardware unit is out of range. In the graph of this measure however, the <b>Measure Values</b> are represented using the numeric equivalents only.</td></tr>
</table>

1.2 The Operating System Layer

Using the tests mapped to this layer, administrators can monitor the CPU utilization and the memory utilization of the Check Point Smart-1 appliance and proactively be alerted to potential CPU and memory resource contentions, if any.



Operating System

CheckPoint CPU

CheckPoint Memory

Figure 3: The tests mapped to the Operating System layer

1.2.1 CheckPoint CPU Test

This test monitors the current CPU utilization of the Check Point Smart-1 appliance. In the process, this test helps you to obtain the statistics for the CPU utilized for system level processing and user level processing. Using this test, administrators can identify the tasks that are consuming too much of CPU resources and take necessary steps to minimize such tasks.

Purpose	Monitors the current CPU utilization of the Check Point Smart-1 appliance. In the process, this test helps you to obtain the statistics for the CPU utilized for system level processing and user level processing
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter.

<table>
<tr><td></td><td colspan="3">7. <b>AUTHPASS</b> – Specify the password that corresponds to the above-mentioned <b>USERNAME</b>. This parameter once again appears only if the <b>SNMPVERSION</b> selected is <b>v3</b>.
8. <b>CONFIRM PASSWORD</b> – Confirm the <b>AUTHPASS</b> by retyping it here.
9. <b>AUTHTYPE</b> – This parameter too appears only if <b>v3</b> is selected as the <b>SNMPVERSION</b>. From the <b>AUTHTYPE</b> 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:
➢ <b>MD5</b> – Message Digest Algorithm
➢ <b>SHA</b> – Secure Hash Algorithm
10. <b>ENCRYPTFLAG</b> – This flag appears only when <b>v3</b> is selected as the <b>SNMPVERSION</b>. By default, the eG agent does not encrypt SNMP requests. Accordingly, the <b>ENCRYPTFLAG</b> is set to <b>NO</b> by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the <b>YES</b> option.
11. <b>ENCRYPTTYPE</b> – If the <b>ENCRYPTFLAG</b> is set to <b>YES</b>, then you will have to mention the encryption type by selecting an option from the <b>ENCRYPTTYPE</b> list. SNMP v3 supports the following encryption types:
➢ <b>DES</b> – Data Encryption Standard
➢ <b>AES</b> – Advanced Encryption Standard
12. <b>ENCRYPTPASSWORD</b> – Specify the encryption password here.
13. <b>CONFIRM PASSWORD</b> – Confirm the encryption password by retyping it here.
14. <b>TIMEOUT -</b> Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
15. <b>DATA OVER TCP –</b> 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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the Check Point Smart-1 appliance that is to be monitored</td></tr>
<tr><td></td><td><b>CPU utilization:</b>
Indicates the current CPU utilization of this appliance.</td><td>Percent</td><td>A high value could signify a CPU bottleneck. The CPU utilization may be high because a few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource. Check the currently running processes to see the exact cause of the problem.</td></tr>
</table>

	CPU usage for system process: Indicates the percentage of CPU utilized for system level processing.	Percent	An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.
	CPU usage for user process: Indicates the percentage of CPU utilized by the user level processing.	Percent	An unusually high value indicates a problem and may be due to too many user level tasks executing simultaneously.

1.2.2 CheckPoint Memory Test

This test reports statistics related to the usage of the memory of the Check Point Smart-1 appliance. Using this test, administrators may be proactively alerted to memory resource contention, if any.

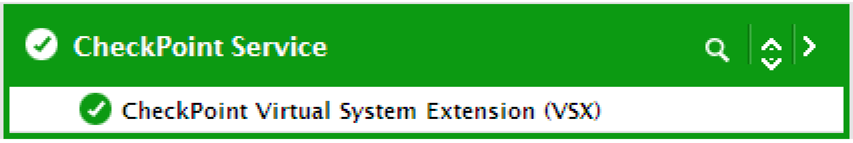
Purpose	Reports statistics related to the usage of the memory of the Check Point Smart-1 appliance. Using this test, administrators may be proactively alerted to memory resource contention, if any.
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter.

	7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Check Point Smart-1 appliance that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total Memory: Indicates the total memory of this appliance.	GB	

	Used Memory: Indicates the amount of memory currently utilized by this appliance.	GB	A high value for this measure indicates that the memory resources are depleting drastically. Administrators may be alerted to add additional resources before memory resources are drained completely.
	Free Memory: Indicates the amount of memory that is currently available for use in this appliance.	GB	
	Memory utilization: Indicates the percentage of memory utilized by this appliance.	IOPS	Ideally, the value of this measure should be low. While sporadic spikes in memory usage could be caused by one/more rogue processes on the system, a consistent increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources. If this unhealthy trend is not repaired soon, it could severely hamper system performance, causing anything from a slowdown to a complete system meltdown.

1.3 The CheckPoint Service Layer

Using the test mapped to this layer, administrators can monitor the amount of data and packets processed through each virtual system of the Check Point Smart-1 appliance.



CheckPoint Service

CheckPoint Virtual System Extension (VSX)

Figure 4: The tests mapped to the CheckPoint Service layer

1.3.1 CheckPoint Virtual System Extension (VSX) Test

VSX (Virtual System Extension) is a security and VPN solution for large-scale environments based on the proven security of Check Point Security Gateway. VSX provides comprehensive protection for multiple networks or VLANs within complex infrastructures. It securely connects them to shared resources such as the Internet and/or a DMZ, and allows them to safely interact with each other. VSX is supported by IPS™ Services, which provide up-to-date preemptive security.

VSX incorporates the same patented Stateful Inspection and Software Blades technology used in the Check Point Security Gateway product line. Administrators manage VSX using a Security Management Server or a Multi-Domain Server, delivering a unified management architecture that supports enterprises and service providers.

A VSX Gateway contains a complete set of virtual devices that function as physical network components, such as Security Gateway, routers, switches, interfaces, and even network cables. Centrally managed, and incorporating key network resources internally, VSX lets businesses deploy comprehensive firewall and VPN functionality, while reducing hardware investment and improving efficiency.

Using the Check Point Smart-1 appliance, administrators may configure multiple virtual systems in their environment. Each **Virtual System** works as a Security Gateway, typically protecting a specified network. When packets arrive at the VSX Gateway, it sends traffic to the Virtual System protecting the destination network. The Virtual System inspects all traffic and allows or rejects it according to the rules defined in the security policy thus preventing unauthorized access to the network which in turn leads to the optimal network resource usage. On the other hand, improper policy configurations may result in fewer virtual systems which may hog the bandwidth and choke the network! To avoid such spurious situations, administrators should periodically monitor the efficiency of the policy configuration, figure out any impending discrepancies and fix them immediately! This is where the CheckPoint Virtual System Extension test helps! This test auto-discovers the virtual systems configured in the Check Point Smart-1 appliance and periodically monitors the amount of data and packets processed through each virtual system. In addition, this test also reports the CPU utilization and the active connections on each virtual system. In the process, this test helps administrators deduce the virtual system that is handling high volume of traffic and is hogging the bandwidth resources available to the network! This way, administrators can figure out if policy configurations are effective and if not, can initiate necessary action to fine tune them.

Purpose	Auto-discovers the virtual systems configured in the Check Point Smart-1 appliance and periodically monitors the amount of data and packets processed through each virtual system. In addition, this test also reports the CPU utilization and the active connections on each virtual system
Target of the test	A Check Point Smart-1 appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Check Point Smart-1 appliance. 3. **SNMPPORT** – The SNMP Port number of the Check Point Smart-1 appliance (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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

	12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Check Point Smart-1 appliance over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each virtual system configured on the Check Point Smart-1 appliance that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	CPU utilization: Indicates the percentage of CPU utilized by this virtual system.	Percent	A value close to 100% is a cause of concern.
	Active connections: Indicates the number of connections that are currently active on this virtual system.	Number	An abnormally high value for this measure could indicate a probable virus attack or spam to a mail server in the network.
	Peak connections: Indicates the maximum number of connections to this virtual system.	Number	

	Data processed: Indicates the amount of data processed by this virtual system during the last measurement period.	MB	Comparing the values of this measure across the virtual systems helps you in identifying the virtual system that is processing the maximum amount of data i.e., you can deduce the virtual system that has consumed the maximum bandwidth over the network. If there is a huge gap between the maximum and minimum bandwidth consumers, it could indicate that one/more virtual systems are hogging the bandwidth resources. You may then need to reconfigure/fine-tune the security policies and rules to minimize the bandwidth usage.
	Accepted data: Indicates the amount of data that was processed successfully by this virtual system during the last measurement period.	MB	
	Dropped data: Indicates the amount of data that was dropped by this virtual system during the last measurement period.	MB	Ideally, the value of this measure should be zero. If there is a consistent increase in the value of this measure, then it clearly indicates that the virtual system is either processing a lot of malicious traffic or is under attack.
	Rejected data: Indicates the amount of data rejected by this virtual system during the last measurement period.	MB	A low value is desired for this measure.
	Success data rate: Indicates the percentage of data that was successfully processed by this virtual system during the last measurement period.	Percent	A high value is desired for this measure.

	Packets processed: Indicates the number of packets processed by this virtual system during the last measurement period.	Number	Comparing the values of this measure across the virtual systems helps you in identifying the virtual system that is processing the maximum amount of data i.e., you can deduce the virtual system that has consumed the maximum bandwidth over the network. If there is a huge gap between the maximum and minimum bandwidth consumers, it could indicate that one/more virtual systems are hogging the bandwidth resources. You may then need to reconfigure/fine-tune the security policies and rules to minimize the bandwidth usage.
	Accepted packets: Indicates the number of packets that were processed successfully by this virtual server during the last measurement period.	Number	
	Dropped packets: Indicates the number of packets that were dropped by this virtual server during the last measurement period.	Number	Ideally, the value of this measure should be zero.
	Rejected packets: Indicates the number of packets that were rejected by this virtual server during the last measurement period.	Number	
	Success packets rate: Indicates the percentage of packets that were successfully processed by this virtual system during the last measurement period.	Percent	

2 Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **Check Point Smart Appliance**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.