# Monitoring Cisco VPN Concentrator

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

# Table of Contents

CHAPTER 1: INTRODUCTION ........ 1

CHAPTER 2: HOW DOES EG ENTERPRISE MONITOR CISCO VPN CONCENTRATOR? ........ 2

2.1 Managing the Cisco VPN Concentrator ........ 2

CHAPTER 3: MONITORING THE CISCO VPN CONCENTRATOR ........ 5

3.1 The VPN Hardware Layer ........ 5

3.1.1 VPN Fans Test ........ 5

3.1.2 VPN Temperature Test ........ 8

3.1.3 VPN Voltage Test ........ 11

3.2 The Network Layer ........ 14

3.3 The VPN Server Layer ........ 14

3.3.1 VPN Server Test ........ 14

3.4 The VPN Service Layer ........ 17

3.4.1 VPN Throughput  Test ........ 17

3.4.2 VPN Sessions Test ........ 20

ABOUT EG INNOVATIONS ........ 24

# Table of Figures

Figure 2.1: Adding a Cisco VPN Concentrator component 3

Figure 2.2: List of unconfigured tests to be configured for the Cisco VPN Concentrators 3

Figure 2.3: Configuring the VPN Fans test 4

Figure 3.1: Figure 6.1: The layer model of a Cisco VPN Concentrator 5

Figure 3.2: The tests mapped to the VPN Hardware layer 5

Figure 3.3: The test  mapped to the VPN Server layer 14

Figure 3.4: The tests associated with the VPN Service layer 17

# Chapter 1: Introduction

The Cisco VPN 3000 Series Concentrators are purpose-built, remote access virtual private network (VPN) platforms that support connectivity mechanisms including IP security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) over IPSec, and Cisco WebVPN (clientless secure sockets layer [SSL] browser- based connectivity). Since they are critical components that provide secure access across disparate networks, VPN concentrators need to be monitored 24*7 to ensure that they are operating well at all times. This is where the eG Enterprise lends a helping hand to administrators for continuously monitoring the VPN concentrators.

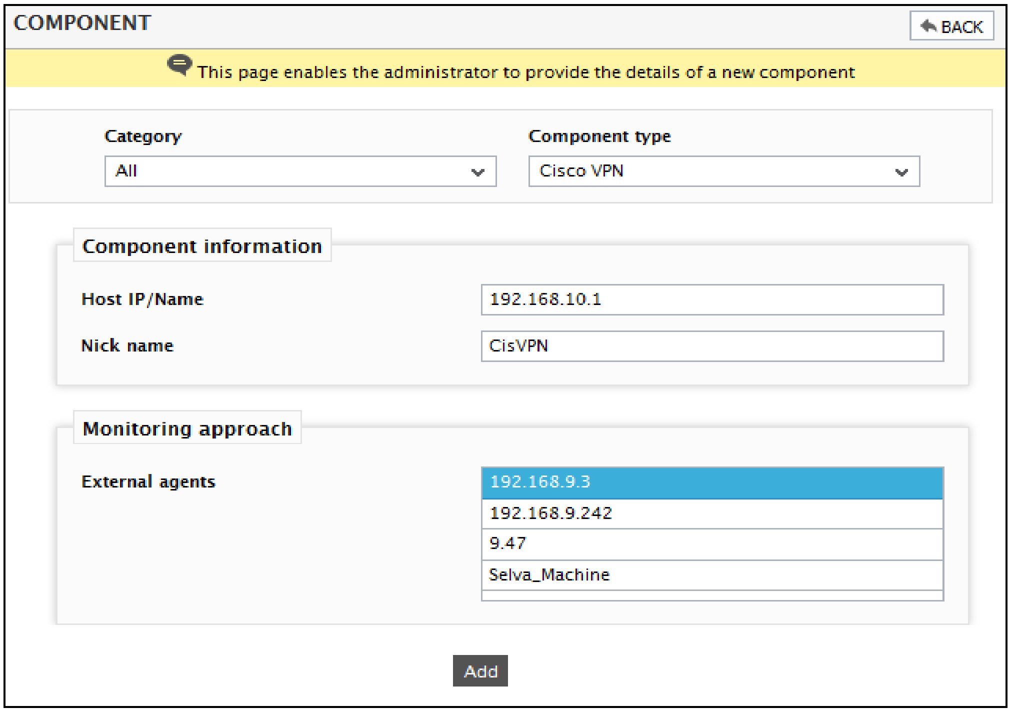
# Chapter 2: How does eG Enterprise Monitor Cisco VPN Concentrator?

The eG Enterprise is capable of monitoring the Cisco VPN Concetrator in using an eG external agent that is deployed on any remote host. The eG external agent periodically polls the SNMP MIB of the  Cisco VPN Concentrator and fetches metrics related to the performance of the Cisco VPN Concentrator. This sections that follow describe how to manage and monitor the Cisco VPN Concentrator.

## 2.1 Managing the Cisco VPN Concentrator

The eG Enterprise cannot automatically discover a Cisco VPN Concentrator so that you need to manually add the component for monitoring. To manage a Cisco VPN Concentrator component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears next, select Cisco VPN Concentrator as the **Component** type. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

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

Category: All

Component type: Cisco VPN

Component information

Host IP/Name: 192.168.10.1

Nick name: CisVPN

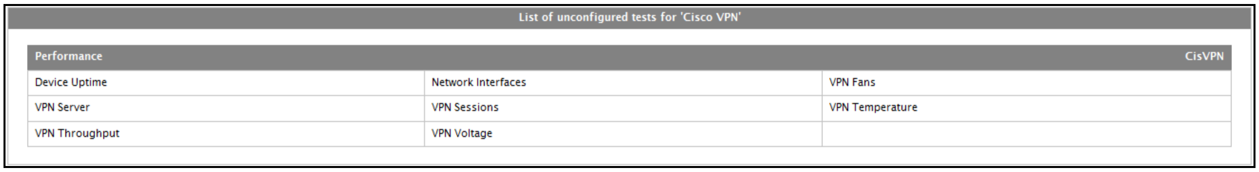
Monitoring approach

External agents:
- 192.168.9.3
- 192.168.9.242
- 9.47
- Selva_Machine

Figure 2.1: Adding a Cisco VPN Concentrator component

4. Specify the **Host IP/Name** and **Nick name o**f the Cisco VPN Concentrator component to be monitored as shown in Figure 2.1. Then, click **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears.

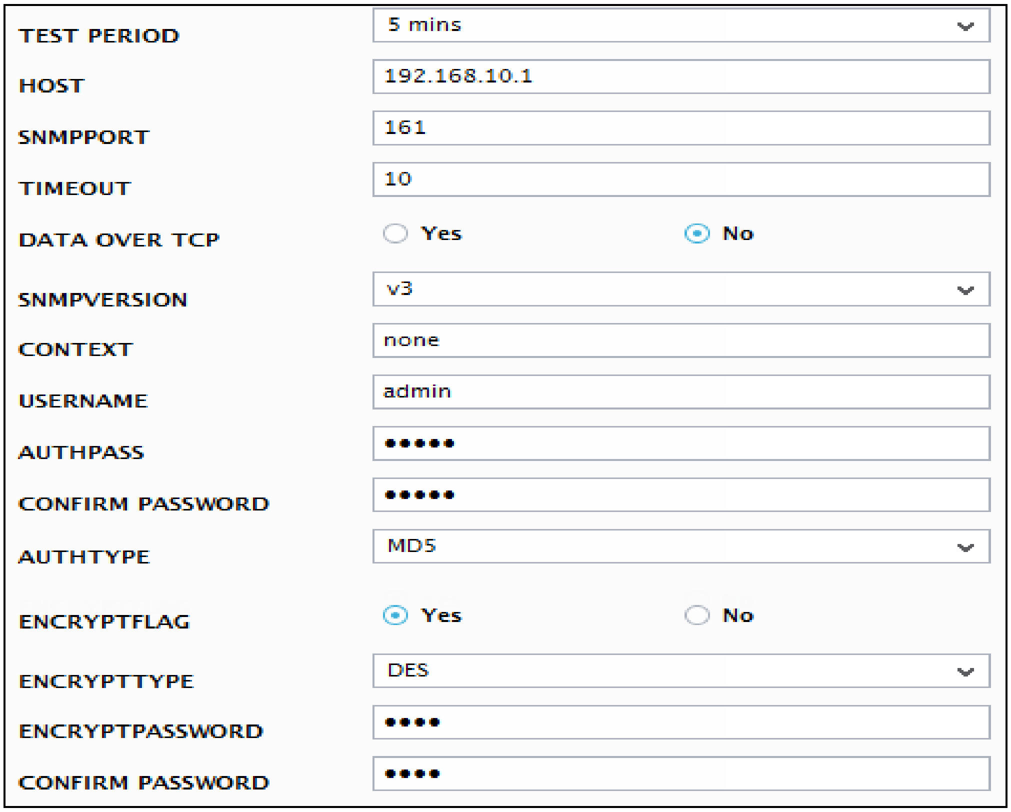


List of unconfigured tests for 'Cisco VPN'

| Performance | | CisVPN |
|---|---|---|
| Device Uptime | Network Interfaces | VPN Fans |
| VPN Server | VPN Sessions | VPN Temperature |
| VPN Throughput | VPN Voltage | |

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

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



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

Figure 2.3: Configuring the VPN Fans test

To know how to configure the tests, refer to the **Monitoring the Cisco VPN Concentrator**.

7. Finally, signout of the eG administrative interface.

# Chapter 3: Monitoring the Cisco VPN Concentrator

eG Enterprise presents a specialized *Cisco VPN* monitoring model (see Figure 3.1), which executes external tests on the VPN concentrator, and reports its current status.

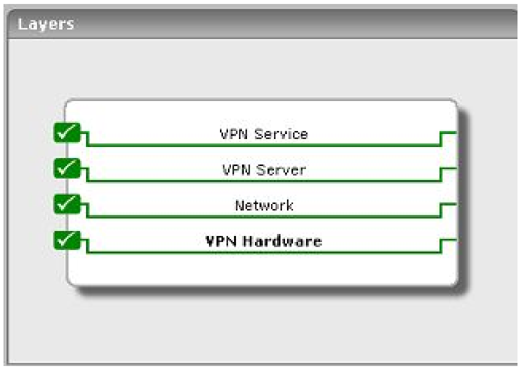


Figure 3.1: Figure 6.1: The layer model of a Cisco VPN Concentrator

The sections below focus on each layer of Figure 3.1, and tests mapped to the layers.

## 3.1 The VPN Hardware Layer

This layer, as its name suggests, helps administrators assess the performance of the VPN hardware (see Figure 3.2).

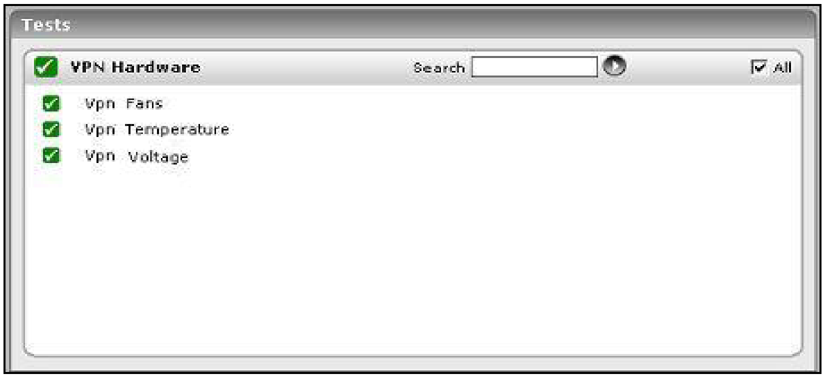


Figure 3.2: The tests mapped to the VPN Hardware layer

### 3.1.1 VPN Fans Test

This test monitors the individual fans on the concentrator and reports whether they are operating normally.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every fan on the VPN concentrator being monitored

**Configurable parameters for the test**

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

| Parameters | 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:<br>• **MD5** – Message Digest Algorithm<br>• **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:<br>• **DES** – Data Encryption Standard<br>• **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 |
|---|---|---|---|
| Fan1 speed | Indicates the speed of | Rpm | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | Fan1. | | |
| Fan1 status | Indicates the status of Fan1. | Boolean | If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0. |
| Fan2 speed | Indicates the speed of Fan2. | Rpm | |
| Fan2 status | Indicates the status of Fan2. | Boolean | If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0. |
| Fan3 speed | Indicates the speed of Fan3. | Rpm | |
| Fan3 status | Indicates the status of Fan3. | Boolean | If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0. |

## 3.1.2 VPN Temperature Test

This test monitors the temperature of the different hardware components and alerts if any abnormalities are detected.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every hardware component being monitored

**Configurable parameters for the test**

| Parameters | 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. |
| SNMPPort | The port at which the monitored target exposes its SNMP MIB; the default is *161*. |
| SNMPVersion | By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. |

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

| Parameters | Description |
|---|---|
| | selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:<br>• **DES** – Data Encryption Standard<br>• **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 temperature | Indicates the current temperature of the CPU. | DegreeC | |
| CPU temperature status | Indicates the current status of the CPU temperature. | Boolean | This metric has a value of 0 if the CPU temperature is abnormal. Otherwise, the value is 1. |
| Cage temperature status | Indicates the current cage temperature. | DegreeC | |
| Cage temperature | Indicates the current status of the cage temperature. | Boolean | This metric has a value of 0 if the cage temperature is abnormal. Otherwise, the value is 1. |

## 3.1.3 VPN Voltage Test

This test monitors whether all voltage levels in the different hardware components are within norms and generates alerts if this is not the case.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every hardware component being monitored

**Configurable parameters for the test**

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

| Parameters | 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:<br>• **MD5** – Message Digest Algorithm<br>• **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:<br>• **DES** – Data Encryption Standard<br>• **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 voltage | Indicates the current voltage of the CPU. | Volts | |
| Cpu voltage status | Indicates whether the CPU voltage is normal or not. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |
| Ps1 3v value | Indicates the current voltage of the 3v power supply 1. | Volts | |
| Ps1 3v status | Indicates the status of the 3v power supply's voltage. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |
| Ps1 5v value | Indicates the current voltage of the 5v power supply 1. | Volts | |
| Ps1 5v status | Indicates the status of the 5v power supply's voltage. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |
| Ps2 3v value | Indicates the current voltage of the 3v power supply 2. | Volts | |
| Ps2 3v status | Indicates the status of the 3v power supply's voltage. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |
| Ps2 5v value | Indicates the current voltage of the 5v power supply 2. | Volts | |
| Ps2 5v status | Indicates the status of the 5v power supply's voltage. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |
| Board voltage 3v | Indicates the current voltage of the 3v supply to the board. | Volts | |
| Board 3v status | Indicates the status of the | Boolean | The value is 1 if the voltage is normal. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | 3v power supply's voltage. | | Otherwise, this metric has a value of 0. |
| Board voltage 5v | Indicates the current voltage of the 5v supply to the board. | Volts | |
| Board 5v status | Indicates the status of the 5v power supply's voltage. | Boolean | The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0. |

## 3.2 The Network Layer

Since the **Network** test, **Network Interfaces** test, and **Device Uptime** test associated with this layer have been dealt with in great detail in the *Monitoring Cisco Router*, let us proceed to the VPN Server layer.

## 3.3 The VPN Server Layer

Using the metrics reported by this layer, administrators can determine whether additional resources need to be allocated to the VPN concentrator for handling the current load.

Figure 3.3: The test  mapped to the VPN Server layer

### 3.3.1 VPN Server Test

This test monitors whether the concentrator is adequately sized to handle the current load.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every VPN concentrator being monitored

### Configurable parameters for the test

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

| Parameters | Description |
|---|---|
| | the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>• **MD5** – Message Digest Algorithm<br>• **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:<br>• **DES** – Data Encryption Standard<br>• **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**. |

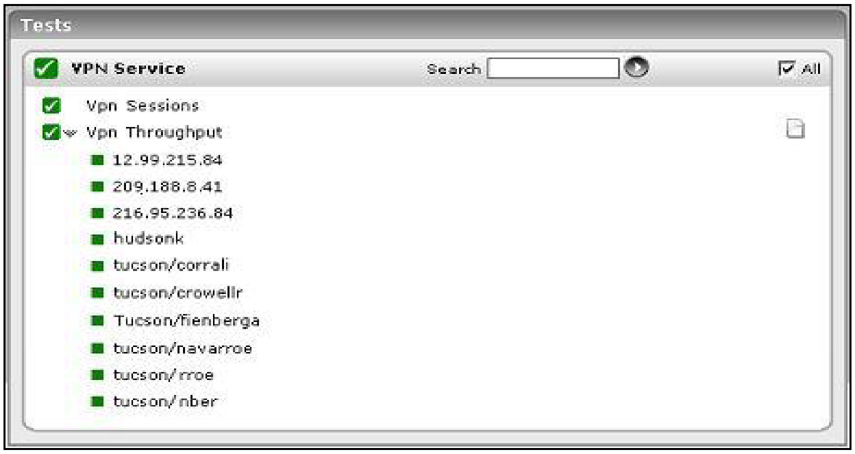
### Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Cpu utilization | Indicates the current CPU utilization of the VPN Concentrator. | Percent | A consistent value greater than 90% indicates a potential bottleneck. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Session utilization | Indicates the utilization of the VPN concentrator in terms of sessions supported. This value is the ratio of the current sessions to the maximum sessions that the VPN Concentrator can support. | Percent | |
| Throughput utilization | Indicates the utilization of the VPN concentrator in terms of throughput offered. This value is the ratio of the current throughput to the maximum throughput that the VPN concentrator can support. | Percent | |

## 3.4 The VPN Service Layer

The tests mapped to the **VPN Service** layer (see Figure 3.4) measure the throughput of the VPN concentrator and the session load on the server.



☑ Vpn Sessions

☑ Vpn Throughput

- 12.99.215.84
- 209.188.8.41
- 216.95.236.84
- hudsonk
- tucson/corrali
- tucson/crowellr
- Tucson/fienberga
- tucson/navarroe
- tucson/ rroe
- tucson/ nber

Figure 3.4: The tests associated with the VPN Service layer

### 3.4.1 VPN Throughput Test

This test tracks the top 10 user sessions with highest data throughput.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every user session being monitored

**Configurable parameters for the test**

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

| Parameters | 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:<br>• **MD5** – Message Digest Algorithm<br>• **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:<br>• **DES** – Data Encryption Standard<br>• **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 |
|---|---|---|---|
| Connect time | Indicates the time in mins since when the user connected via the VPN concentrator. | Mins | |
| Data transmitted | Indicates the data transmitted over the session. | MB | |
| Data received | Indicates the data received over the session. | MB | eG Enterprise's detailed diagnosis capability will be used to log the IP address of the user, protocol used, encryption type, and the public IP of the user. |

## 3.4.2 VPN Sessions Test

This test monitors the different types of sessions to the Cisco VPN Concentrator.

**Target of the test :** A Cisco VPN Concentrator

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for the VPN concentrator being monitored

### Configurable parameters for the test

| Parameters | 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. |
| SNMPPort | The port at which the monitored target exposes its SNMP MIB; the default is *161*. |
| SNMPVersion | By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. |
| SNMPCommunity | The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen |

| Parameters | Description |
|---|---|
| | 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:<br>• **MD5** – Message Digest Algorithm<br>• **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: |

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

## Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Active sessions | Indicates the number of sessions currently actively using the VPN concentrator. | Number | |
| New sessions | Indicates the number of new sessions added in the last measurement period. | Number | |
| Max active sessions | Indicates the maximum number of active sessions that the VPN concentrator has been configured to handle. | Number | |
| Session utilization | Indicates the percentage utilization of sessions - this metric is the ratio of the current number of active sessions to the maximum | Percent | This measure is a good indicator of the capacity of the concentrator to support more sessions. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | sessions that the concentrator has been configured to handle. | | |
| Lan2Lan sessions | Indicates the number of current LAN to LAN sessions supported by the concentrator. | Number | |
| Management sessions | Indicates the current number of management sessions to the VPN concentrator. | Number | |
| Remote sessions | Indicates the current number of remote sessions handled by the VPN concentrator. | Volts | |

# 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.