
SC Deployment via VPN Deployment Mode

<https://campus.barracuda.com/doc/46208890/>

If you do not have physical access to the Secure Connector, you can configure the SC to connect to the SAC and Control Center by using a passphrase-authenticated VPN tunnel in VPN deployment mode. After the connection is established, the Control Center pushes the configuration to the SC. Now that the SC has the necessary certificates, the VPN tunnel is automatically switched to operational mode.

Before You Begin

Configure the SAC and Control Center. For more information, see [Secure Access Concentrator and Control Center Deployment](#).

Limitations

An SC using Templates where the VPN mode is set to **Operative** cannot be switched to **Deployment Mode**. Exempt the VPN Mode setting from the template, or use a "VPN deployment" template and move the SC to the "production" template after it has successfully connected.

Step 1. Configure the SC on the Control Center

Configure the SC using the Secure Connector Editor. Configure the VPN in Deployment mode. The configuration must be saved for the automatically filled information (blue background) to be visible.

For more information, see [How to Add a Secure Connector Configuration](#).

Step 2. Get Required Information from the SC Configuration

The following information from the SC configuration is necessary to configure the SC via web interface.

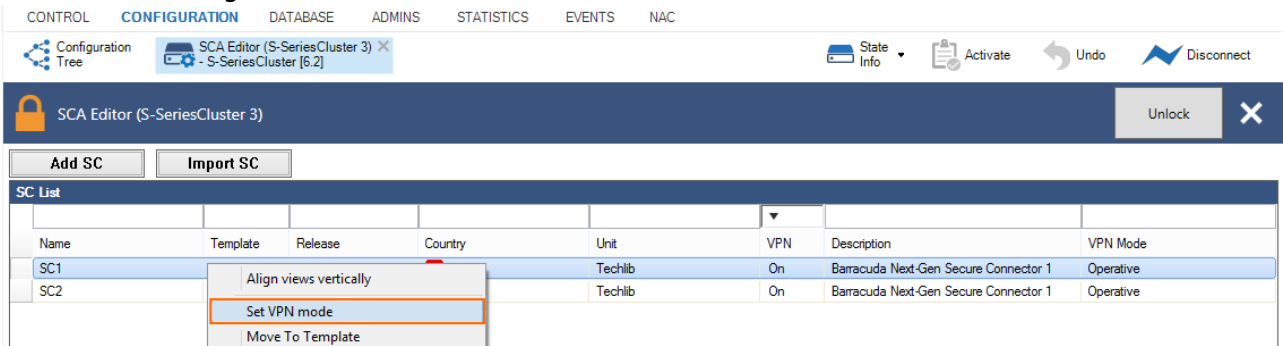
1. Go to **your cluster** > **Cluster Settings** > **Secure Connector Editor**.
2. Double-click on the SC configuration.

3. The following web UI settings must be filled with the values of their corresponding Secure Connector Editor settings:
 - **Box Unique Identifier** - In the SC configuration, go to **Identification Settings > Unique Identifier**.
 - **Virtual IP** - In the SC configuration, go to **VPN Settings > Virtual IP**.
 - **Entry Point Address** - In the SC configuration, go to **VPN Settings > Server Name or Address**.
 - **Entry Point Port** - In the SC configuration, go to **VPN Settings > Server Port**.
 - **Tunnel Mode** - In the SC configuration, go to **VPN Settings > Tunnel Mode**.
 - **Encryption** - In the SC configuration, go to **VPN Settings > Encryption**.

Step 3. Enable VPN Deployment Mode for the SC

Enable VPN deployment mode for the SC. If you are not using a template and the VPN mode is already set to **Deployment Mode** you can skip this step.

1. Go to **your cluster > Cluster Settings > Secure Connector Editor**.
2. Click **Lock**.
3. In the **SC List**, right-click the SC and select **Set VPN Mode**.



The screenshot shows the 'SCA Editor (S-SeriesCluster 3)' interface. At the top, there are navigation tabs: CONTROL, CONFIGURATION (selected), DATABASE, ADMINS, STATISTICS, EVENTS, and NAC. Below the tabs, there are buttons for 'State Info', 'Activate', 'Undo', and 'Disconnect'. The main area has a title bar 'SCA Editor (S-SeriesCluster 3)' with an 'Unlock' button and a close icon. Below the title bar are 'Add SC' and 'Import SC' buttons. The 'SC List' table is shown with the following data:

Name	Template	Release	Country	Unit	VPN	Description	VPN Mode
SC1				Techlib	On	Barracuda Next-Gen Secure Connector 1	Operative
SC2				Techlib	On	Barracuda Next-Gen Secure Connector 1	Operative

A context menu is open over the 'SC1' row, showing options: 'Align views vertically', 'Set VPN mode' (highlighted), and 'Move To Template'.

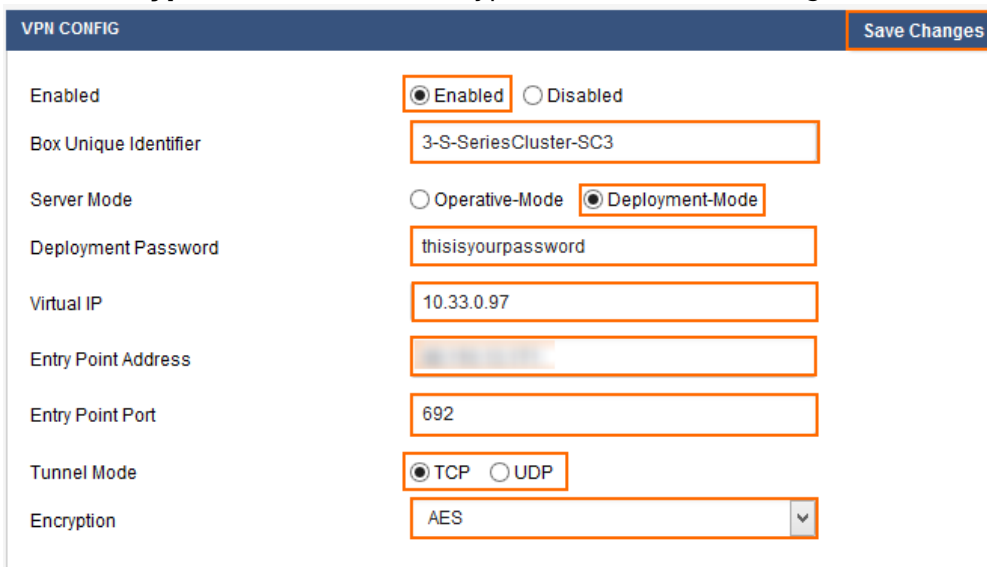
4. From the **Operative Mode** drop-down list, select **Deployment Mode**.
5. Enter the **Deployment** passphrase.
6. Click **OK**.
7. Click **Activate**.

Step 4. Configure the SC to Connect to the SAC

The SC listens on 192.168.200.200 on the LAN port. You must configure your client PC to connect to the SC and then use the web interface to configure the WAN and VPN connection.

1. Change your client PC IP address to:
 - **IP address** - 192.168.200.100
 - **Netmask** - 255.255.255.0

- **Gateway** – 192.168.200.200
2. Connect your client PC to the **LAN** port of the SC.
3. Open a browser and go to <https://192.168.200.200>.
4. Log into the Secure Connector:
 - **Username** – Enter admin.
 - **Password** – Enter admin.
5. Click **Sign In**.
6. Click **Retrieve Lock**.
7. Go to **CONFIGURATION > Network**.
8. Configure the WAN connection. For more information, see [SC WAN Connections](#).
9. Go to **CONFIGURATION > VPN**.
10. Configure the VPN:
 - **Enabled** – Select **Enabled**.
 - **Box Unique Identifier** – Enter the **Unique Identifier** from the SC configuration.
 - **Server Mode** – Select **Deployment Mode**.
 - **Deployment Password** – Enter the deployment passphrase set in Step 3.
 - **Virtual IP** – Enter the Virtual IP address assigned to the SC by the Control Center.
 - **Entry Point Address** – Enter the public IP address through which the SAC can be reached.
 - **Entry Point Port** – Enter the port on the border firewall that forwards the SC VPN traffic to the SAC.
 - **Tunnel Mode** – Select the tunnel mode set in the SC configuration.
 - **Encryption** – Select the encryption set in the SC configuration.



VPN CONFIG		Save Changes
Enabled	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Box Unique Identifier	<input type="text" value="3-S-SeriesCluster-SC3"/>	
Server Mode	<input type="radio"/> Operative-Mode <input checked="" type="radio"/> Deployment-Mode	
Deployment Password	<input type="text" value="thisisyourpassword"/>	
Virtual IP	<input type="text" value="10.33.0.97"/>	
Entry Point Address	<input type="text" value="[blurred]"/>	
Entry Point Port	<input type="text" value="692"/>	
Tunnel Mode	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	
Encryption	<input type="text" value="AES"/>	

11. Click **Save Changes**.
12. Click **Activate Configs**.

The SC now automatically connects to the SAC and automatically receives the configuration from the Control Center. Any existing configuration locks are overridden by the Control Center. As the SC applies the configuration, the VPN connection is terminated and reestablished in operational mode using certificate authentication. Existing configuration locks on the SC are overridden during this

process.

Figures

1. set_vpn.png
2. sca_deploy_vpn_01.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.