

How to Add a Secure Connector Configuration

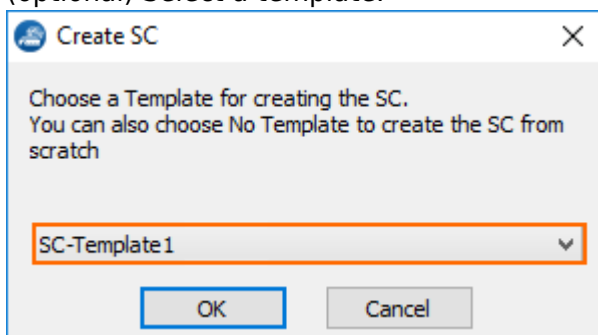
<https://campus.barracuda.com/doc/48202634/>

NextGen Secure Connectors are configured and managed by the NextGen Control Center using the Secure Connector Editor. You can either create the configuration as a template and then assign it to the FSC device, or directly configure the FSC. For more information, see [How to Create and Apply FSC Templates](#).

Step 1. Add a Secure Connector Configuration

Add a Secure Connector Configuration or use a configuration template. Configuration settings configured via template are automatically used and cannot be configured on a per-device basis.

1. Go to **your cluster** > **Cluster Settings** > **Secure Connector Editor**.
2. Click **Lock**.
3. Click **Add SC**.
4. (optional) Select a template.






5. Click **OK**. The **Create SC** window opens.

Step 2. Configure the settings for the FSC









Configure identification settings

1. Enter a **Unique Appliance Name** for the FSC. The name is final and cannot be changed later. The **Unique Identifier** is a string containing the range, cluster and unique appliance name.
2. (optional) Enter a description for the FSC
3. From The **Secure Connector Model** drop-down list, select the hardware version. E.g., **SC1**.
4. (optional) Click **+** to add the serial number of the FSCs allowed to connect with this configuration.
5. (optional) Enter your company details and specify the location and timezone of the FSC unit.

Identification Settings

Unique Appliance Name	<input type="text" value="SC1"/>	
Unique Identifier	<input type="text" value="3-S-SeriesCluster-SC1"/>	
Appliance Description	<input type="text" value="Barracuda Next-Gen Secure Connector 1"/>	

Product and Model

Secure Connector Model	<input type="text" value="SC1"/>	
Serial Numbers	<div style="text-align: right;">   </div> <input type="text"/>	
Organisation	<input type="text" value="Barracuda Networks"/>	
Unit	<input type="text" value="Techlib"/>	

Configure administrative settings

1. In the left menu, click **Administrative Settings**.
2. Select the FSC network from the **S-Series VIP Net** drop-down list. The FSC is automatically assigned to the FSAC associated with the FSC network.
3. In the **CC IP Address** field, enter the IP address of the Control Center.
4. Set the **WebUI Username/ Password** for the web interface of the FSC.
5. Enter the **Root Password** for the FSC. The default root password is: ngf1r3wa11
6. Select the **SSH Remote Access** check box to enable SSH. You must also create an FSC management rule to be able to log in via SSH. For more information, see [How to Create FSC Firewall Management Rules](#).
7. Enter the **Hostname** used for the FSC. You can use the same hostname for all FSCs.
8. In the **Box DNS Domain** field, enter the domain for the FSC.
9. Next to **DNS Server IP**, Click **+** to enter the IP addresses for the DNS servers.
10. Select the **Enable NTP** check box to synchronize the time with an NTP server.
11. Enter the FQDN or IP address for the NTP server located near your location.
Default: 0.pool.ntp.org

Administrative Settings

S-Series VIP Net	<input type="text" value="SCANET1"/>
CC IP Address	<input type="text" value="10.0.15.77"/>
WebUI Username	<input type="text" value="admin"/>
WebUI Password	<input checked="" type="checkbox"/> Current: <input type="password" value="....."/> New: <input type="password" value="....."/> Confirm: <input type="password" value="....."/> Strength: <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Strong
Root Password	<input checked="" type="checkbox"/> Current: <input type="password" value="....."/> New: <input type="password" value="....."/> Confirm: <input type="password" value="....."/> Strength: <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Strong
SSH Remote Access	<input checked="" type="checkbox"/>
Hostname	<input type="text" value="SecureConnector"/>
Box DNS Domain	<input type="text" value="secureconnector.local"/>
DNS Server IP	<input type="text" value="8.8.8.8"/> <input type="button" value="Add"/> <input type="button" value="Remove"/> <input checked="" type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Up"/> <input type="button" value="Down"/>
Enable NTP	<input checked="" type="checkbox"/>
NTP Server	<input type="text" value="0.pool.ntp.org"/>
















Configure WAN settings

1. In the left menu, click **WAN Settings**.
2. From the **WAN Network Mode** drop-down list, select **Manual**.
3. Configure the WAN connection for the WAN port. For more information, see [FSC WAN Connections](#).

Configure LAN settings

1. In the left menu, click **LAN Settings**.
2. Select the **LAN Network Mode**:
 - **Automatic** (default) – The FSC is automatically assigned a subnet from the FSC network with the pool size specified in the FSC network configuration.
 - **Manual** – Define the IP address and all other FSC network settings manually. You can also enable the DHCP server for the network.

LAN Interface Settings

LAN Network Mode	<input checked="" type="checkbox"/> Automatic	
LAN enabled	<input checked="" type="checkbox"/>	
IP Address	192.168.200.200	 
Subnet Mask	24-Bit	
DHCP Server	<input checked="" type="checkbox"/>	
DHCP First IP	192.168.200.10	
DHCP Last IP	192.168.200.100	
Choose Network automatically	<input checked="" type="checkbox"/>	
Auto IP Address	10.33.0.34	
Auto Subnet Mask	28-Bit	
Auto DHCP Start IP	10.33.0.35	
Auto DHCP End IP	10.33.0.46	
Auto Subnet	10.33.0.32/28	 

Configure Wi-Fi settings

1. In the left menu, click **Wi-Fi Settings**.
2. Select the **Wi-Fi Mode**:
 - **Access Point** – Configure the **Wi-Fi Settings**. For more information, see [FSC Wi-Fi Access Point](#).
 - **Wi-Fi Client** – To use the Wi-Fi interface as a WAN interface, see [FSC WAN Connections](#).

Configure Wireless WAN settings

1. In the left menu, click **Wireless WAN Settings**.
2. Select the **WWAN Active** checkbox.
3. Enter the name of the WWAN access point you wish to connect to.
4. If applicable, enter the unlocking PIN code for your SIM card.
5. Enter the **Phone Number** number without the trailing hash (#).
6. Select the **Authentication Method**.
7. Enter the **User Access ID** assigned by your WWAN service provider.
8. (optional) Enter the **User Access Sub-ID** assigned by your WWAN service provider.
9. Enter the **Access Password** assigned by your WWAN service provider.

Wireless WAN Settings

WWAN Active

**Wireless WAN Connection Details**

Access Point Name (APN)

AP01



SIM PIN

New

••••



Confirm

••••

Strength

Weak

Phone Number

*99***1

**Authentication**

Authentication Method

CHAP



User Access ID

123456789



User Access Sub-ID

123456789



Access Password

New

••••••••••



Confirm

••••••••••

Strength

Strong

Configure VPN Settings

1. In the left menu, click **VPN Settings**.
2. Select the **VPN Mode**:
 - **Operative Mode** (default) - Use certificates to authenticate to the FSAC.
 - **Deployment Mode** - Use a passphrase to authenticate to the FSAC.
3. Select the **VPN enabled** check box.
4. (Deployment mode only) Enter the **Deployment Password** used to authenticate when connecting to the FSAC.
5. Click **New Key** and select the **Key Length** to generate the private certificate.
6. Click **Edit** and fill in the certificate information.
7. (Manual network only) - Enter the VIP IP address in the **Virtual IP** field. If automatically assigned, this is the first IP address in the FSC subnet assigned to the unit.

Secure Connector VPN Settings

VPN Mode	Operative-Mode	
VPN enabled	<input checked="" type="checkbox"/>	
Deployment Password	thisisyourdeploymentpassword	
Private Key	<input type="button" value="New Key..."/> <input type="button" value="Ex/Import"/> Hash: EENZVQ 2048 Bits	
Access Concentrator Service Name	Automatically configured	
Virtual IP	10.33.0.33	
Virtual IP Mask	28-Bit	

- Next to **Remote Networks**, click **+** to add the networks routed through the VPN tunnel. To send everything through the tunnel and to offer Internet access, enter `0.0.0.0/0`. The **Server Port** is the **Entry Port** configured for the FSAC. The **VPN Access Concentrator Public Key** is automatically filled in when the configuration is saved.
- From the **Tunnel Mode** drop-down list, select the transport protocol. Select **TCP** (default) for more reliability and **UDP** for high performance.
- Select the **Encryption** algorithm used.

VPN Access Concentrator Settings

Remote Networks	
	0.0.0.0/0
Server Entry Point	
VPN Access Concentrator Public Key	<input type="button" value="Ex/Import"/> No key present
Server Port	692
Tunnel Mode	TCP
Encryption	AES

Configure Routing Settings

- In the left menu, click **Routing Settings**.
- Click **+** to add **System Routes**. For more information, see [FSC Routing](#).

Configure Firewall Settings

- In the left menu, click **Firewall Settings**.
- Configure the **Firewall Settings**. For more information, see [FSC Firewall](#).

Firewall Settings

Firewall Rules

Name	Action	Source Zone
lantovpn	ACCEPT	LAN
lantowifi	ACCEPT	LAN
vontolan	ACCEPT	VPN

Firewall Management

Name	Allow	Source Zone
lan	1	LAN
vpn	1	VPN
wifi	1	WIFI

Source NAT

Name	Source Interface	NAT Interface
------	------------------	---------------


Destination NAT

Name	Source Zone	IP Address
------	-------------	------------

Configure advanced settings

1. In the left menu, click **Advanced**:
2. Configure **Logging**. For more information, see [FSC Logging](#).
3. Select **USB Mass Storage support** to use the FSC as a mass storage device on your desktop computer. This allows you to copy configuration files directly to the FSC.

Advanced System Settings

Enable Persistent Logging	<input type="checkbox"/>	
USB Mass Storage support	<input checked="" type="checkbox"/>	
Enable Syslog Streaming	<input checked="" type="checkbox"/>	
Syslog Target Address/Host	<input type="text" value="10.0.15.70"/>	

4. To configure syslog streaming, see [FSC Syslog Streaming](#).
5. Click **OK**.
6. Click **Activate**.

Next Steps

For information on how to deploy an FSC using this configuration, see:

- [FSC Deployment via FSC Configuration File](#)
- [FSC Deployment via VPN Deployment Mode](#)

Figures

1. sc_01.png
2. id_settings.png
3. adm_settings.png
4. lan_settings.png
5. wap_conf.png
6. sc_vpn.png
7. vpn_ac.png
8. acfw_settings.png
9. sc_advanced_settings.png

© Barracuda Networks Inc., 2020 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.