

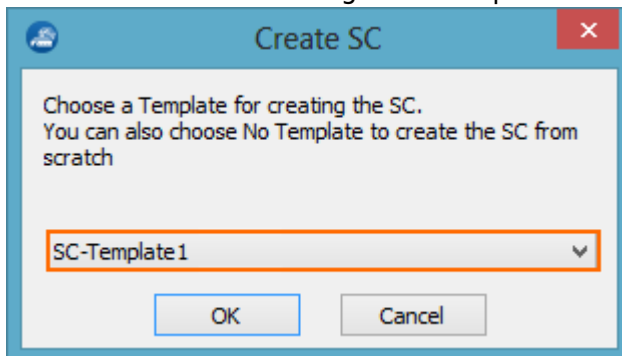
How to Add a Secure Connector Configuration

<https://campus.barracuda.com/doc/46895049/>

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 SC device, or directly configure the SC. For more information, see [How to Create and Apply SC Templates](#).




Add a Secure Connector configuration

1. Log in to your Control Center.
2. Go to **your Cluster** > **Cluster Settings** > **Secure Connector Editor**.
3. Click **Lock**.
4. Click **Add SC**. The **Create SC** window opens.
5. (optional) Select a template. Configuration settings configured via template are automatically used and cannot be configured on a per-device basis.






6. Configure the **Identification Settings**:
 - **Unique Appliance Name** – Enter a unique name for the SC. The name is final and cannot be changed later.
 - (automatic) **Unique Identifier** – The identifier is a string containing the range, cluster, and unique appliance name.
 - (optional) **Appliance Description**
7. Configure the **Product and Model**:
 - **Secure Connector Model** – Select the hardware version. E.g., **SC1**.
 - (optional) **Serial Numbers** – Click + to add the serial number of the SCs allowed to connect with this configuration.
 - (optional) **Organization**
 - (optional) **Unit**

Identification Settings





Unique Appliance Name	SC1	
Unique Identifier	3-S-SeriesCluster-SC1	
Appliance Description	Barracuda Next-Gen Secure Connector 1	

Product and Model

Secure Connector Model	SC1	
Serial Numbers	<div style="text-align: right;">      </div> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	
Organisation	Barracuda Networks	
Unit	Techlib	

8. Configure the **Location Specific Settings**:
- (optional) **Location** – Enter the location.
 - (optional) **Country** – Select the country.
 - (optional) **State** – If applicable, select the state.
 - **Located in Timezone** – Select the SC time zone.

Location Specific Settings

Location	Innsbruck	
Country	AUSTRIA	
State	--not-set--	
Located in Timezone	Europe/Vienna	

9. In the left menu, click **Administrative Settings** and configure:
- **S-Series VIP Net** – Select the SC Network. The SC is automatically assigned to the SAC associated with the SC network.
 - **WebUI Username** and **WebUI Password** – Set the username and password for the web interface of the SC.
 - **Root Password** – Enter the root password. The default root password is: ngf1r3wall
 - **SSH Remote Access** – Select the check box to enable SSH. You must also create an SC management rule to be able to log in via SSH. For more information, see [How to Create SC Firewall Management Rules](#).
 - **Hostname** – Enter the hostname used for the SC. You can use the same hostname for all SCs.

- **Box DNS Domain** – Enter the domain for the SC.
- **DNS Server IP** – Click + to enter the IP addresses for the DNS servers.
- **Enable NTP** – Select the check box to synchronize the time with an NTP server.
- **NTP Server IP** – 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="Automatically configured"/>
WebUI Username	<input type="text" value="admin"/>
WebUI Password	<input checked="" type="checkbox"/> Current <input type="password" value="••••"/> <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 <input type="checkbox"/>
Root Password	<input checked="" type="checkbox"/> Current <input type="password" value="••••"/> <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 <input type="checkbox"/>
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="text"/>
Enable NTP	<input checked="" type="checkbox"/>
NTP Server	<input type="text" value="0.pool.ntp.org"/>







10. In the left menu, click **WAN Settings**.

11. Configure the WAN connection for the WAN port. For more information, see [SC WAN Connections](#).

WAN Interface Settings

WAN Network Mode	<input checked="" type="checkbox"/> DHCP-Client	
DHCP Client	<input checked="" type="checkbox"/>	
IP Address	<input type="text"/>	  
Subnet Mask	24-Bit	

Advanced Settings

WAN enabled	<input checked="" type="checkbox"/>	
WAN Device	eth1	
WAN Zone	WAN	
Description	Predefined WAN Interface	
DHCP Server	<input type="checkbox"/>	
Choose Network automatically	<input type="checkbox"/>	
















12. In the left menu, click **LAN Settings**.

13. Select the **LAN Network Mode**:

In the left menu, click **LAN Settings**:

- **Automatic** (default) – The SC is automatically assigned a subnet from the SC network with the pool size specified in the SC network configuration.
- **Manual** – Define the IP address and all other SC 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	 

14. In the left menu, click **Wi-Fi Settings**.

15. Configure the **Wi-Fi Settings**:

- **Access Point** – Configure the **Wi-Fi Settings**. For more information, see [SC Wi-Fi Access Point](#).
- **Wi-Fi Client** – To use the Wi-Fi interface as a WAN interface, see [SC WAN Connections](#).

Wi-Fi Settings

Wi-Fi Mode: Access-Point-Automatic

SSID

Name	Active	SSID
------	--------	------

Network Mode: 802.11g

Wi-Fi Channel: Auto

Wi-Fi HW Mode: AP

Wi-Fi enabled:

DHCP Client:

IP Address:

Subnet Mask: 24-Bit

DHCP Server enabled:

DHCP Start IP:

DHCP End IP:

Choose Network automatically:

Auto IP Address: 10.33.0.49

Auto Subnet Mask: 28-Bit

Auto DHCP Start IP: 10.33.0.50

Auto DHCP End IP: 10.33.0.62


Auto Subnet: 10.33.0.48/28

16. In the left menu, click **UMTS/3G Modem Settings**.


17. Configure the **UMTS/3G Modem Settings**:

- **UMTS/3g Modem Active** - Select the check box to enable the USB modem.
- **UMTS 3G Connection Details** - Enter the connection details of your mobile provider.
- **Authentication** - Enter the authentication settings supplied by your mobile provider.


UMTS/3G Settings

UMTS/3G Modem Active 

UMTS/3G Connection Details


Access Point Name (APN) 

SIM PIN


New 


Confirm

Strength Weak

Phone Number 


Authentication

Authentication Method 

User Access ID 

User Access Sub-ID

Access Password

New 









Confirm

Strength Weak

18. Configure the **Secure Connector VPN Settings**:

- **VPN Mode**:
 - **Operative Mode** (default) – Use certificates to authenticate to the SAC.
 - **Deployment Mode** – Use a passphrase to authenticate to the SAC.
- **VPN enabled** – Select the check box.
- (Deployment mode only) **Deployment Password** – Enter the passphrase used to authenticate when connecting to the SAC.
- **Private Key** – Click **New Key** and select the **Key Length** to generate the private certificate.
- (manual network only) **Virtual IP** – Enter the VIP IP address. If automatically assigned, this is the first IP address in the SC subnet assigned to the unit.

Secure Connector VPN Settings

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

19. Configure the **VPN Access Concentrator Settings**:

- **(automatic) Server Name or Address** - This is automatically filled in with the **Point of Entry** configured for the SAC when the configuration is saved.
- **(automatic) VPN Access Concentrator Public Key** - The key is automatically filled in when the configuration is saved.
- **(automatic) Server Port** - This is the **Entry Port** configured for the SAC.
- **Tunnel Mode** - Select the transport protocol. Select **TCP** (default) for more reliability and **UDP** for high performance.
- **Encryption** - Select the encryption algorithm used.
- **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**.

VPN Access Concentrator Settings

Server Name or Address + × ↑ ↓ 📄

VPN Access Concentrator Public Key 📄

Ex/Import ▼ Hash: LZLJNY 2048 Bits

Server Port 📄

692

Tunnel Mode 📄

TCP

Encryption 📄

AES

Remote Networks 📄 + × ↑ ↓ 📄

0.0.0.0/0

20. In the left menu, click **Routing Settings**.
21. Click **+** to add **System Routes**. For more information, see [SC Routing](#).
22. (optional) In the **Link Selection** section, configure the failover policies if you are using more than one WAN connection. For more information, see [FSC Link Selection](#).
23. In the left menu, click **Firewall Settings**.
24. Configure the **Firewall Settings**. For more information, see [SC 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
------	-------------	------------

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

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"/>	

28. To configure syslog streaming, see [SC Syslog Streaming](#).
29. Click **OK**.

30. Click **Activate**.

Next steps

To deploy a SC using this configuration, see:

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

Figures

1. tmp_select.png
2. id_settings.png
3. loc_settings.png
4. adm_settings.png
5. wan_settings.png
6. lan_settings.png
7. wifi_settings.png
8. umts_settings.png
9. sc_vpn_settings.png
10. vpn_ac_settings.png
11. acfw_settings.png
12. sc_advanced_settings.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.