Secure Access Controller and Control Center Deployment

https://campus.barracuda.com/doc/79462668/

To integrate Secure Connectors into your network, you must configure the Secure Access Controller and the Firewall Control Center to manage and route traffic from and to the Secure Connector VIP networks. The Control Center can manage multiple Secure Access Controllers. There has to be at least one management network per Access Controller, configured in the global settings. The size of the network is read only, if more IP addresses are needed, additional networks can be added to the Access Controller. The data networks have to be configured on cluster level, best in the cluster where the Access Controller is configured.

Before You Begin

- Define the public IP address for **Point of Entry** for the Secure Access Controller. The Secure Connectors will connect to this public IP address.
- Define the management and data networks used for the Secure Connectors. Depending on your setup, create a global/range or cluster network object for them.
- Create a service object for the following Secure Connector services:
  - **NGS-MGMT** – TCP/UDP 888 and TCP/UDP 889
  - **NGS-VPN** – TCP/UDP 692. If a custom port is used, replace the port with the custom port

  For more information, see Service Objects.
- Create network objects for the Secure Connector management and data networks. For more information, see Network Objects.
- You must have the license tokens for the Secure Access Controller and the Secure Connector Energize Updates pool license.

Deploy and Configure a Secure Access Controller

Step 1. Deploy a CloudGen Firewall Image to be Used as the Access Controller

Deploy a virtual or public cloud CloudGen Firewall. Verify that the number of CPU cores, storage, and RAM are sized according to your Access Controller model. If you are deploying in the public cloud, see Secure Access Controller in Azure and AWS for more information on Access Controller cloud deployment options.

VF / ACC Model	Number of Licensed Cores	Minimum Storage [GB]	Minimum Memory [GB]
VACC400	2	80	2
VACC610	4	80	2
VACC820	8	80	2

For more information, see Virtual Systems (Vx) or Microsoft Azure Deployment.

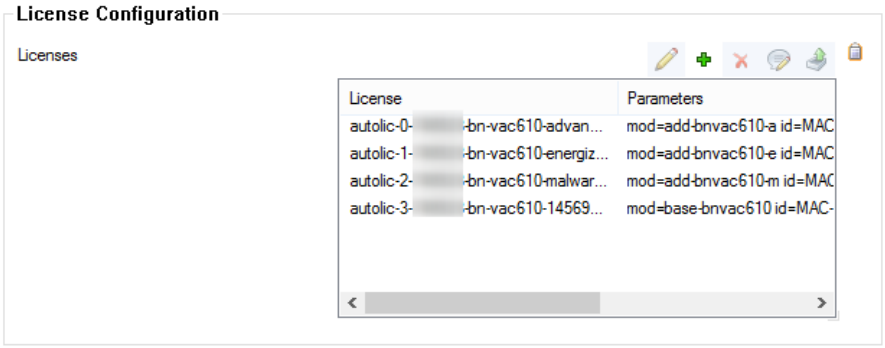
Step 2. Import the Access Controller into the Control Center

The Access Controller must be managed by the same Control Center that is managing the Secure Connectors.

For more information, see How to Import an Existing CloudGen Firewall into a Control Center.

Step 3. License the Secure Access Controller

License and activate the Access Controller using Barracuda Activation on the Control Center. The licenses are automatically downloaded and installed. On your Access Controller, go to **CONTROL > Licenses** or **CONFIGURATION > Configuration Tree > Box > Licenses** to verify that the licenses are installed.

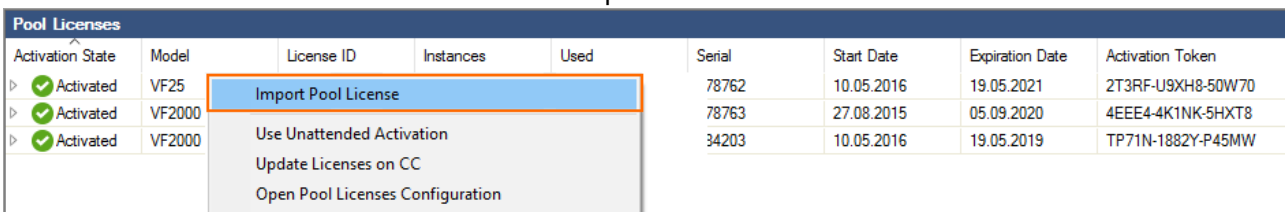


For more information, see How to Assign and Activate Single Licenses on a Control Center.

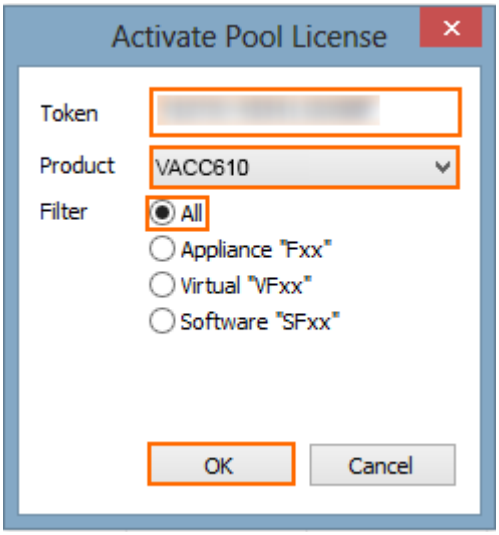
Step 4. Import the Secure Connector Pool License

Import and activate the Secure Connector Energize Updates (EU) pool license. The number of Secure Connectors allowed to connect to a single Access Controller is determined by the EU pool licenses assigned to the Access Controller.

1. Log into the Control Center.
2. Go to **CONTROL > Barracuda Activation**.
3. Right-click in the **Pool Licenses** section and select **Import Pool License** from the context menu. The **Activate Pool License** window opens.



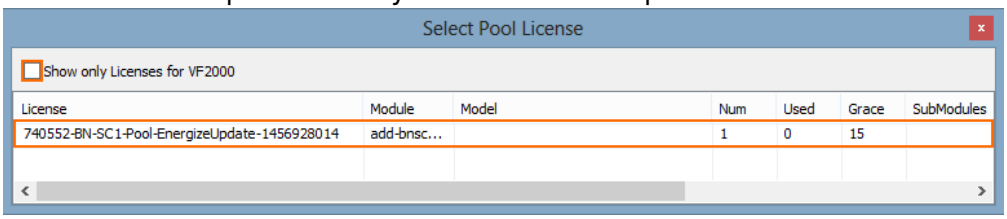
4. Enter the Secure Connector Energize Updates license **Token**.
5. From the **Filter** list, select **All**.
6. From the **Product** list, select your Access Controller model: **VACC400**, **VACC610**, or **VACC820**.
7. Click **OK**.



8. Fill in the **Activation Form**. Wait for the license to be activated and downloaded.

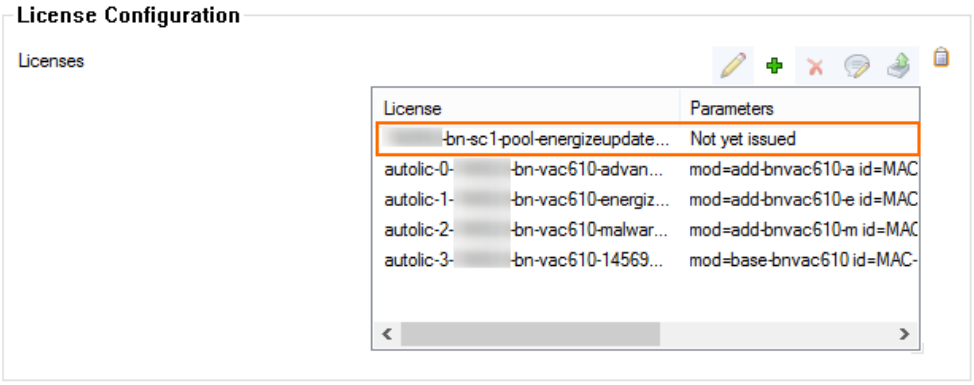
Step 5. Assign the Secure Connector Pool License to the Access Controller

1. Go to ***your cluster*** **>** ***your Access Controller*** **>** **Box Licenses**.
2. Click **Lock**.
3. In the **Licenses** list, click **+** and select **Import from Pool Licenses.** The **Select Pool Licenses** window opens.
4. Clear the **Show only Licenses for VFxxx** check box.
5. Double-click the pool license you installed in Step 4.



6. Click **Send Changes** and **Activate**.

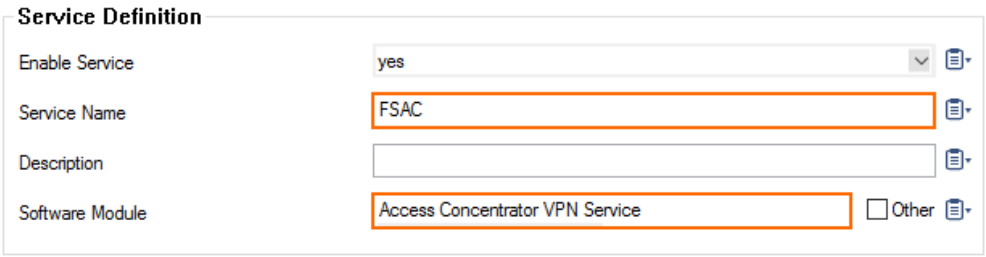
The Secure Connector EU pool license is now added to the Access Controller licenses.



Step 6. Create the Access Controller VPN Service

Create the Access Controller VPN service. The Access Controller VPN service and the VPN service are mutually exclusive - only one can run on a firewall at the same time.

1. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your virtual server*** **>** **Assigned Services**.
2. Right-click **Assigned Services** and select **Create Service**.
3. Enter a **Service Name**. The name must be unique and no longer than six characters. The service name cannot be changed later.
4. From the **Software Module** list, select **Access Controller VPN Service**.



5. (optional) Change the **Service IPs**. For more information, see How to Configure Services.
6. Click **Finish**.
7. Click **Activate**.

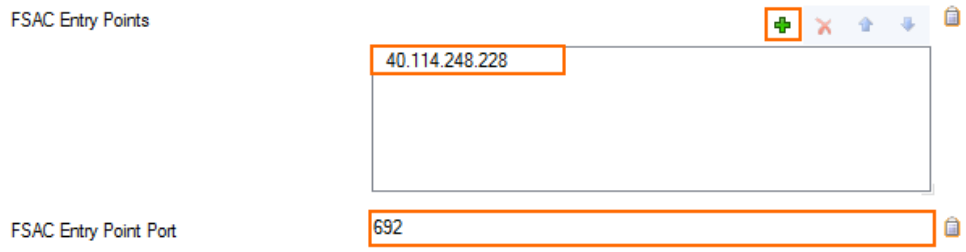
Step 7. Configure the Access Controller VPN Service

Create the Access Controller VPN key used to authenticate the Secure Connectors and enter the IP address and port the Secure Connectors will use to connect to this Access Controller.

If managed CloudGen Firewalls also connect through the same public IP address, adjust the ports on the firewalls to avoid redirecting the firewall management tunnels to the Access Controller. To configure the Access Controller to also handle CloudGen Firewall management tunnels, see How to Configure Management Tunnel Offloading using an Access Controller.

1. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your Access Controller virtual server*** **>** **Assigned Services > VPNAC > VPN Settings**.

2. Click **Lock**.
3. In the left menu, click **Secure Connector**.
4. Add the public IP address the Secure Connectors use to connect as the **VACC Entry Point**.
5. (optional) Enter the **VACC Entry Point Port**. Default: 692

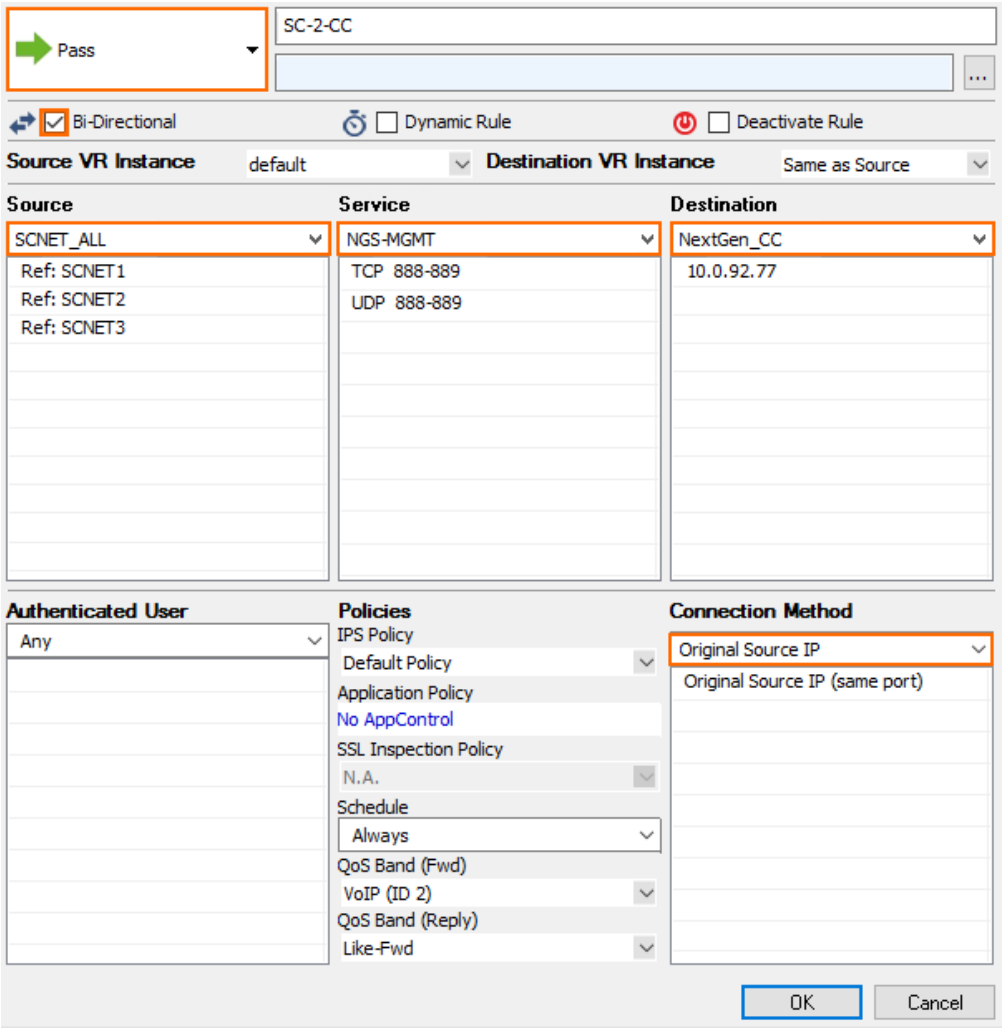


6. In the left menu, click **Secure Access Controller**.
7. Click **New Key** to create a **Server Key**.
8. Click **Send Changes** and **Activate**.

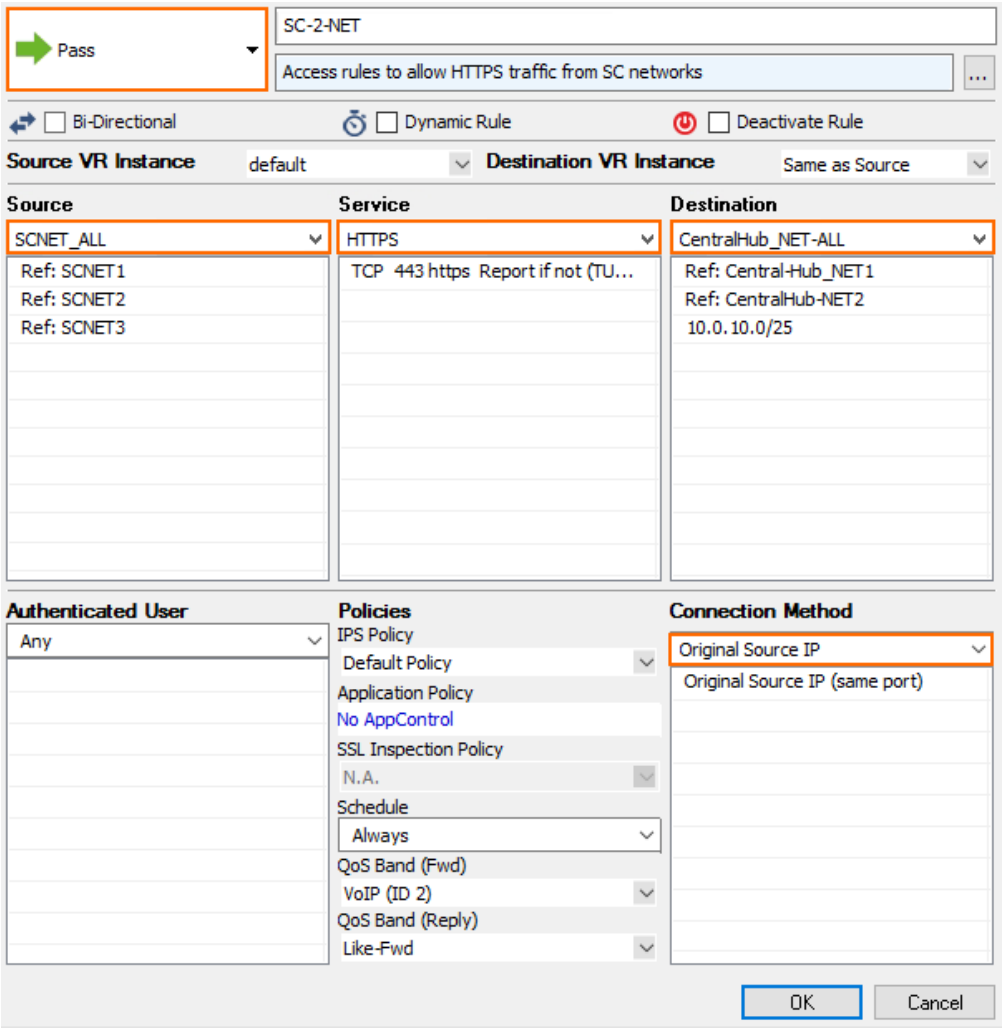
Step 8. Add Access Rules for Secure Connector VIP Network

Create access rules to allow Secure Connector traffic to the Control Center and to the border firewall. TCP/UDP 888 - 889 is used for communication between the Control Center and the Secure Connectors.

1. Go to ***your cluster*** **> Virtual Servers >** ***your Access Controller virtual server*** **> Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a PASS access rule to allow management traffic from the Secure Connector VIP network to the Control Center:
   - **Action** – Select **PASS**.
   - **Bi-Directional** – Select the check box to apply the rule in both directions.
   - **Source** – Select the Secure Connector VIP network(s) associated with this Access Controller.
   - **Service** – Select the **NGS-MGMT** service object for Secure Connector management traffic: TCP/UDP 888 and TCP/UDP 889.
   - **Destination** – Select the network object for the Control Center IP address.
   - **Connection** – Select **Original Source IP**.



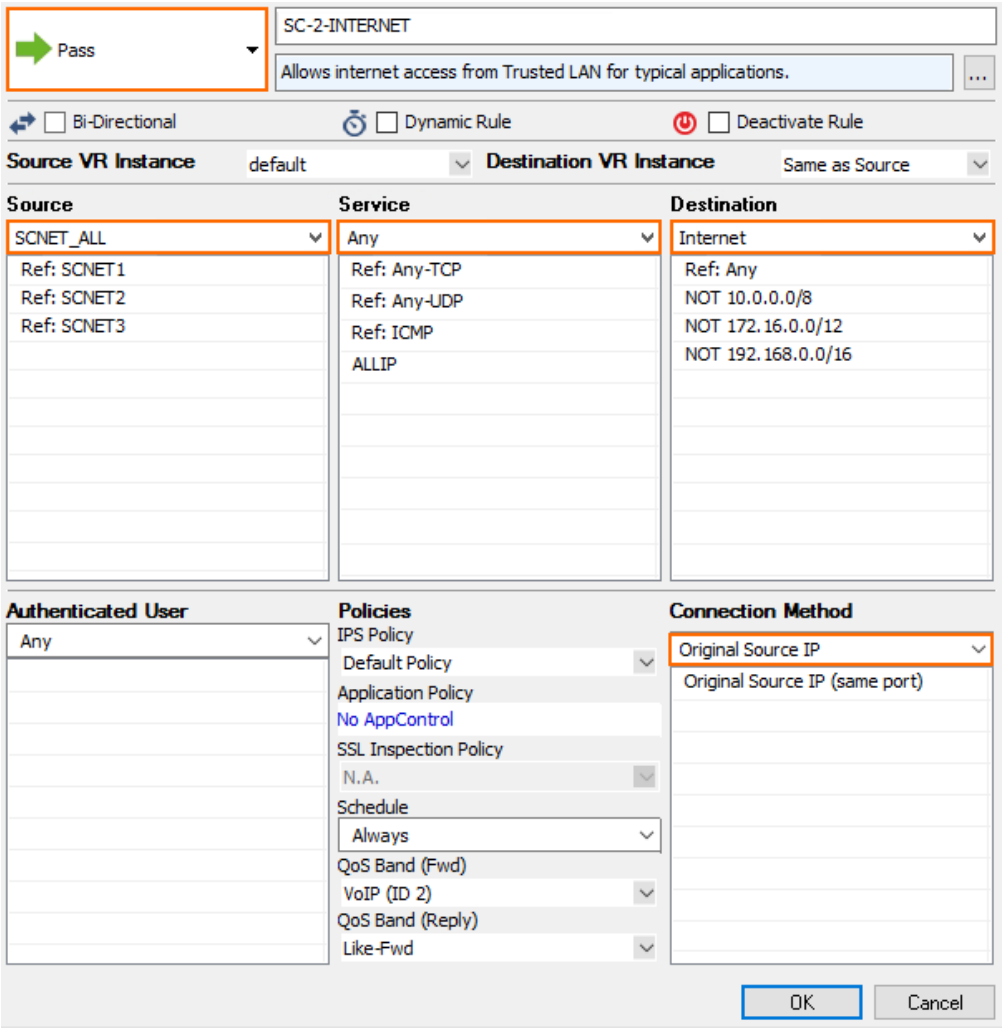
4. Create a PASS access rule to allow all other traffic from the Secure Connector VIP network(s):
   - **Action** – Select **PASS**.
   - **Source** – Select the Secure Connector VIP network(s) associated with this Access Controller.
   - **Service** – Select the service you want to allow.
   - **Destination** – Select the destination network
   - **Connection** – Select **Original Source IP**.



5. (optional) Create a PASS access rule to allow Internet access from the Secure Connector VIP network(s):

   You must use `0.0.0.0/0` as the **Remote Network** in the Secure Connector VPN settings.

   - **Action** – Select **PASS**.
   - **Source** – Select the Secure Connector VIP network(s) associated with this Access Controller.
   - **Service** – Select the service you want to allow.
   - **Destination** – Select **Internet**.
   - **Connection** – Select **Original Source IP**.



6. Adjust the order of the access rules, so that no rule above them matches the same traffic.
7. Click **Send Changes** and **Activate**.

(optional) Configure the CloudGen Border Firewall

For the data networks assigned to the Secure Connectors to be able to reach on-premises networks or the Internet, the border firewall must be configured to route and allow traffic to these networks using the Access Controller as the default gateway. Also, create a Dst NAT access rule to redirect incoming Secure Connector VPN tunnels to the Access Controller.

Step 1. Add Gateway Routes

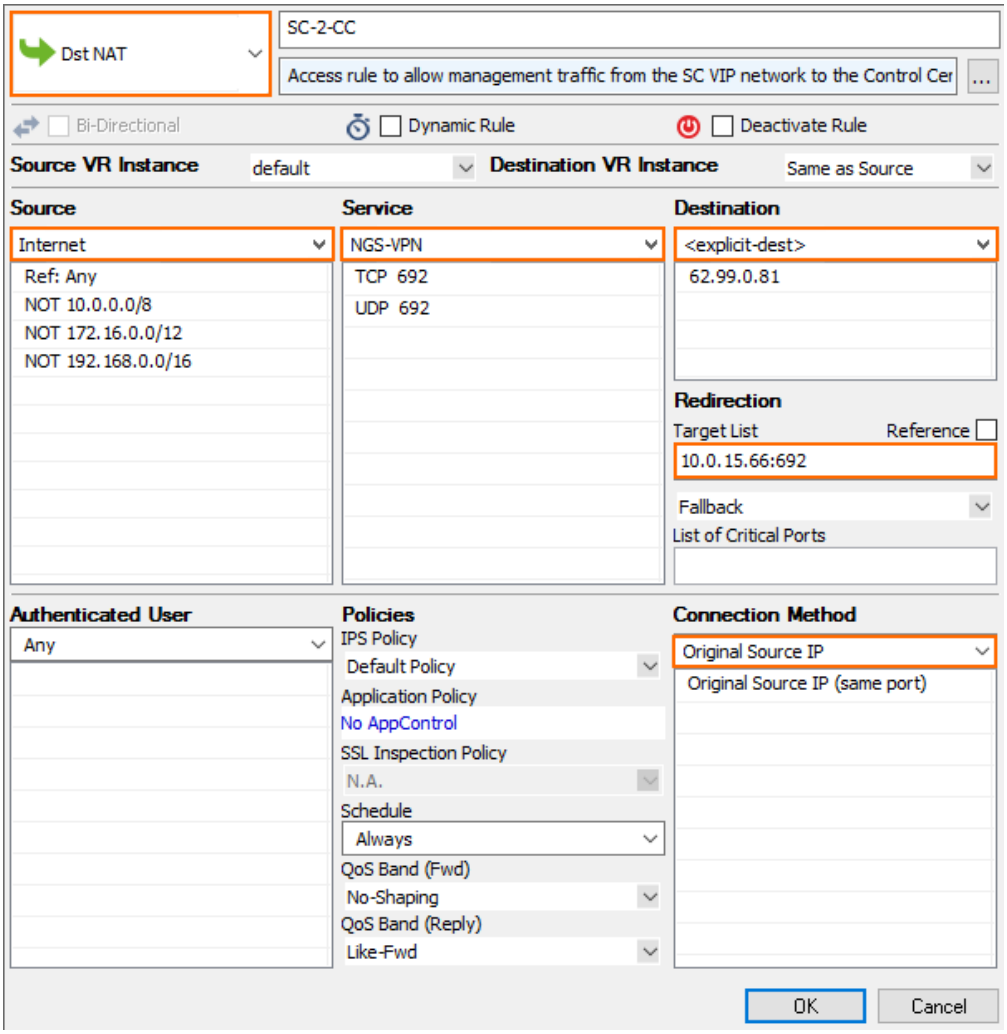
Configure a gateway route to send traffic for the Secure Connector data networks through the Access Controller.

1. Go to ***your cluster*** **>** **Boxes** **>** ***your border CloudGen Firewall*** **>** **Network**.
2. Click **Lock**.

3. Add a gateway route for every Secure Connector data network assigned to the Access Controller.
   - **Target Network Address** – Enter the Secure Connector VIP network.
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the server IP of the Access Controller.
4. Click **Send Changes** and **Activate**.
5. Activate the network configuration. For more information, see How to Activate Network Changes.

Step 2. Forward Incoming Secure Connector VPN Tunnels to the Access Controller

1. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your Access Controller virtual server*** **>** **Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a PASS access rule to allow management traffic from the Secure Connector VIP network to the Control Center:
   - **Action** – Select **Dst NAT**.
   - **Source** – Select **Internet**.
   - **Service** – Select the **NGS-VPN** service object for the incoming Secure Connector VPN tunnel. Default: TCP 692
   - **Destination** – Enter the IP address used as the **VACC Entry Point** in Step 7.
   - **Connection** – Select **Original Source IP**.
   - **Redirect to** – Enter the server IP address the Access Controller is listening on. If a non-standard port is used, add the port number: E.g., `10.0.15.66:692`



4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Step 2. Add Access Rules to Allow Secure Connector Traffic

Create access rules to allow traffic from the Secure Connector network to the local networks and/or to the Internet.

1. Go to ***your cluster*** **> Virtual Servers >** ***your CloudGen border Firewall virtual server*** **> Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Add the following PASS access rule for access to other networks reachable by the border firewall:
   - **Action** – Select **PASS**.
   - **Source** – Select the network object containing the Secure Connector networks.
   - **Service** – Select the service object. E.g., **HTTP+S**
   - **Destination** – Select the destination networks.
   - **Connection** – Select **Dynamic NAT** for Internet and connections to the same subnet
4. Add the following access rule to allow devices and users in a Secure Connector network access

to the Internet:
- **Action** – Select **PASS**.
- **Source** – Select the network object containing the Secure Connector networks.
- **Service** – Select the service object. E.g., **HTTP+S**
- **Destination** – Select **Internet**.
- **Connection** – Select **Dynamic NAT** for Internet and connections to the same subnet.

5. Click **Send Changes** and **Activate**.

Configure the Firewall Control Center

The Control Center manages the configuration for all Secure Connector devices and the associated Access Controller. The Control Center communicates with the Secure Connectors on TCP 889. If the Control Center and the Access Controller are in the same network, you must also add a gateway route. Otherwise, the Access Controller must be reachable via the default gateway of the Control Center.

Step 1. Enable CC Database Support

Enable CC database support on the box level of the Firewall Control Center.

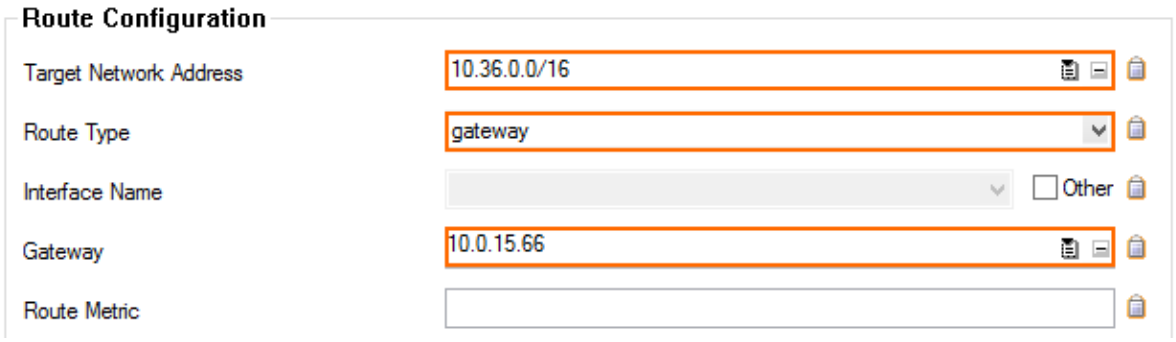
1. Log into the box layer of your Firewall Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > CC Database.**
3. Click **Lock**.
4. Set **Use CC Database** to **yes**.

5. Click **Send Changes** and **Activate**.

Step 2. Add a Gateway Route if Access Controller and Control Center are in the Same Subnet

If the Secure Access Controller and the Control Center are in the same subnet, you must add a gateway route to direct all Secure Connector traffic directly to the Access Controller. If the Access Controller is reachable via the default gateway of the Firewall Control Center, proceed with the next step.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. Add a gateway route for every Secure Connector management network:
   - **Target Network Address** – Enter the Secure Connector VIP network.
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the Server IP of the Access Controller.



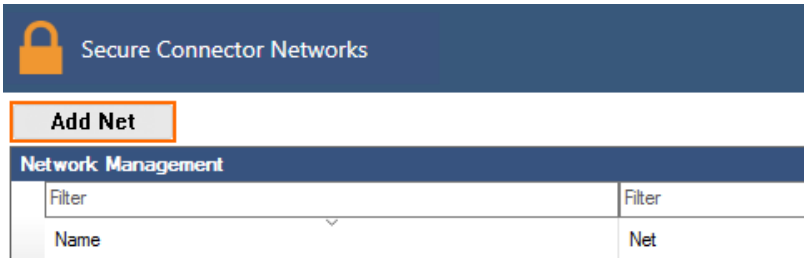
4. Click **Send Changes** and **Activate**.
5. Activate the network configuration. For more information, see How to Activate Network Changes.

You can now reach the server IP address of every Access Controller from the Control Center.

Step 3. Add Secure Connector VIP Networks

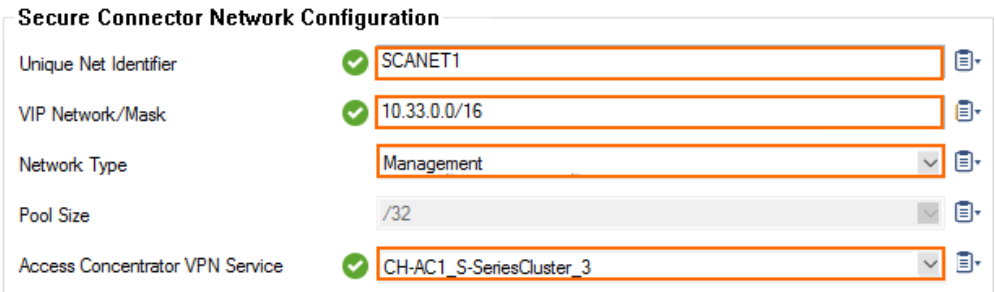
The individual Secure Connectors automatically receive a subnet from the Secure Connector VIP network defined on the Control Center. Choose a VIP network large enough to support the number of Secure Connector appliances you are deploying. Secure Connector networks cannot be resized later.

1. Log into the Control Center.
2. Go to **Multi-Range > Global Settings > Secure Connector Networks**.
3. Click **Lock**.
4. Click **Add Net**.



The **Create Net** windows opens.

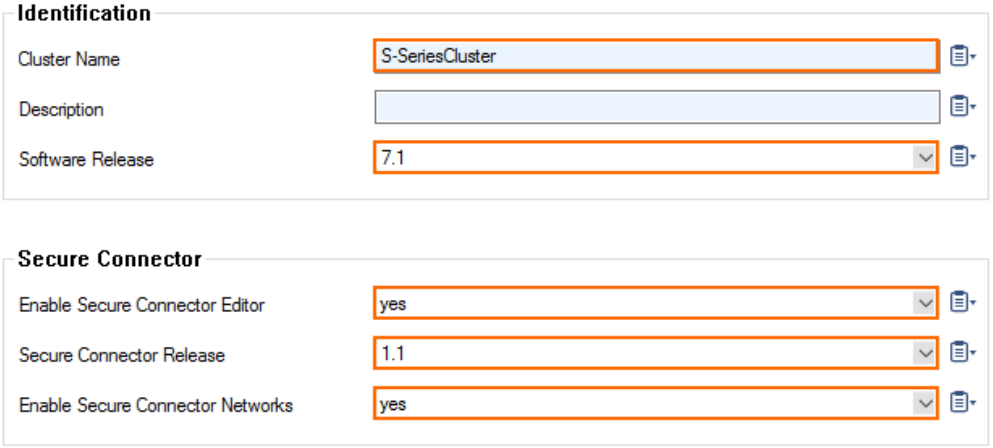
5. Enter the **Unique Net Identifier**.
6. Enter the **VIP Network/Mask**.
7. Select **Management** as the **Network Type**.
8. Select the **Access Controller VPN Service** this Secure Connector VIP network will be assigned to.



9. Click **OK**.
10. (optional) Create additional Secure Connector VIP networks.
11. Click **Send Changes** and **Activate**.

Step 3. Enable Secure Connector Support for the Cluster

1. Go to ***your cluster*** **> Cluster Properties**.
2. Click **Lock**.
3. Set **Enable Secure Connector Editor** to **yes**.
4. From the **Secure Connector Release** drop-down list, select the Secure Connector firmware version. E.g.: 1.1 for SC1.
5. Set **Enable Secure Connector Networks** to **yes**.



6. Click **Send Changes** and **Activate**.

Next Steps

- Create configurations for your Secure Connectors. For more information, see How to Add a Secure Connector Configuration.
- You can deploy the Secure Connector devices directly via configuration file. For more information, see Secure Connector Deployment via Configuration File

Figures

1. deploy_SAC_01.png
2. deploy_SAC_03.png
3. deploy_VACC_04.png
4. deploy_SAC_04a.png
5. deploy_SAC_05.png
6. deploy_SAC_02.png
7. deploy_SAC_06.png
8. sca_rule_1.png
9. sca_rule_02.png
10. sca_rule_03.png
11. sca_rule_04.png
12. deploy_CC_01.png
13. sca_route_01.png
14. add_net.png
15. create_net1.png
16. enable_fsc.png