Secure Access Concentrator and Control Center Deployment

https://campus.barracuda.com/doc/46209420/

To integrate Secure Connectors into your network, you must configure the Secure Access Concentrator and the NextGen Control Center to manage and route traffic from and to the SC VIP networks. The Control Center can manage multiple Secure Access Concentrators.

In this article:

Before You Begin

- Define the public IP address for **Point of Entry**. This is the public IP address through which the Secure Access Concentrator can be reached.
- Define the VIP 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 SC services:
  - **NGS-MGMT** – TCP/UDP 889 and TCP/UDP 888
  - **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 SC VIP networks. For more information, see Network Objects.
- You must have the license tokens for the Secure Access Concentrator and the SC Energize Updates pool license.
- You must have a fully licensed and configured Control Center running at least 6.2.1 with SC hotfix, or 6.2.2 without hotfix. For more information, see NextGen Control Center

Deploy and Configure a Secure Access Concentrator

Step 1. Deploy an F-Series Image to be used as the SAC

Deploy a virtual F-Series Firewall and assign the F-Series VF model, CPU cores, storage, and RAM according to your SAC model.

NextGen S-Series SAC	F-Series VF Model	Number of Licensed Cores	Minimum Storage [GB]	Minimum Memory [GB]
SAC 400	VF1000	2	80	2
SAC 600	VF2000	4	80	2
SAC 800	VF4000	8	80	2

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

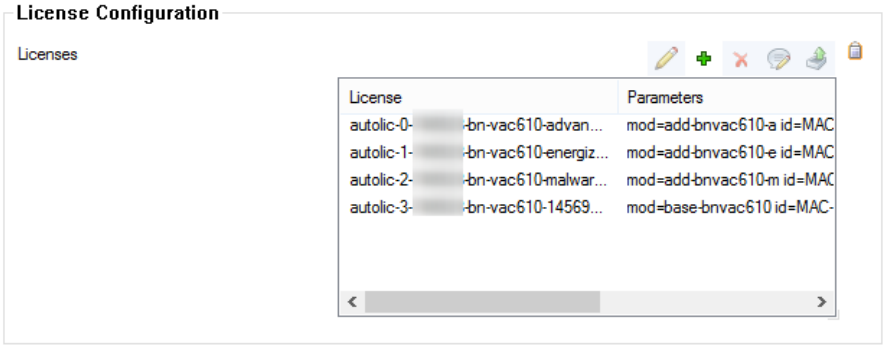
Step 2. Import the SAC into the Control Center

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

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

Step 3. License the Secure Access Concentrator

License and activate the SAC using Barracuda Activation on the Control Center. The licenses are automatically downloaded and assigned to the SAC. Go to ***your SAC*** > **Box Licenses** and verify that the licenses are installed.

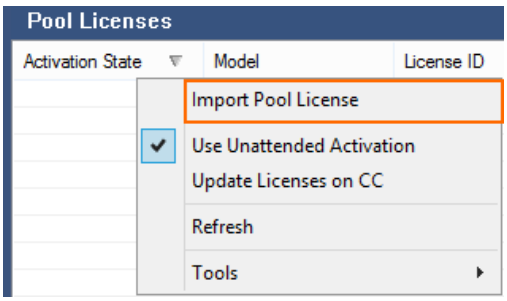


For more information, see How to Assign and Activate Single Licenses on a Control Center.

Step 4. Import SC Pool License

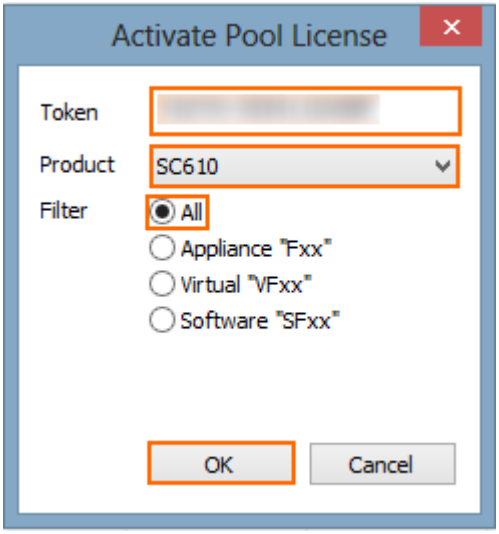
Import and activate the SC Energize Updates pool license. Each SC EU pool license is assigned to one SAC and determines the number of Secure Connectors that are allowed to connect to that SAC.

1. Log in to 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 SC Energize Updates license **Token**.

5. From the **Filter** list, select **All**.
6. From the **Product** list, select your SCA model: **SC400**, **SC610**, or **SC820.**
7. Click **OK**.

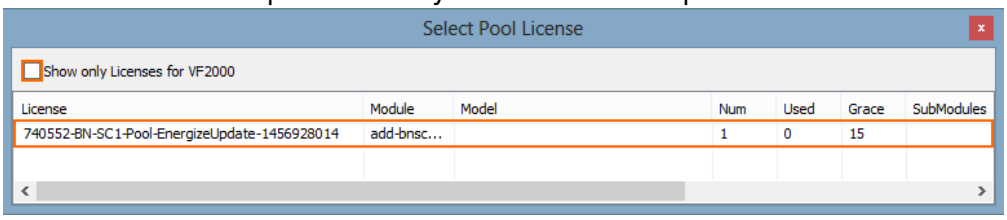


8. Fill in the **Activation Form**. Wait for the license to be activated and downloaded.

Step 5. Assign the SC pool license to the SAC

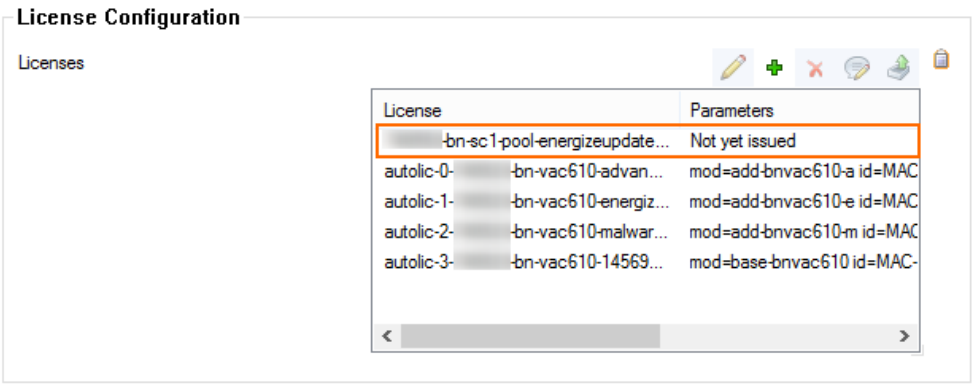
Add the SC EU pool license to the SAC licenses.

1. Log in to the Control Center.
2. Go to ***your Cluster* > *your SAC* > Box Licenses.**
3. Click **Lock**.
4. In the **Licenses** list, click **+** and select **Import from Pool Licenses.** The **Select Pool Licenses** window opens.
5. Clear the **Show only Licenses for VFxxx** check box.
6. Double-click on the pool license you installed in step 4.



7. Click **Send Changes** and **Activate**.

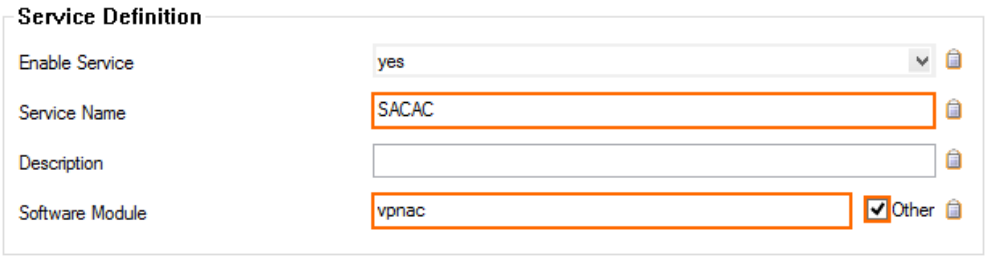
The SC pool license is now added to the SAC licenses.



Step 6. Create SAC VPN Service

Create the access concentrator VPN service.

1. Log in to the Control Center.
2. Go to ***your Cluster*** **>** **Virtual Servers** **>** ***your SAC virtual server*** **>** **Assigned Services** .
3. Right-click **Assigned Services** and select **Create Service**.
4. Enter a **Service Name**. The name must be unique and no longer than six characters. The service name cannot be changed later.
5. To enter the **Software Module**, click **Other** and enter vpnac.



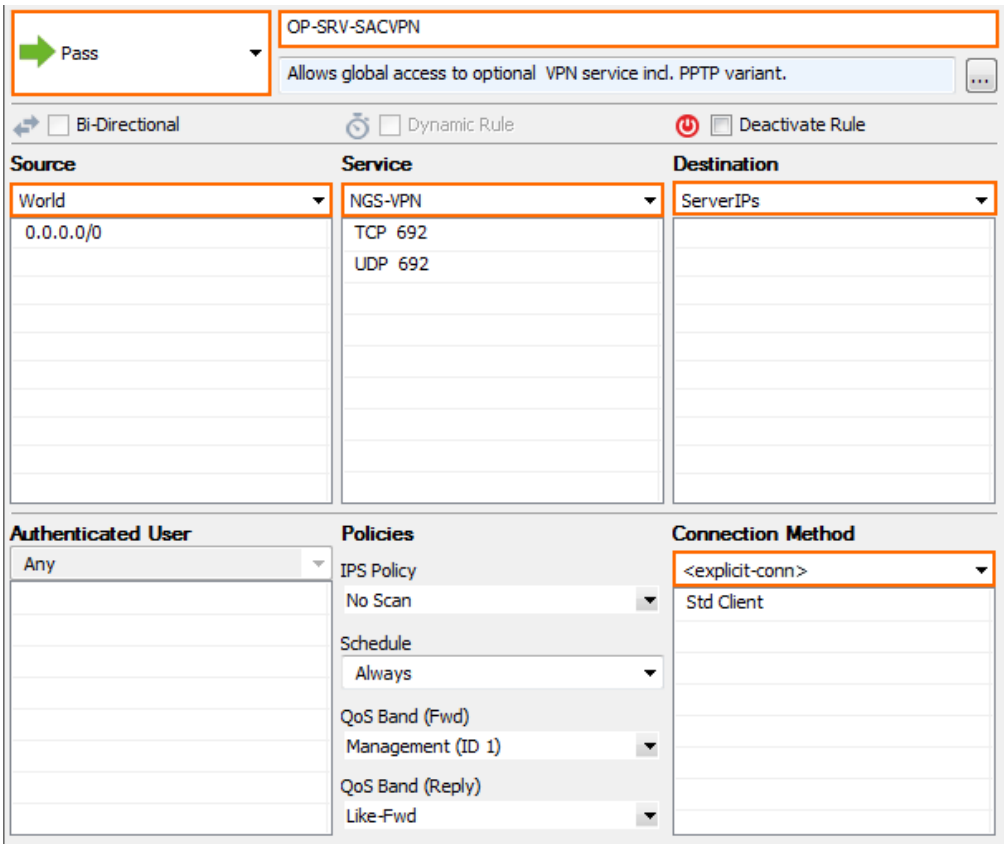
6. (optional) Change the **Service IPs**. For more information, see How to Configure Services.
7. Click **Finish**.
8. Click **Activate**.

Step 7. Create a Host Firewall Rule for the SAC VPN Service

If necessary, create the host firewall rule for the SAC VPN service.

1. Log in to the Control Center.
2. Go to ***your SAC*** **> Infrastructure Services > Host Firewall > Host Firewall Rules**.
3. Click **Lock**.
4. Add the following PASS access rule:
   - **Action** – Select **PASS**.
   - **Name** – Enter OP-SRV-SACVPN.
   - **Source** – Select **World**.
   - **Service** – Select the **NGS-VPN** service object
   - **Destination** – Select **ServerIPs**.

- **Connection** – Select **No Src NAT [Client]**.

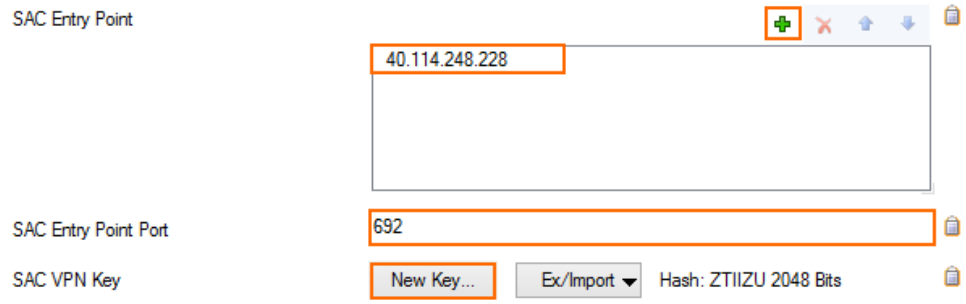


5. Click **OK**.
6. Use drag-and-drop to place the rule above the OP-SRV-VPN rule.
7. Click **Send Changes** and **Activate**.

Step 8. Configure SAC Access Concentrator VPN Service

Create the SAC VPN key used to authenticate the SCs. Then, enter the IP address and port the SCs will use to connect to this SAC. If managed F-Series Firewalls will also connect through the same public IP address, change the port to avoid redirecting the F-Series Firewall management tunnels to the SAC.

1. Log in to the Control Center.
2. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your SAC virtual server*** **>** **Assigned Services** **>** **SAC VPN** **>** **SAC VPN Settings**.
3. Click **Lock**.
4. In the left menu, click **S-Series SAC Settings**.
5. Click **+** and enter the public IP address the SCs use to connect as the **SAC Entry Point**.
6. (optional) Enter the **SAC Entry Point Port**. Default: 692
7. Click **New Key** to create a **SAC VPN Key**.

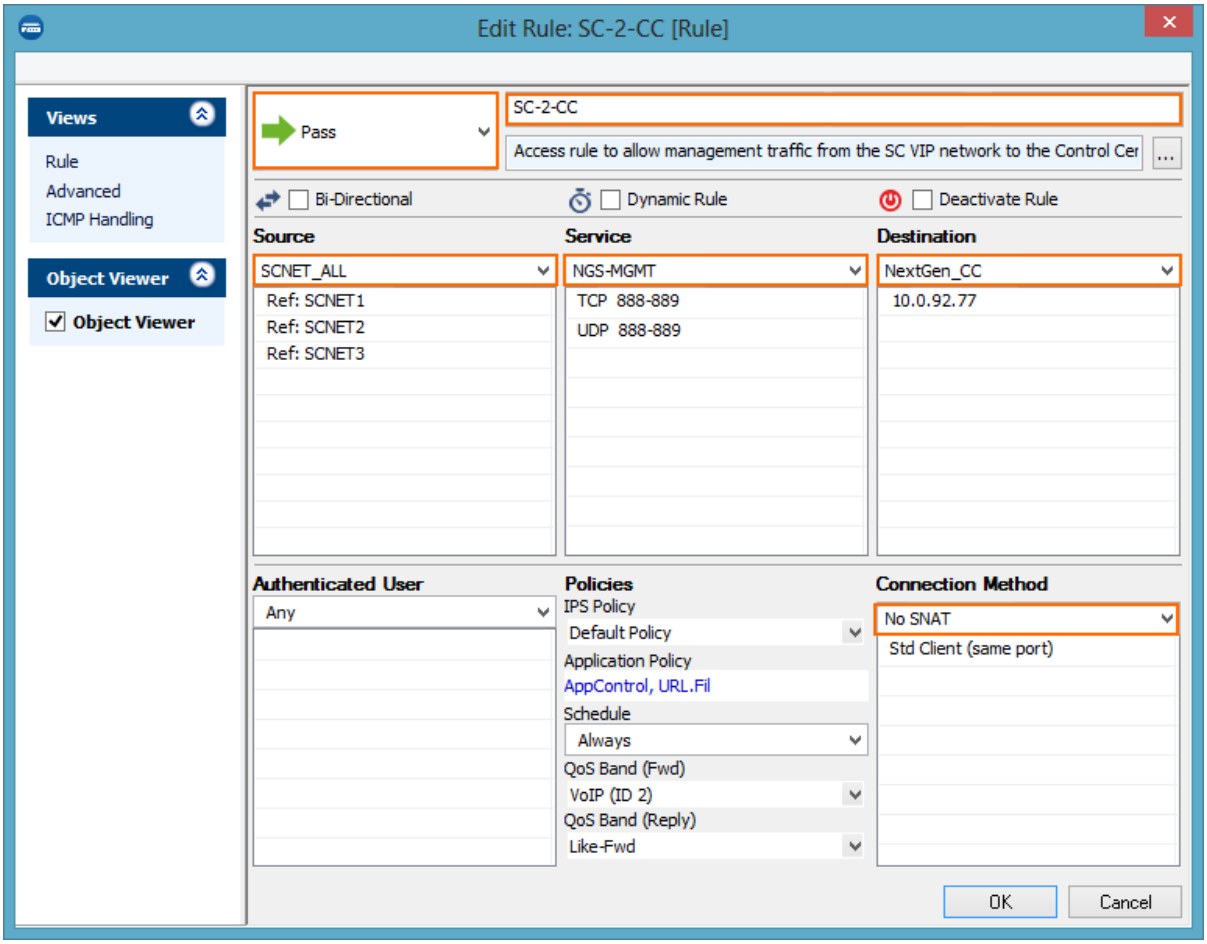


8. Click **Send Changes** and **Activate**.

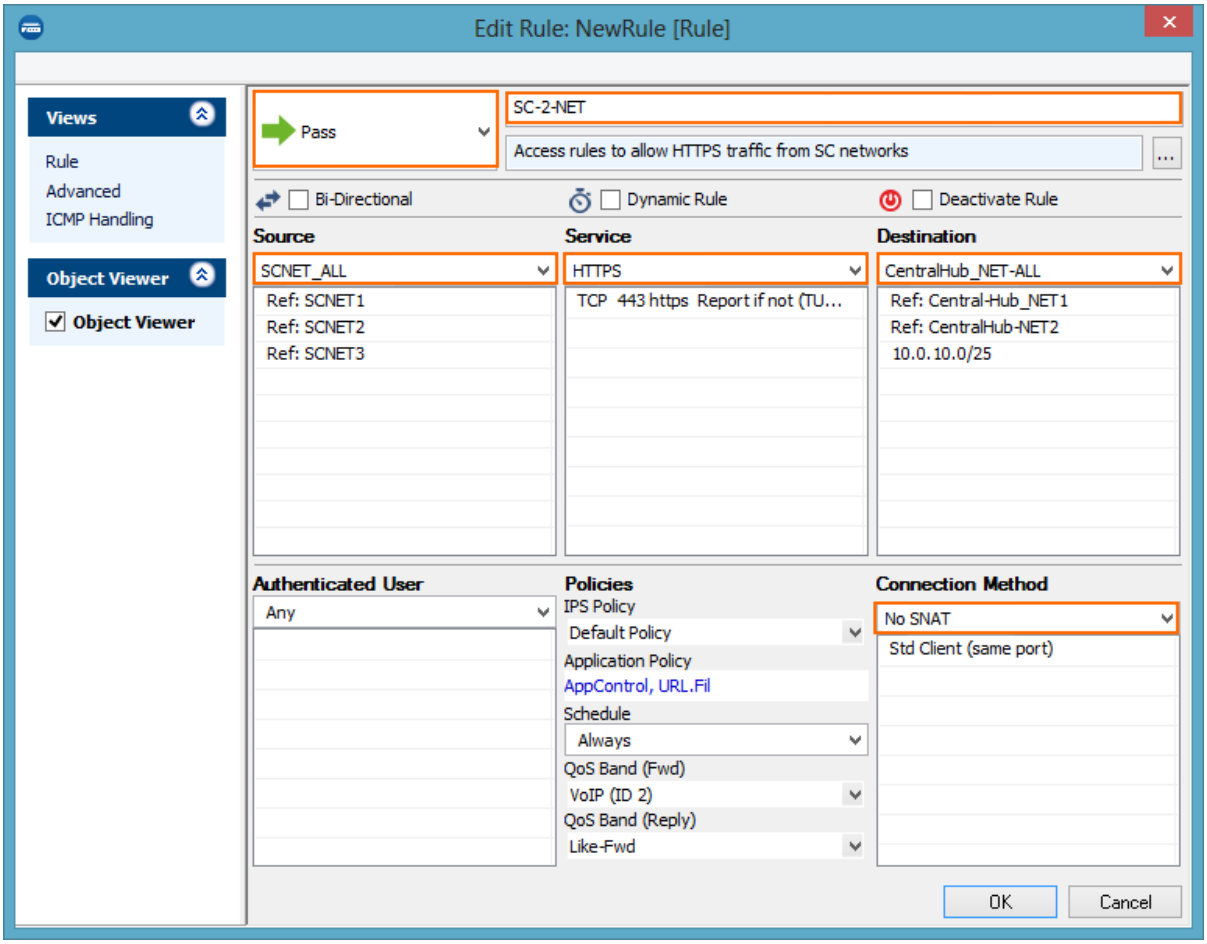
Step 9. Add Access Rules for SC VIP Network

Create access rules to allow SC traffic to the Control Center and to the border firewall. TCP/UDP 888 is used for communication initiated from the SC to the Control Center. TCP/UDP 889 is used for communication initiated from the Control Center to the SC.

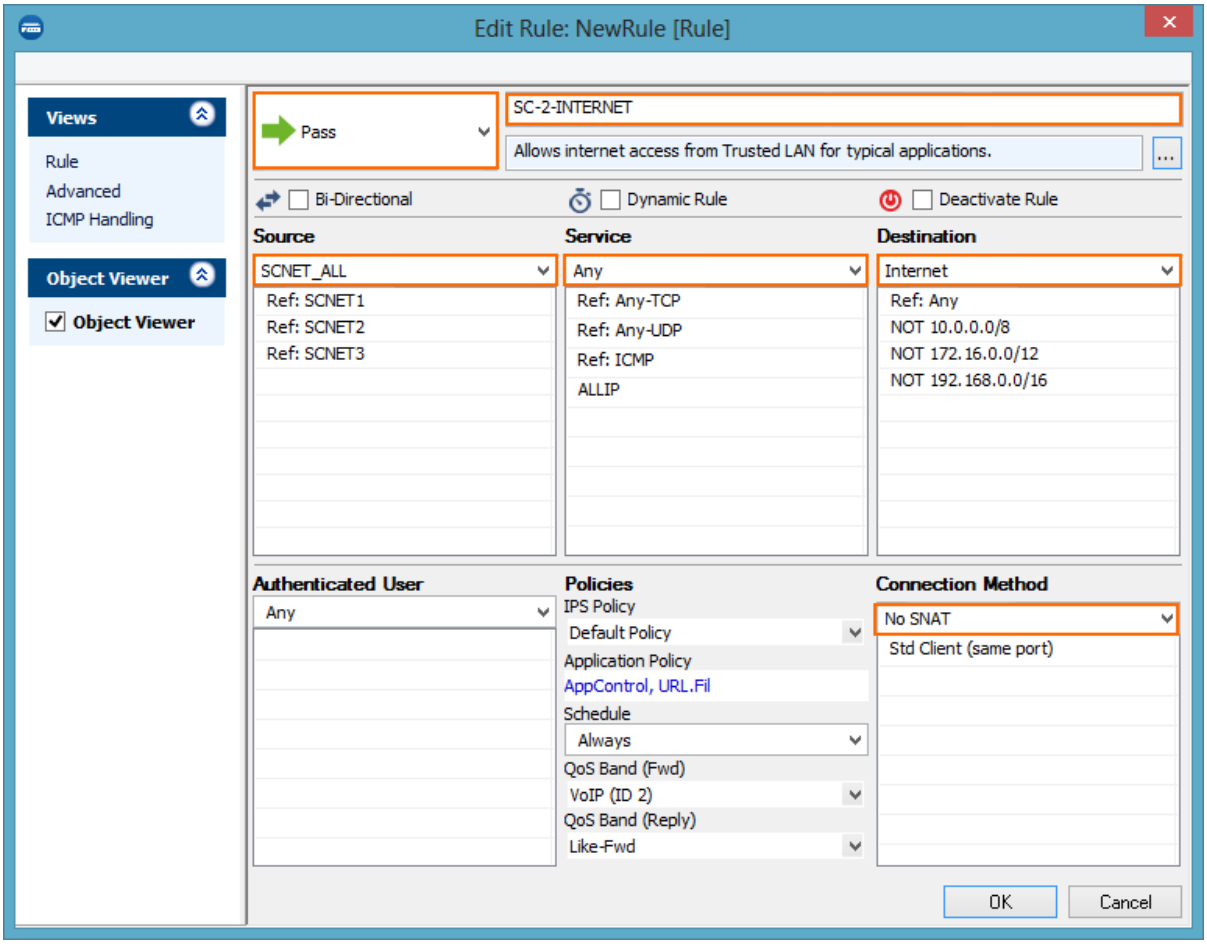
1. Log in to the Control Center.
2. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your SAC virtual server*** **>** **Assigned Services** **>** **Firewall** **>** **Forwarding Rules**.
3. Click **Lock**.
4. Create a PASS access rule to allow management traffic from the SC VIP network to the Control Center:
   - **Action** – Select **PASS**.
   - **Source** – Select the SC VIP network(s) associated with this SAC.
   - **Service** – Select the **NGS-MGMT** service object for SC management traffic: TCP/UDP 889 and TCP/UDP 888.
   - **Destination** – Select the network object for the Control Center IP address.
   - **Connection** – Select **No SNAT**.



5. Create a PASS access rule to allow all other traffic from the SC VIP network(s):
   - **Action** – Select **PASS**.
   - **Source** – Select the SC VIP network(s) associated with this SAC.
   - **Service** – Select the service you want to allow.
   - **Destination** – Select the destination network
   - **Connection** – Select **No SNAT**.



6. (optional) Create a PASS access rule to allow Internet access from the SC VIP network(s):
   You must use `0.0.0.0/0` as the **Remote Network** in the SC VPN Settings.
   - **Action** – Select **PASS**.
   - **Source** – Select the SC VIP network(s) associated with this SAC.
   - **Service** – Select the service you want to allow.
   - **Destination** – Select **Internet**.
   - **Connection** – Select **No SNAT**.



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

(optional) Configure the F-Series Border Firewall

The border firewall acts as the default gateway for all traffic from the SC VIP networks. You must configure routing and access rules to allow traffic from the SC and SAC to the Control Center and the networks the devices behind the SC must connect to.

Step 1. Add Gateway Routes

Configure a gateway route to send traffic for the SC VIP networks through the SAC.

1. Log into the Control Center.
2. Go to ***your cluster*** **>** **Boxes** **>** ***your border F-Series Firewall*** **>** **Network**.
3. Click **Lock**.
4. Add a gateway route for every SC VIP network assigned to the SC Access Cluster:
   - **Target Network Address** – Enter the SC VIP network.
   - **Route Type** – Select **gateway**.

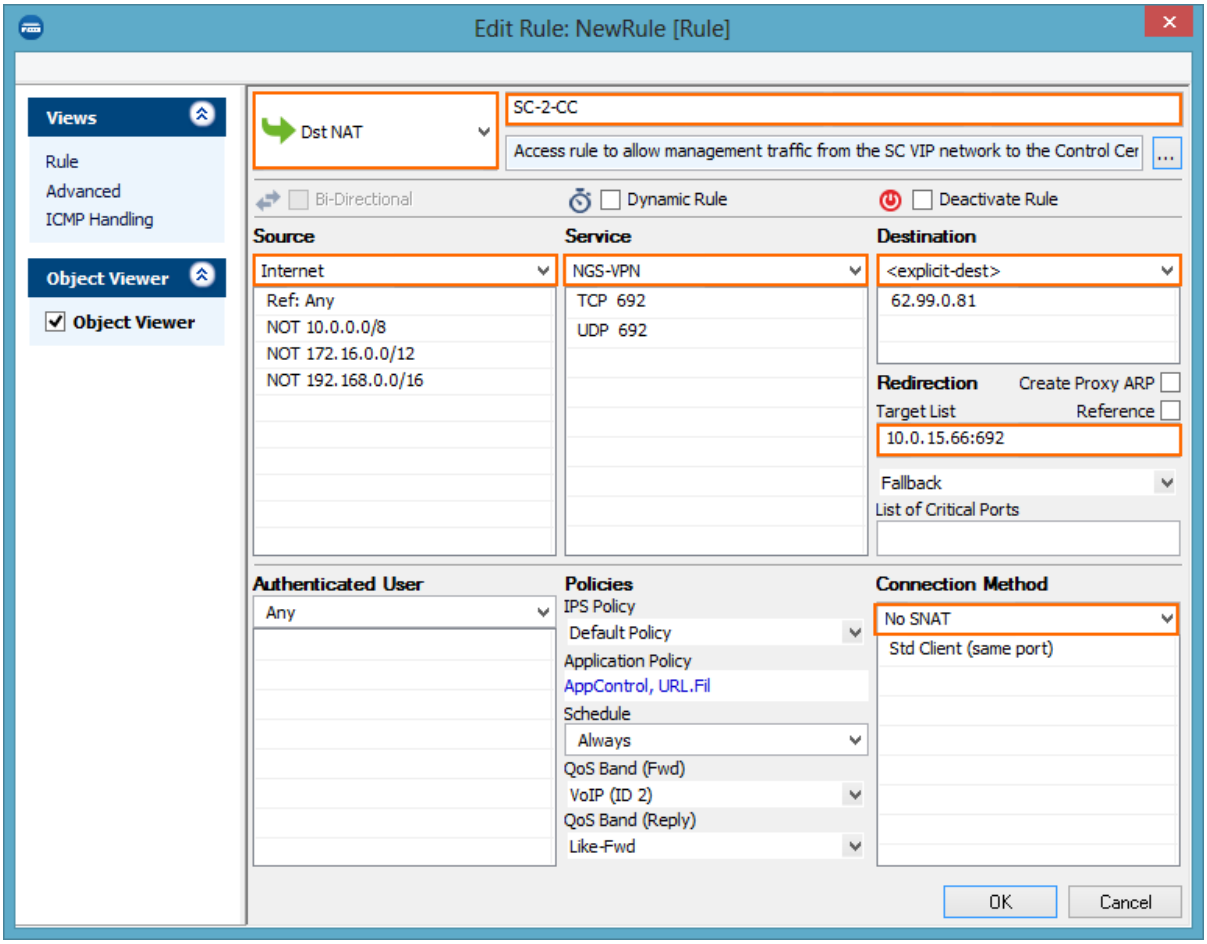
- **Gateway** – Enter the Server IP of the SAC.

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

Step 2. Forward Incoming SC Tunnels to the SAC

Create a DNAT access rule to forward incoming SC VPN connections to the SAC. Use a separate public IP address if the same border firewall also forwards F-Series Firewall management tunnels to the Control Center.

1. Log into the Control Center.
2. Go to ***your cluster*** **>** **Virtual Servers** **>** ***your SAC virtual server*** **>** **Assigned Services** **> Firewall > Forwarding Rules**.
3. Click **Lock**.
4. Create a PASS access rule to allow management traffic from the SC VIP network to the Control Center:
   - **Action** – Select **Dst NAT**.
   - **Source** – Select **Internet**
   - **Service** – Select the **NGS-VPN** service object for the incoming SC VPN tunnel. Default: TCP/UDP 692
   - **Destination** – Enter the IP address used as the **SAC Entry Point**.
   - **Connection** – Select **No SNAT**.
   - **Redirect to** – Enter the Server IP address the SAC is listening on. If a non-standard port is used, add the port number: E.g., 10.0.15.66:692



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

Step 3. Add Access Rules to Allow SC Traffic

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

1. Log into the Control Center.
2. Go to ***your cluster*** **> Virtual Servers >** ***your F-Series border Firewall virtual server*** **> Assigned Services > Firewall > Forwarding Rules.**
3. Click **Lock**.
4. 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 SC networks.
   - **Service** – Select the service object. E.g., **HTTP+S**
   - **Destination** – Select the destination networks.
   - **Connection** – Select **Dynamic SNAT** for Internet and connections to the same subnet
5. Add the following access rule to allow devices and users in an SC network access to the Internet:
   - **Action** – Select **PASS**.
   - **Source** – Select the network object containing the SC networks.

- **Service** – Select the service object. E.g., **HTTP+S**
- **Destination** – Select **Internet**.
- **Connection** – Select **Dynamic SNAT** for Internet and connections to the same subnet

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

Configure the NextGen Control Center

The Control Center manages the configuration for all S-Series devices and the associated F-Series Firewalls used as border firewalls. The Control Center communicates with the SC on TCP/UDP 889 and TCP/UDP 888. If the Control Center and the SAC are in the same network, you must also add a gateway route. Otherwise, the SAC 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 NextGen Control Center.

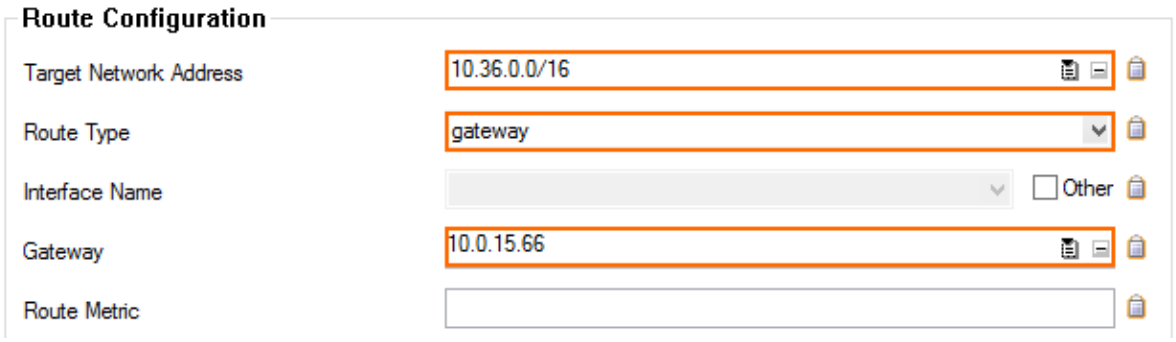
1. Log into the box layer of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > CC Database.**
3. Click **Lock**.
4. Set **Use CC Database** to **yes**.

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

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

If the Secure Access Concentrator and the Control Center are in the same subnet, you must add a gateway route to direct all SC traffic directly to the Access Concentrator. If the SAC can be reached via the default gateway of the NextGen Control Center, proceed with the next step.

1. Log into the box layer of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu click on **Routing**.
5. Add a gateway route for every SC VIP network: For more information, see How to Configure Gateway Routes.
   - **Target Network Address** – Enter the SC VIP network.
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the Server IP of the SAC.



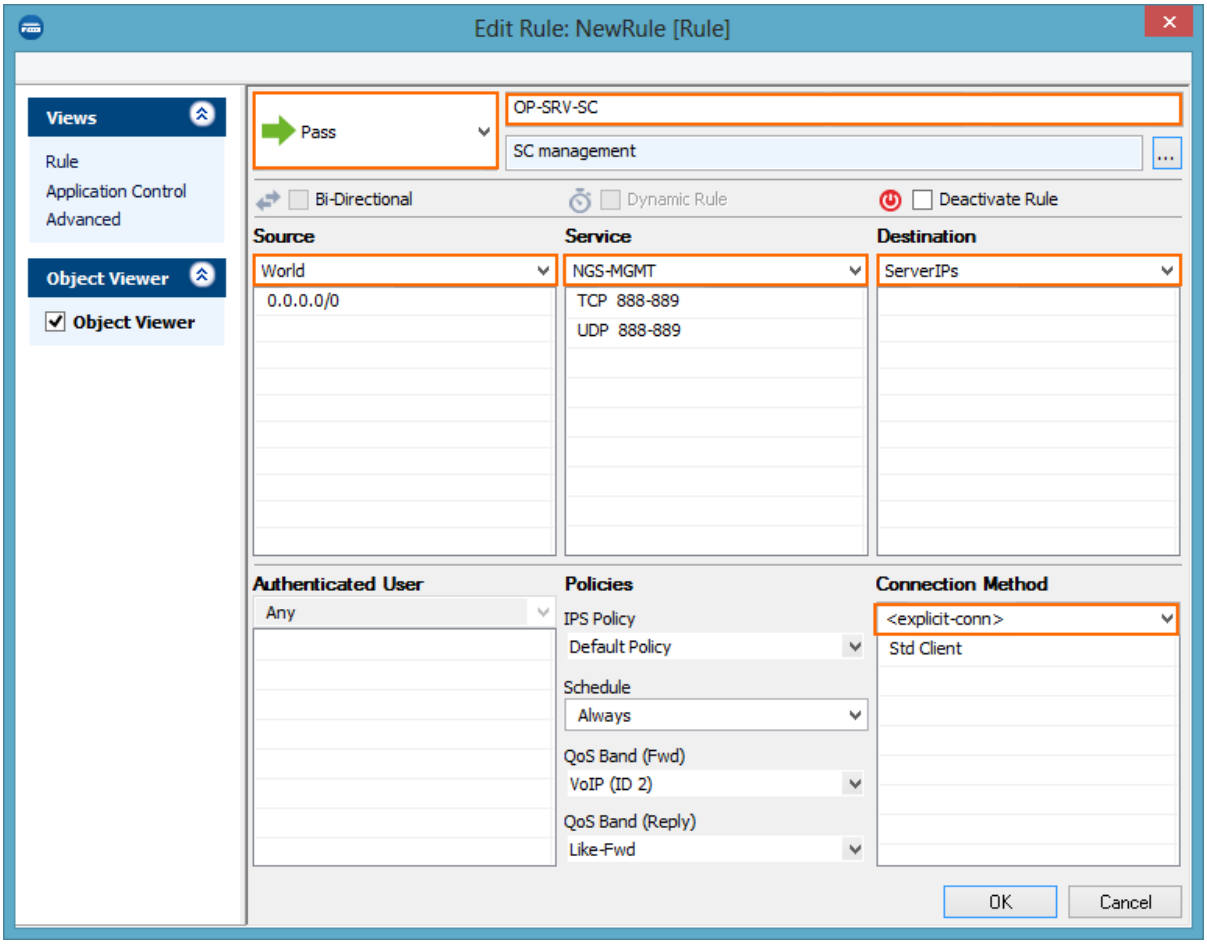
6. Click **Send Changes** and **Activate**.
7. Activate the network configuration. For more information, see How to Activate Network Changes.

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

Step 3. Verify the Host Firewall Rule for S-Series Management Access

If necessary, create the host firewall rule for SC management.

1. Log into the box layer of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall > Host Firewall Rules** .
3. Click **Lock**.
4. Add the following PASS access rule:
   - **Action** – Select **PASS**.
   - **Name** – Enter OP-SRV-SC.
   - **Source** – Select **World**.
   - **Service** – Select the **NGS-MGMT** service object for SC management traffic: TCP/UDP 889 and TCP/UDP 888.
   - **Destination** – Select **Server IPs**.
   - **Connection** – Select **No Src NAT [Client]**.



5. Click **OK**.
6. Use drag-and-drop to place the host firewall rule so that no rule above it matches the same traffic.
7. Click **Send Changes** and **Activate**.

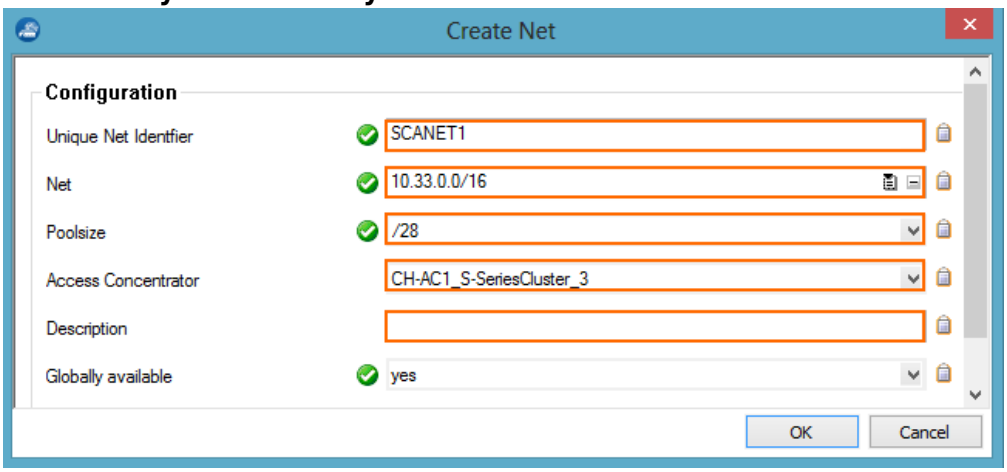
Step 4. Configure SC VIP Networks

The individual S-Series SCs automatically receive a subnet from the SC VIP network defined on the Control Center. Choose a VIP network large enough to support the number of SC appliances you are deploying. SC networks cannot be resized later. The Wi-Fi access point uses a separate network and does not need to be accounted for when choosing the SC subnet size.

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

The **Create Net** windows opens.

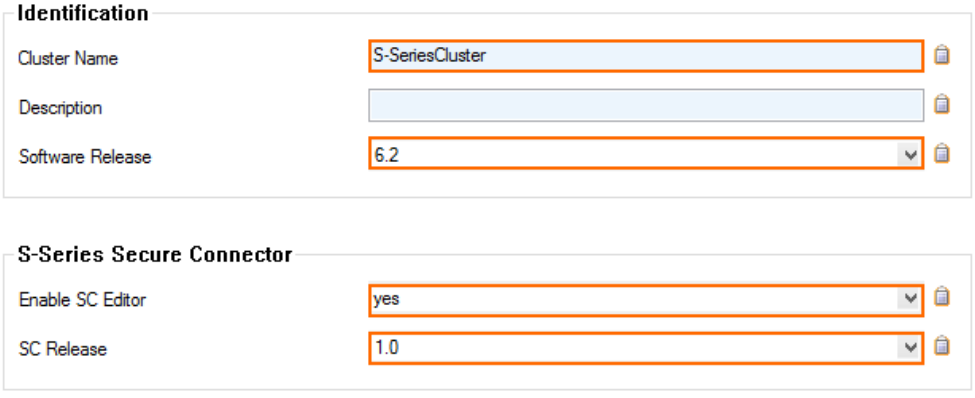
5. Enter the **Unique Net Identifier**.
6. Enter the **Net** address.
7. Select the **Poolsize**. Recommended pool size: /28
8. Select the **Access Concentrator** this SC VIP network will be assigned to.
9. Set **Globally available** to **yes** for this network to be visible to all CC admins.



10. Click **OK**.
11. (optional) Create additional SC VIP networks.
12. Click **Send Changes** and **Activate**.

Step 5. Enable S-Series Support for the Cluster

1. Log into the Control Center.
2. Go to ***your cluster*** **> Cluster Properties** .
3. Click **Lock**.
4. Set **Enable SC Editor** to **yes**.
5. From the **SC Release** drop-down list, select the SC major firmware version.



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 SC devices either directly via configuration file or by connecting to the SAC using the VPN deployment mode.
  - SC Deployment via SC Configuration File
  - SC Deployment via VPN Deployment Mode

Figures

1. deploy_SAC_01.png
2. deploy_SAC_03.png
3. deploy_SAC_04.png
4. deploy_SAC_04a.png
5. deploy_SAC_05.png
6. deploy_SAC_02.png
7. deploy_SAC_02a.png
8. deploy_SAC_06.png
9. sca_rule_01.png
10. sca_rule_02.png
11. sca_rule_03.png
12. sca_rule_04.png
13. deploy_CC_01.png
14. sca_route_01.png
15. sca_rule_05.png
16. add_SC_NET.png
17. create_net.png
18. enable_sc.png