Secure Access Concentrator and Control Center Deployment

https://campus.barracuda.com/doc/48203287/

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 FSC VIP networks. The Control Center can manage multiple Secure Access Concentrators.

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 FSC 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 FSC VIP networks. For more information, see Network Objects.
- You must have the license tokens for the Secure Access Concentrator and the FSC Energize Updates pool license.

Deploy and configure a Secure Access Concentrator

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

Deploy a virtual or public cloud F-Series Firewall. Verify that the number of CPU cores, storage, and RAM according are sized according to your FSAC model. If your FSAC is deployed in Azure or AWS, see Secure Access Concentrator in Azure and AWS for more information how to integrate the FSAC with your existing cloud resources.

NextGen FSC-Series FSAC	Model	Number of Licensed Cores	Minimum Storage [GB]	Minimum Memory [GB]
FSAC 400	VF1000	VF1000 / ACC400	80	2
FSAC 600	VF2000	VF2000 / ACC610	80	2
FSAC 800	VF4000	VF4000 / ACC820	80	2

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

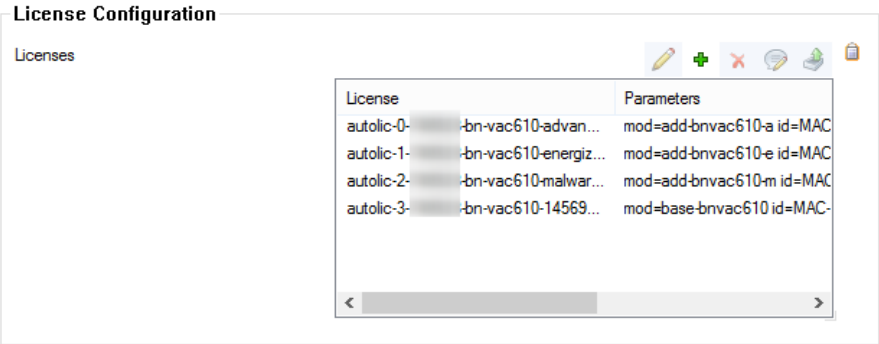
Step 2. Import the FSAC into the Control Center

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

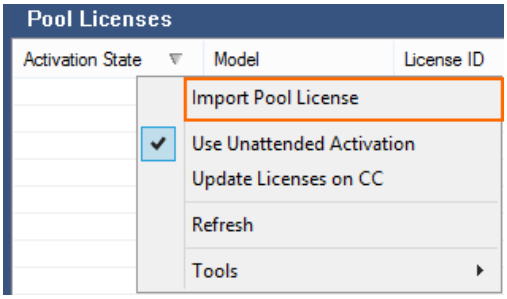


For more information, see How to Assign and Activate Single Licenses on a Control Center.

Step 4. Import the FSC pool license

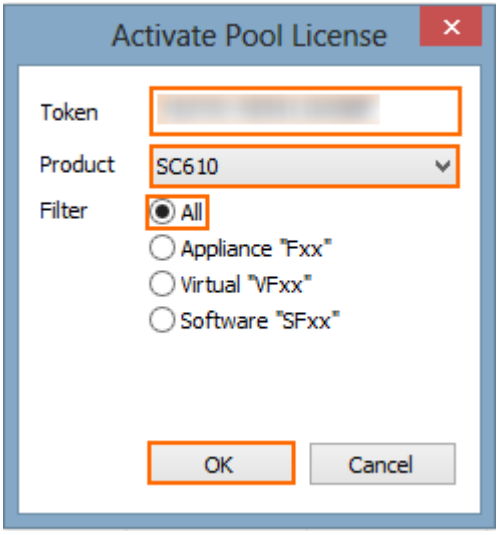
Import and activate the FSC Energize Updates pool license. Each FSC EU pool license is assigned to one FSAC and determines the number of Secure Connectors that are allowed to connect to that FSAC.

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 FSC Energize Updates license **Token**.
5. From the **Filter** list, select **All**.
6. From the **Product** list, select your FSAC model: **FSAC400**, **FSAC610**, or **FSAC820.**

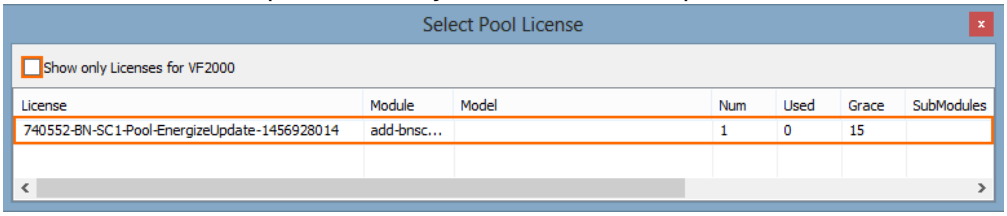
7. Click **OK**.



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

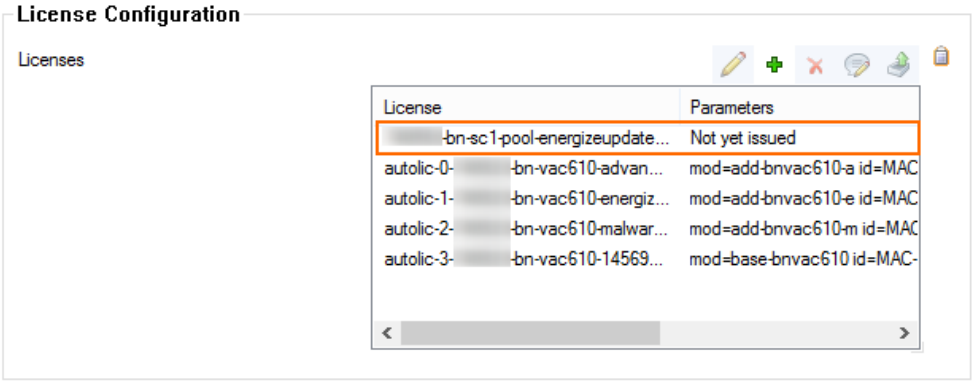
Step 5. Assign the FSC pool license to the FSAC

1. Go to ***your cluster*** **>** ***your FSAC*** **> 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 on the pool license you installed in step 4.



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

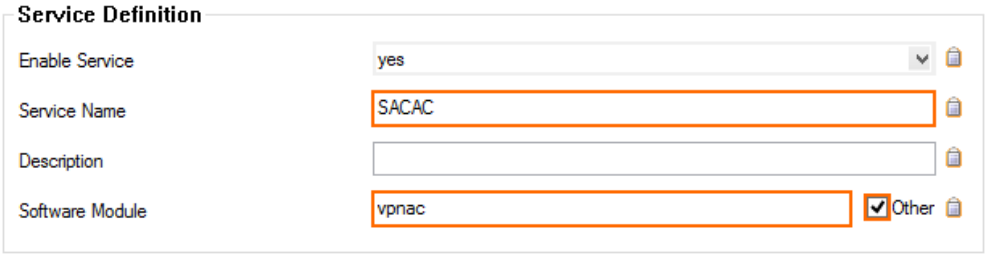
The FSC pool license is now added to the FSAC licenses.



Step 6. Create the FSAC VPN service

Create the access concentrator VPN service.

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. To enter the **Software Module**, click **Other** and enter vpnac.



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

Step 7. Configure the FSAC Access Concentrator VPN service

Create the FSAC VPN key used to authenticate the FSCs. Then, enter the IP address and port the FSCs will use to connect to this FSAC. 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 FSAC.

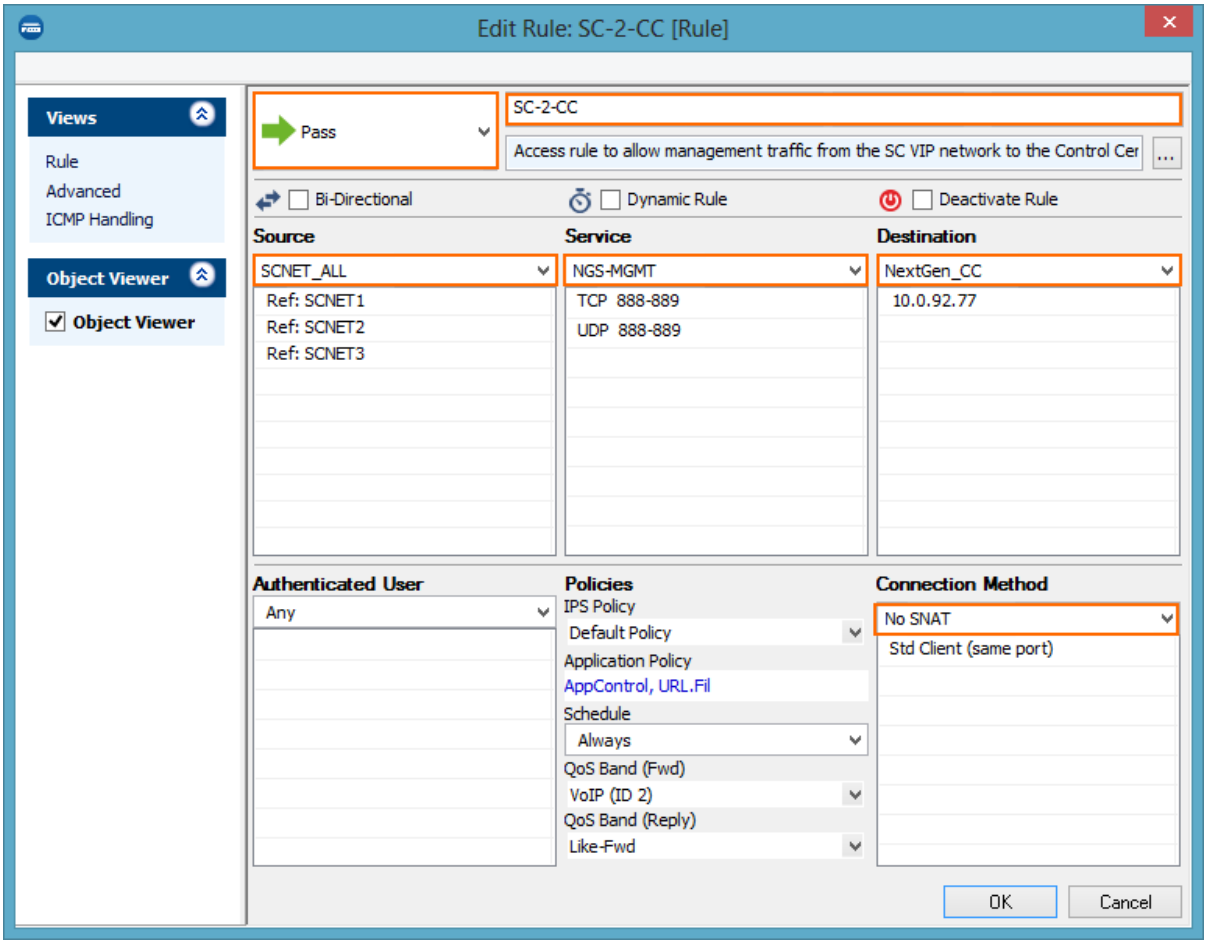
1. Go to ***your cluster*** > **Virtual Servers** > ***your FSAC virtual server*** > **Assigned Services** > **VPNAC** > **Master VPN Settings**.
2. Click **Lock**.
3. In the left menu, click **FSC-Series SAC Settings**.
4. Enter the public IP address the FSCs use to connect as the **SAC Entry Point**.
5. (optional) Enter the **SAC Entry Point Port**. Default: 692
6. Click **New Key** to create a **SAC VPN Key**.

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

Step 8. Add access rules for FSC-Series VIP network

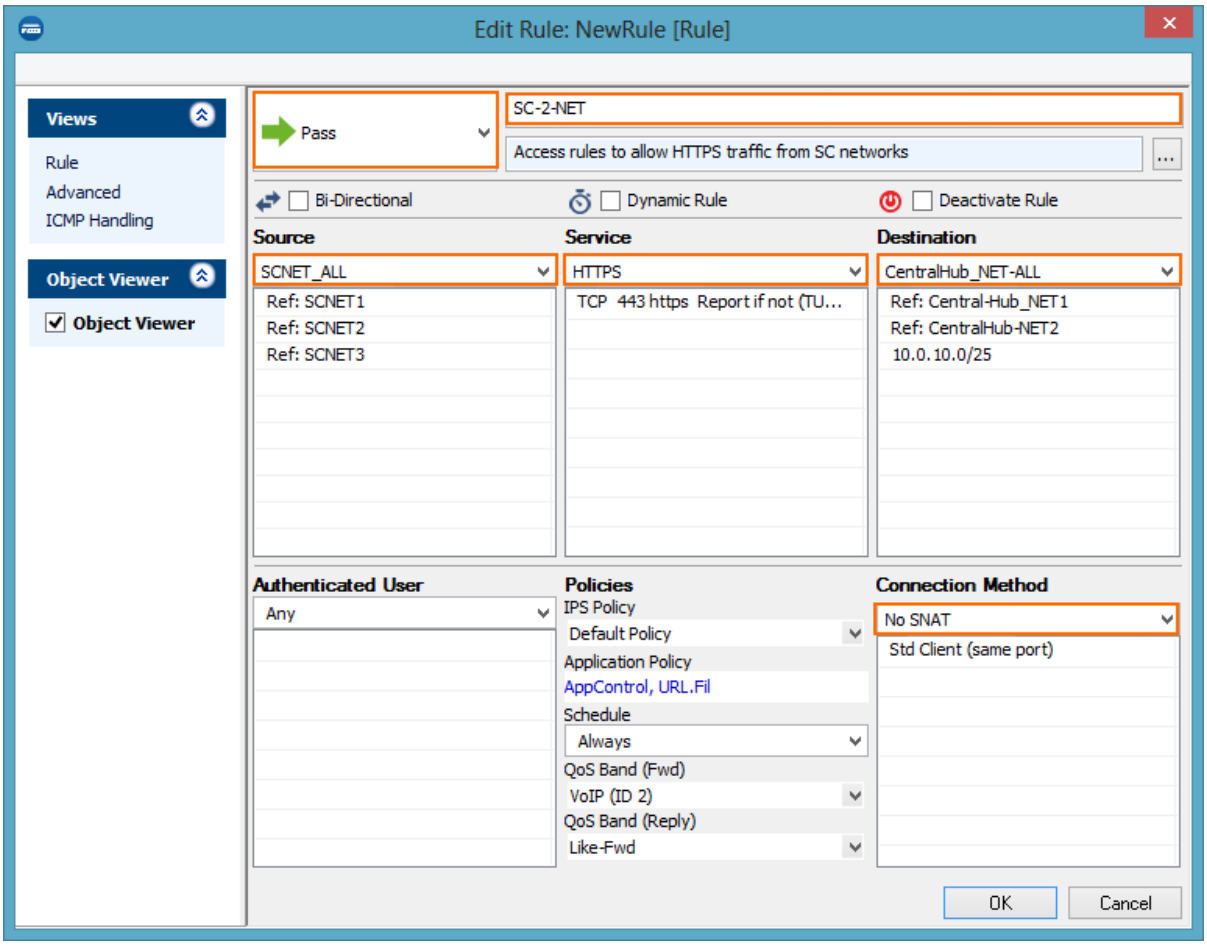
Create access rules to allow FSC traffic to the Control Center and to the border firewall. TCP/UDP 888 is used for communication initiated from the FSC to the Control Center. TCP/UDP 889 is used for communication initiated from the Control Center to the FSC.

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

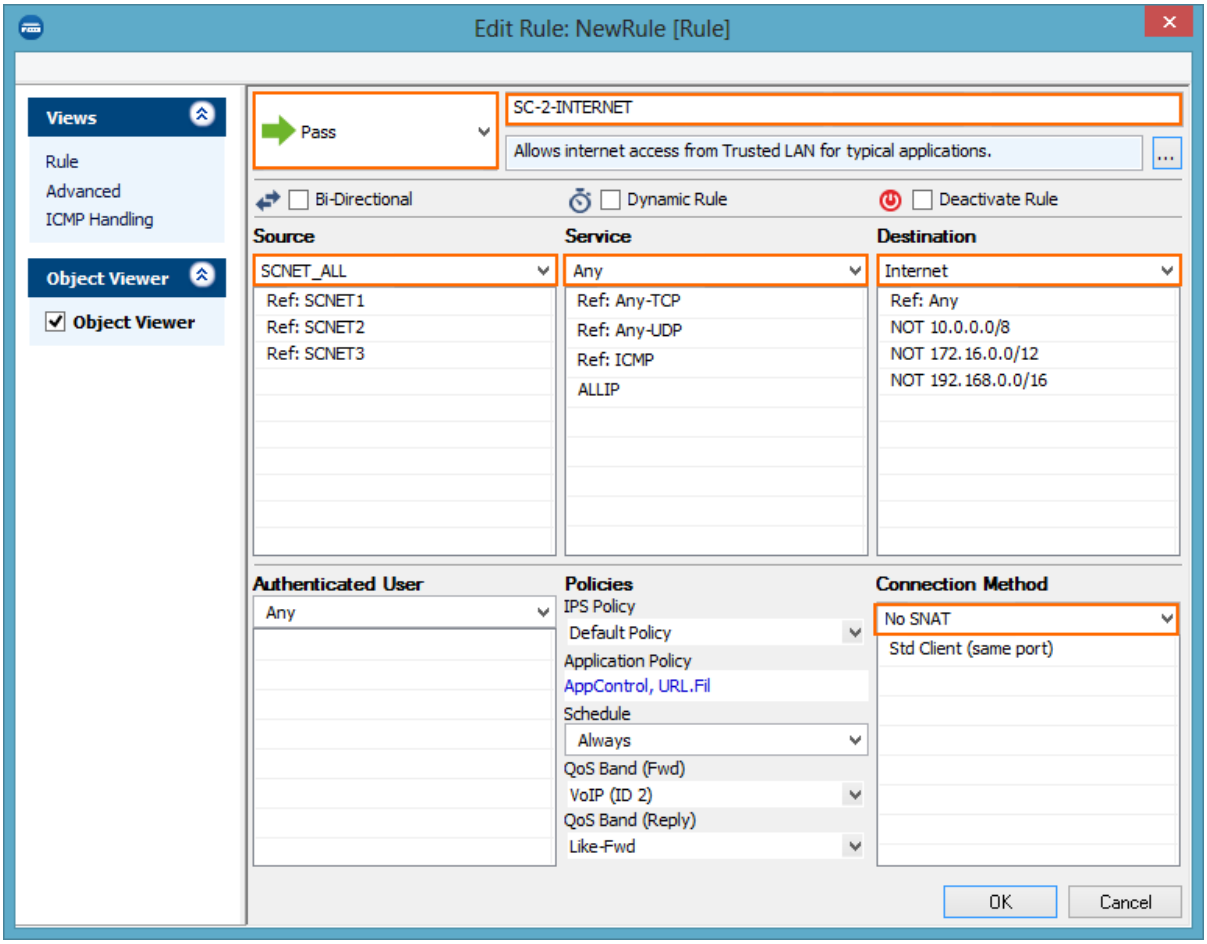


4. Create a PASS access rule to allow all other traffic from the FSC VIP network(s):
   - **Action** – Select **PASS**.
   - **Source** – Select the FSC VIP network(s) associated with this FSAC.
   - **Service** – Select the service you want to allow.

- **Destination** – Select the destination network
- **Connection** – Select **No SNAT**.



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



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 F-Series border firewall

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

Step 1. Add gateway routes

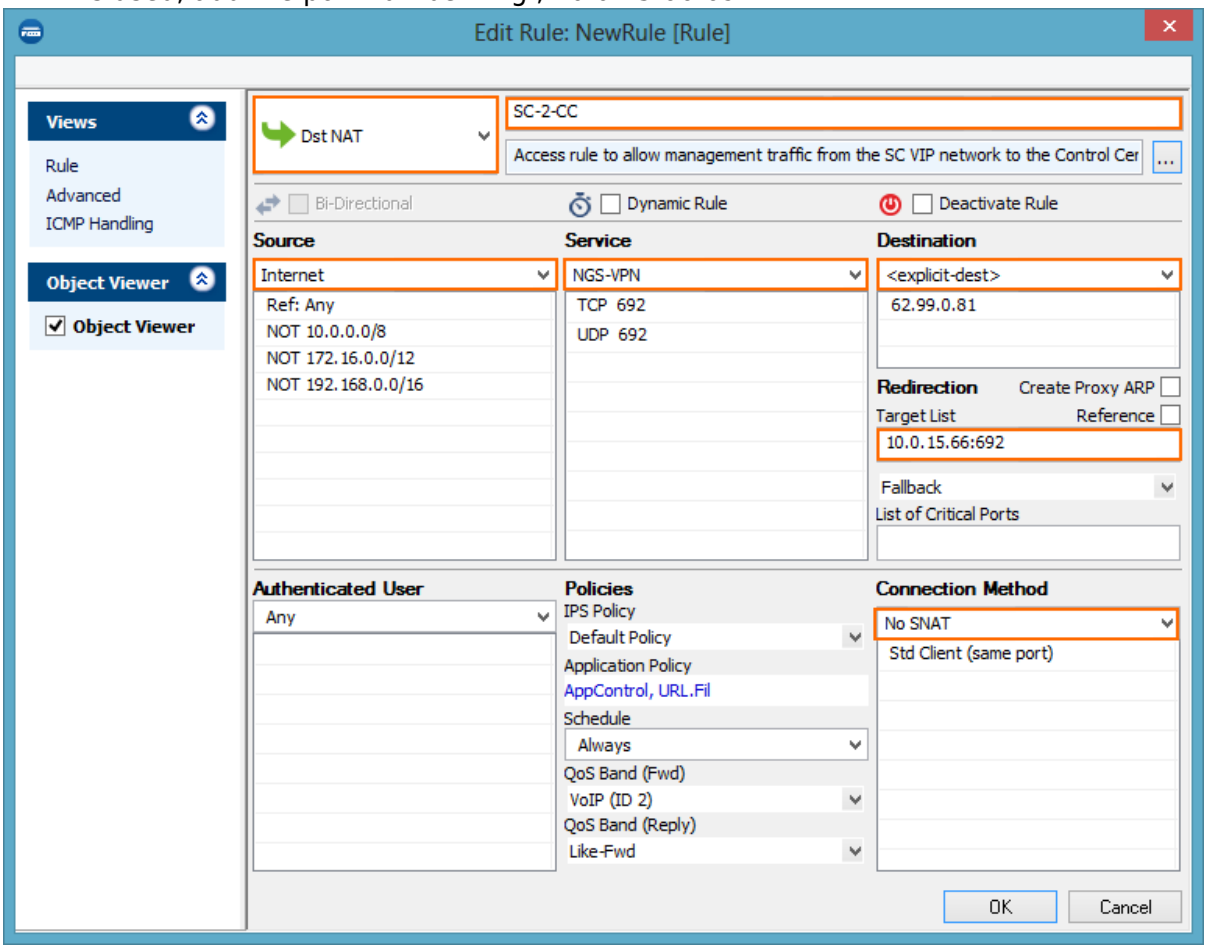
Configure a gateway route to send traffic for the FSC VIP networks through the FSAC.

1. Go to ***your cluster*** **>** **Boxes** **>** ***your border F-Series Firewall*** **>** **Network**.
2. Click **Lock**.
3. Add a gateway route for every FSC VIP network assigned to the FSC Access Cluster:
   - **Target Network Address** – Enter the FSC VIP network.
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the Server IP of the FSAC.

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

Step 2. Forward incoming FSC tunnels to the FSAC

1. Go to ***your cluster*** **> Virtual Servers >** ***your FSAC virtual server*** **> Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a PASS access rule to allow management traffic from the FSC VIP network to the Control Center:
   - **Action** – Select **Dst NAT**.
   - **Source** – Select **Internet**.
   - **Service** – Select the **NGS-VPN** service object for the incoming FSC VPN tunnel. Default: TCP/UDP 692
   - **Destination** – Enter the IP address used as the **SAC Entry Point** in Step 7.
   - **Connection** – Select **No SNAT**.
   - **Redirect to** – Enter the Server IP address the FSAC 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 FSC traffic

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

1. Go to ***your cluster*** **> Virtual Servers >** ***your F-Series 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 FSC 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
4. Add the following access rule to allow devices and users in an FSC network access to the Internet:
   - **Action** – Select **PASS**.
   - **Source** – Select the network object containing the FSC 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
5. Click **Send Changes** and **Activate**.

Configure the NextGen Control Center

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

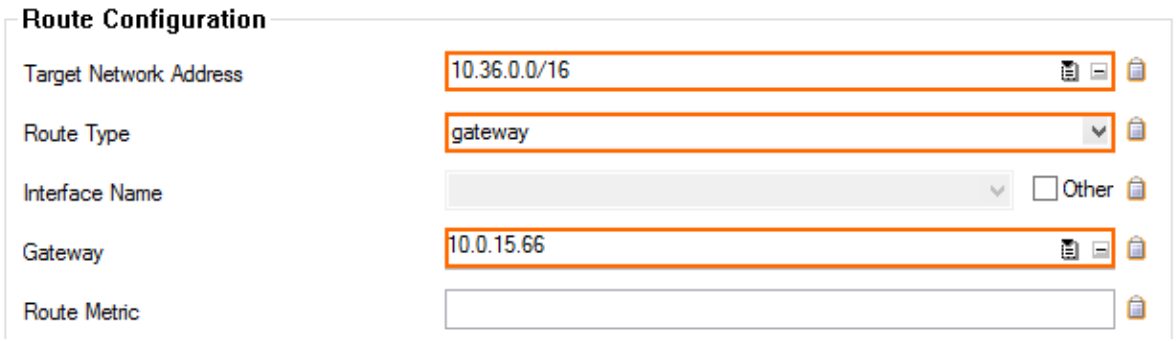
1. Log into the box layer of your NextGen Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > CC Database.**
3. Click **Lock**.
4. Set **Use CC Database** to **yes**.

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

Step 2. Add a gateway route if FSAC 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 FSC traffic directly to the Access Concentrator. If the FSAC can be reached via the default gateway of the NextGen 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 FSC VIP network:
   - **Target Network Address** – Enter the FSC VIP network.
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the Server IP of the FSAC.



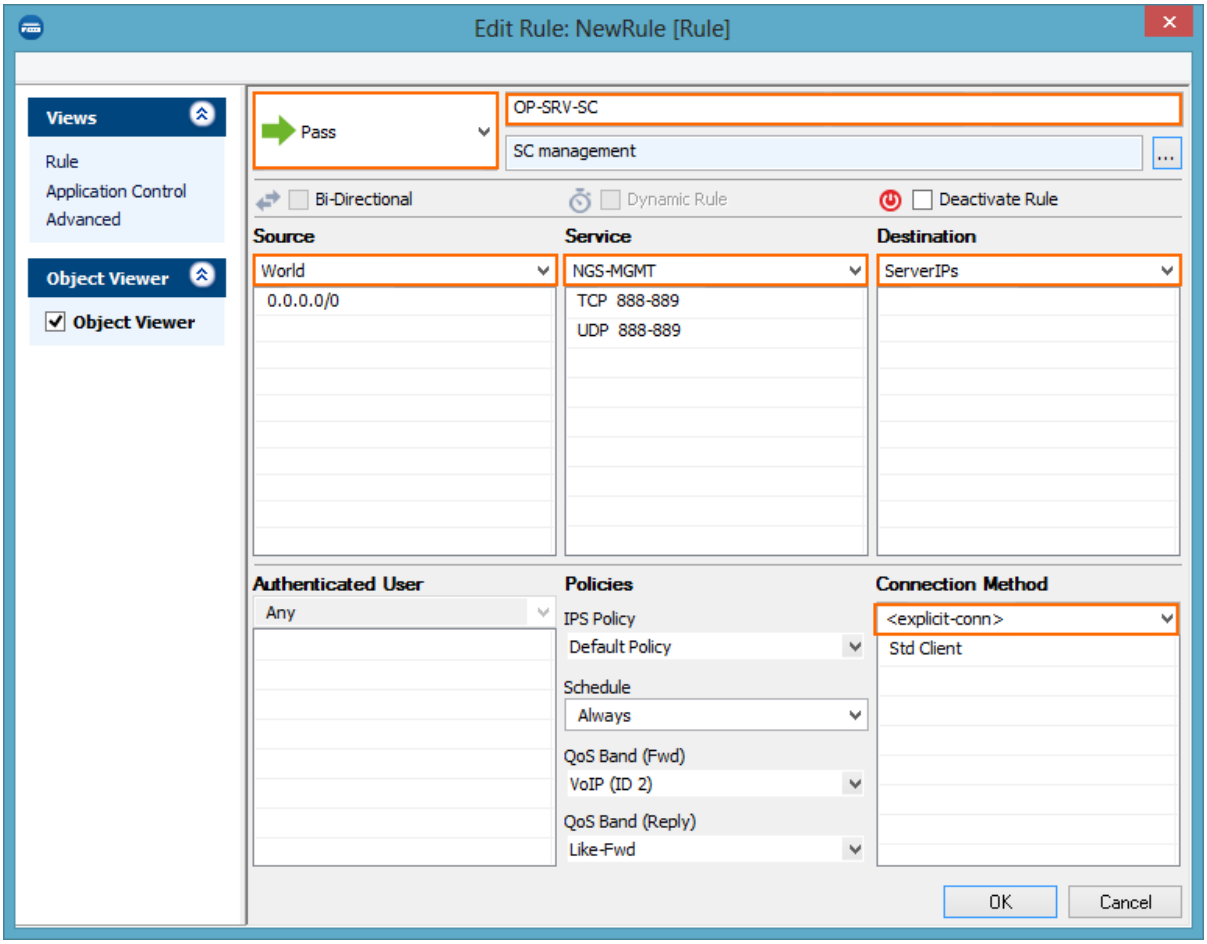
4. Click **Send Changes** and **Activate**.
5. Activate the network configuration. For more information, see How to Activate Network Changes.

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

Step 3. Verify the host firewall rule for FSC-Series management access

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

1. Log into the box level of the 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 0P-SRV-SC.
   - **Source** – Select **World**.
   - **Service** – Select the **NGS-MGMT** service object for FSC management traffic: TCP/UDP 889 and TCP/UDP 888.
   - **Destination** – Select **Server IPs**.
   - **Connection** – Select **No Src NAT [Client]**.

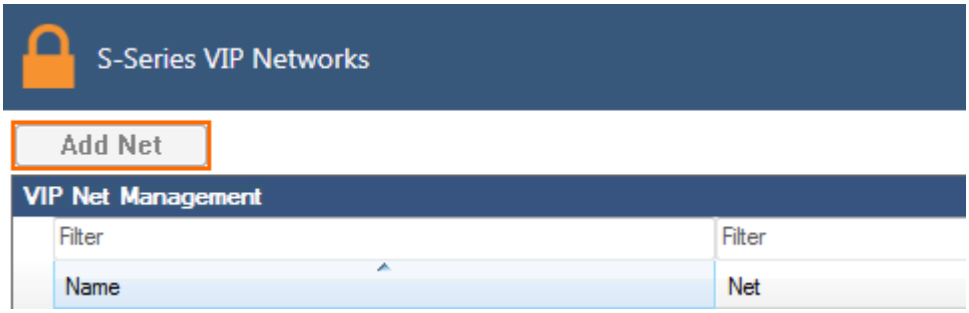


5. Click **OK**.
6. Use drag-and-drop to place the host firewall rule so that no rule above it matches the same traffic.
7. Click **Send Changes** and **Activate**.

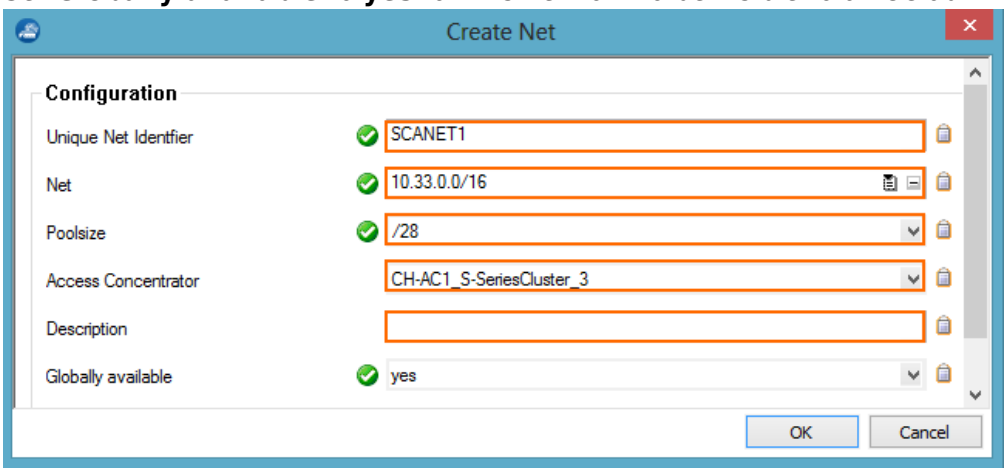
Step 3. Configure FSC-Series VIP networks

The individual FSC-Series FSCs automatically receive a subnet from the FSC VIP network defined on the Control Center. Choose a VIP network large enough to support the number of FSC appliances you are deploying. FSC 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 FSC subnet size.

1. Log into the Control Center.
2. Go to **Multi-Range > Global Settings > SCA VIP Net Management**.
3. Click **Lock**.
4. Click **Add Net**. The **Create Net** windows opens.



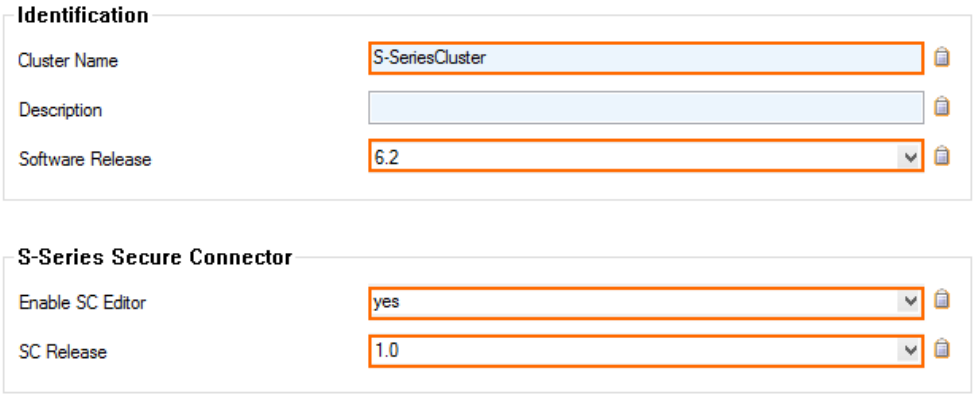
5. Enter the **Unique Net Identifier**.
6. Enter the **Net** address.
7. Select the **Poolsize**. Recommended pool size: /28
8. Select the **Access Concentrator** this FSC VIP network will be assigned to.
9. Set **Globally available** to **yes** for this network to be visible to all CC admins.



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

Step 7. Enable FSC-Series support for the cluster

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



5. 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 FSC devices either directly via configuration file or by connecting to the FSAC using the VPN deployment mode.
  - FSC Deployment via FSC Configuration File
  - FSC 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_06.png
8. sca_rule_01.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. sca_rule_05.png
15. add_net.png
16. create_net.png
17. enable_sc.png