How to Configure Application Rules Matching SCADA Protocols

https://campus.barracuda.com/doc/73719261/

System Control and Data Acquisition (SCADA) is a wide family of protocols used in industrial processes. The Barracuda CloudGen Firewall handles the most common ones. To allow the SCADA protocol to access a destination, a protocol object is required. SCADA protocols are handled via protocol objects in application rules. The following SCADA protocols are supported:

- S7
- IEC 60870-5-104
- IEC 6485
- MODBUS
- DNP3

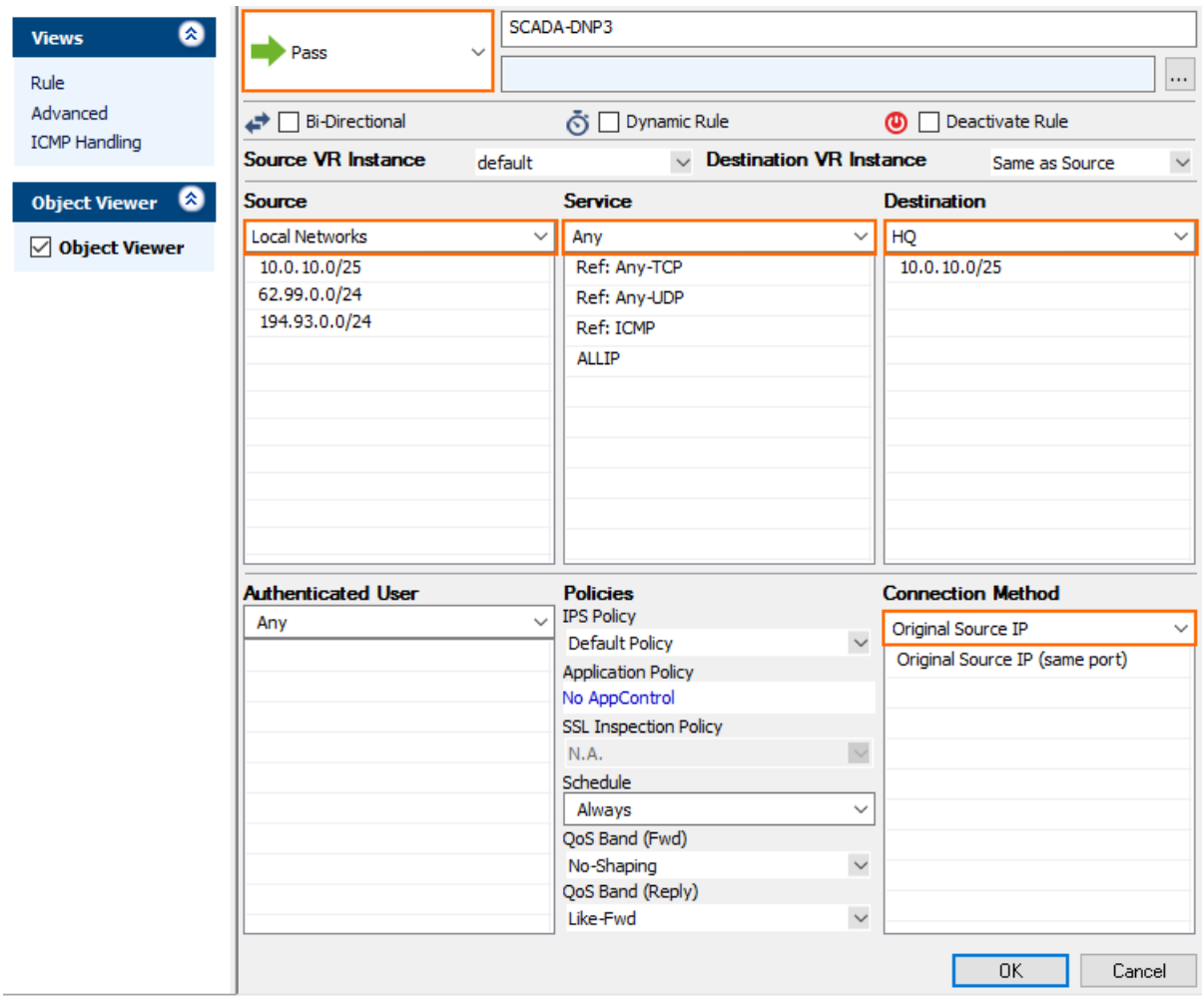
Before You Begin

Verify that you have enabled Application Control and that you are using the latest feature level of the Firewall service. For more information, see How to Enable Application Control.

Step 1. Create an Access Rule

Create an access rule to allow traffic from the source to the destination network.

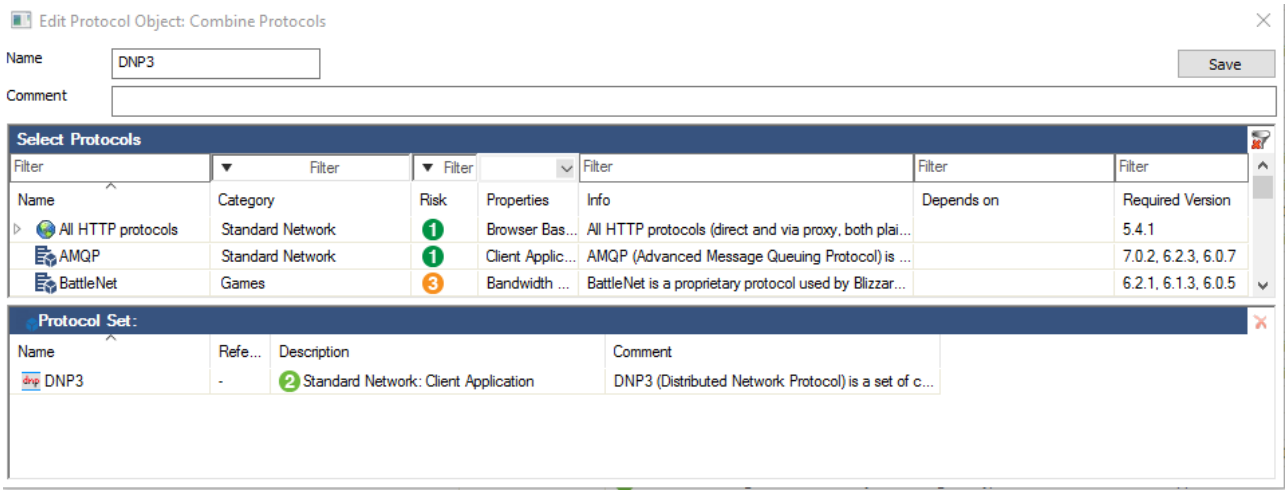
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
4. Select **Pass** as the action.
5. Enter a name for the rule. For example, `SCADA-DNP3.`
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Source** – The source addresses of the traffic.
   - **Destination** – The destination addresses of the traffic.
   - **Service** – Select a service object, or select **Any** for this rule to match for all services. For more information, see How to Create Service Objects.
   - **Connection Method** – Select **Original Source IP**.



7. Click **OK**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
9. Click **Send Changes** and **Activate**.

Step 2. Create a Protocol Object

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, expand **Firewall Objects** and select **Applications**.
4. Create the protocol object by either right-clicking the table and selecting **New > Protocol Object** or by using the icons in the top-right area of the ruleset.
5. Enter a descriptive **Name**, depending on the protocol. For example, DNP3**.**
6. Either search or filter for the protocol to include in the object.
7. Add the protocol by either dragging it to the **Protocol Set** section or clicking the plus sign (**+**) next to the name.

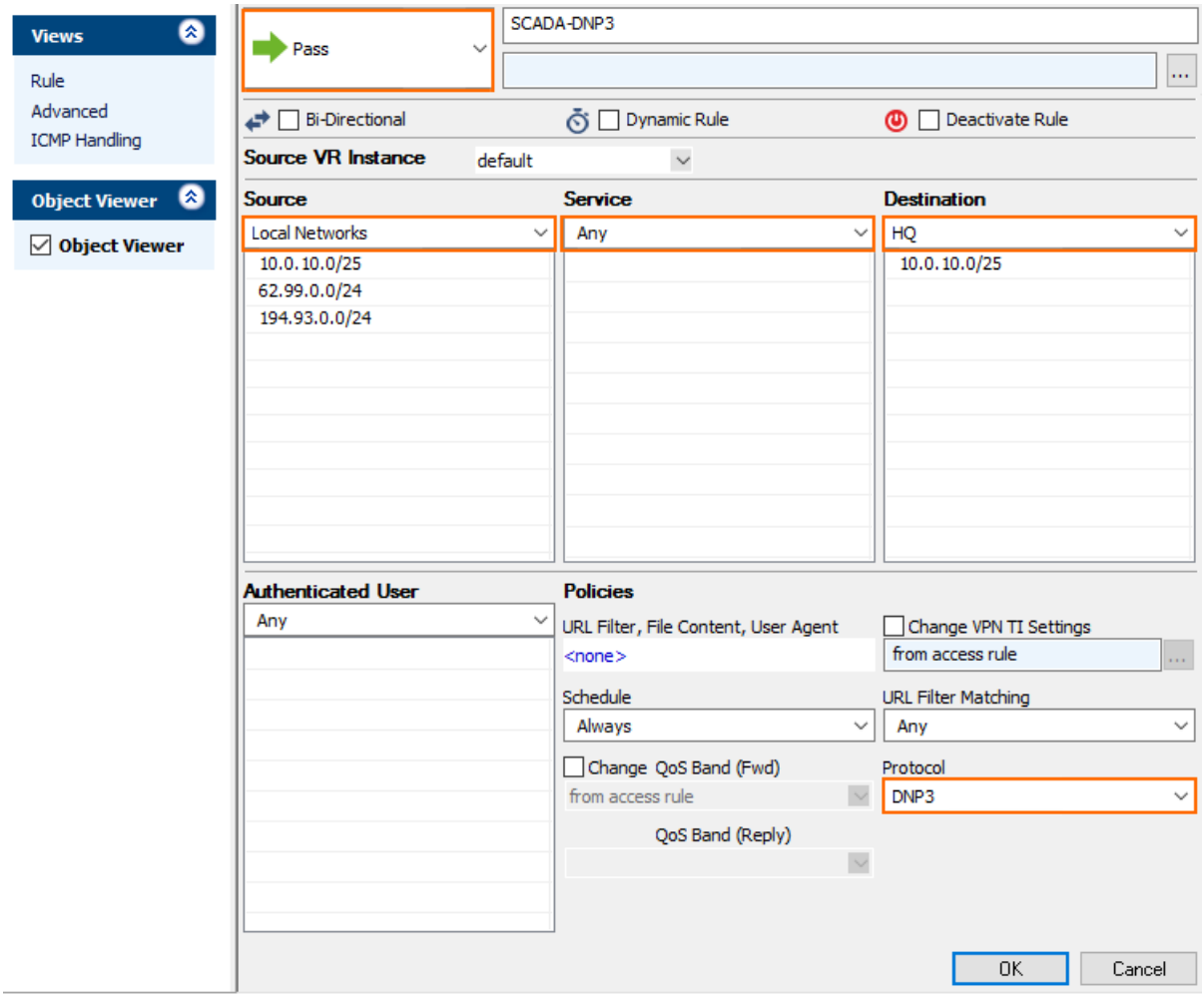


8. Click **Save**.
9. Click **Send Changes** and **Activate**.

Step 3. Create an Application Rule

Create an application rule that contains the application object created in Step 2.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules**.
3. Click **Lock**.
4. Click the green plus sign (**+**) in the top right of the page, or right-click the ruleset and select **New > Rule**. An application rule **New Rule** is added to the application ruleset.
5. Double-click the **New Rule** application rule you just created. The **Edit Rule** window opens.
6. Select **Pass** as the action.
7. Enter a name for the rule. For example, `DNP3 Access`.
8. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Source** – The source addresses of the traffic. The source must be the same or a subset of the source of the matching access rule.
   - **Destination** – The destination addresses of the traffic.The destination must be the same or a subset of the destination of the matching access rule.
   - **Application** – Select the application object or application filter. For more information, see How to Create an Application Object and How to Create an Application Filter.
9. From the **Protocol** drop-down list, select the protocol object that you created in Step 2.



10. Click **OK**.
11. Drag and drop the application rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located above the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
12. Click **Send Changes** and **Activate**.

Step 4. (optional) Enable Detailed SCADA Protocol Detection

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**
2. In the left menu, click **Application Detection**.
3. Click **Lock**.
4. Go to the **Supervisory Control and Data Acquisition Section (SCADA)**.
5. From the drop-down list select:
    1. **Enable without Parsing Log** – Detected SCADA protocols are included in the Firewall Activity log.
    2. **Enable with Parsing Log** – Enabled with detailed logs (box/SCADA/parsing).
6. Click **Send Changes** and **Activate**.

Figures

1. scada_rule.png
2. scada_proto.png
3. scada_access.png