

How to Configure Application Rules Matching SCADA Protocols

<https://campus.barracuda.com/doc/79462970/>

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

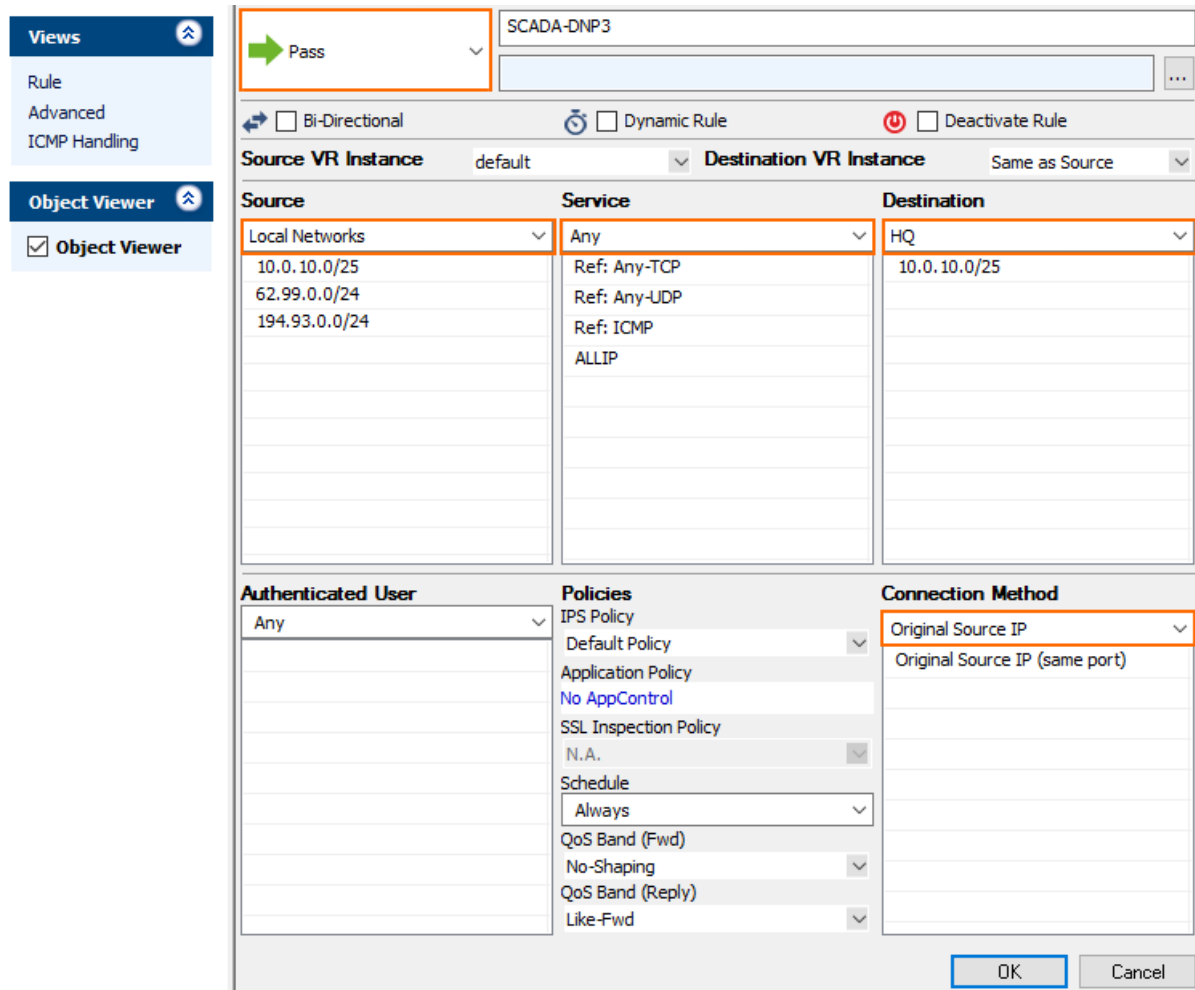
Before You Begin

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**.



Views

- Rule
- Advanced
- ICMP Handling

Object Viewer

- Object Viewer

Pass SCADA-DNP3

Bi-Directional Dynamic Rule Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
Local Networks	Any	HQ
10.0.10.0/25	Ref: Any-TCP	10.0.10.0/25
62.99.0.0/24	Ref: Any-UDP	
194.93.0.0/24	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
Any	IPS Policy	Original Source IP
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	No-Shaping	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

- Click **OK**.
- 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.
- Click **Send Changes** and **Activate**.

Step 2. Create a Protocol Object

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
- Click **Lock**.
- In the left menu, expand **Firewall Objects** and select **Applications**.
- 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.
- Enter a descriptive **Name**, depending on the protocol. For example, DNP3.
- Either search or filter for the protocol to include in the object.
- Add the protocol by either dragging it to the **Protocol Set** section or clicking the plus sign (+) next to the name.

Edit Protocol Object: Combine Protocols

Name: Save

Comment:

Select Protocols						
Filter	Filter	Filter	Filter	Filter	Filter	Filter
Name	Category	Risk	Properties	Info	Depends on	Required Version
> All HTTP protocols	Standard Network	1	Browser Bas...	All HTTP protocols (direct and via proxy, both plai...		5.4.1
AMQP	Standard Network	1	Client Applic...	AMQP (Advanced Message Queuing Protocol) is ...		7.0.2, 6.2.3, 6.0.7
BattleNet	Games	3	Bandwidth ...	BattleNet is a proprietary protocol used by Blizzar...		6.2.1, 6.1.3, 6.0.5

Protocol Set:			
Name	Ref...	Description	Comment
DNP3	-	2 Standard Network: Client Application	DNP3 (Distributed Network Protocol) is a set of c...

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:
 - o **Source** - The source addresses of the traffic. The source must be the same or a subset of the source of the matching access rule.
 - o **Destination** - The destination addresses of the traffic. The destination must be the same or a subset of the destination of the matching access rule.
 - o **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.

Figures

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