
How to Configure Application Rules Matching SCADA Protocols

<https://campus.barracuda.com/doc/72515754/>

System Control and Data Acquisition (SCADA) is a wide family of protocols used in industrial processes. The 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 **FIREWALL > Access Rules**.
2. Click **Add Access Rule**.
3. The **Add Access Rule** window opens.
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.
 - **Connection Method** - Select **Original Source IP** .

Add Access Rule ?

General
Advanced

Action: Pass

→

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda NextGen Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: SCADA-DNP3

Description:

Connection: Original Source IP

Adjust Bandwidth: Internet

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: Yes No

Disable: Yes No

IPS: Yes No

Application Control: Yes No

SSL Interception: Yes No

URL Filter: Yes No

Virus Scanner: Yes No

ATP: Yes No

Mail Security: Yes No

Safe Search: Yes No

Source

HA Management IP +

Ref. Local Networks -

Network Objects IP Addresses Geo Loc.

Network Services

Any-EMAIL +

Any -

Destination

Port-p4 +

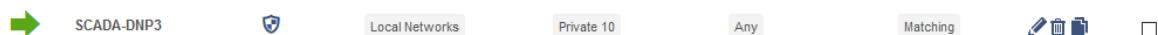
Ref. Private 10 -

Network Objects IP Addresses Geo Loc.

Cancel
Save


7. Click **Save**.

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.




Step 2. Create an Application Rule

1. Go to **FIREWALL > Application Rule**.
2. Click **Add Application Rule**.
3. Select **Pass** as the action.
4. Enter a name for the rule. For example, SCADA-DNP3 .

Add Application Rule 

General **Advanced**

Action: 

Disable: Yes No

Name:

Description:

Adjust Bandwidth:

URL Filter:

Native Apps

Select applications...

< previous next >

Any application will match

< previous next >

5. Click **Advanced**.
6. Specify the following settings:
 - **Source Networks** – The source addresses of the traffic, e.g., Local Networks.
 - **Protocols** – One of the above-mentioned SCADA-protocols, e.g., DNP3.

Add Application Rule ?

General
Advanced

Schedule

Any

Users

All Authenticated Users

Source Networks

HA Management IP
+

Ref. Local Networks

-
+

Network Objects IP Addresses

Protocols

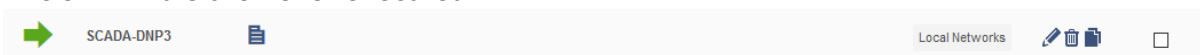
TINA VPN
+

DNP3

-
+

Cancel
Save

7. Click **Save**.
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.



Figures

1. scada_rule.png
2. scada_access_rule_added.png
3. scada_access_pg1.png
4. scada_access_pg2.png
5. scada_app_rule_added.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.