FORTINET FORTIGATE AND NOZOMI SCADAGUARDIAN
# DEPLOYMENT GUIDE: FORTINET FORTIGATE AND NOZOMI SCADAGUARDIAN

# FORTINET FORTIGATE AND NOZOMI SCADAGUARDIAN

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Deployment Prerequisites</td>
<td>3</td>
</tr>
<tr>
<td>Version Compatibility</td>
<td>3</td>
</tr>
<tr>
<td>Licensing</td>
<td>3</td>
</tr>
<tr>
<td>Deployment</td>
<td>3</td>
</tr>
<tr>
<td>Architecture Overview</td>
<td>3</td>
</tr>
<tr>
<td>FortiGate Configuration</td>
<td>4</td>
</tr>
<tr>
<td>Interfaces</td>
<td>6</td>
</tr>
<tr>
<td>Protocol Service</td>
<td>7</td>
</tr>
<tr>
<td>Policy</td>
<td>7</td>
</tr>
<tr>
<td>Create Appropriate User for Nozomi SCADAGuardian</td>
<td>9</td>
</tr>
<tr>
<td>Nozomi Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Enable FortiGate + Nozomi Configuration:</td>
<td>10</td>
</tr>
<tr>
<td>Preparing the integration for Testing and Deployment</td>
<td>10</td>
</tr>
<tr>
<td>Placing SCADAGuardian in Learning mode</td>
<td>12</td>
</tr>
<tr>
<td>Placing the system in Protecting Mode</td>
<td>12</td>
</tr>
<tr>
<td>Testing the Integration and Deployment</td>
<td>12</td>
</tr>
<tr>
<td>References</td>
<td>12</td>
</tr>
</tbody>
</table>
OVERVIEW

Fortinet (NASDAQ: FTNT) is a global provider of high-performance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer tour Technology Alliances here: [https://www.fortinet.com/partners/partnerships/alliance-partners.html](https://www.fortinet.com/partners/partnerships/alliance-partners.html)

Nozomi Networks is a leading provider of real-time visibility, advanced monitoring capabilities, and strong security for industrial control networks supporting critical infrastructure. Built by a team of industrial SecOps, Nozomi’s SCADAguardian appliances inspect industrial networks non-intrusively and apply machine-learning technology to provide unique insight into the topology, devices, and behaviors present in it.

Industrial Control Systems have strict and unique environments that require security to be the top priority. In this document, we will look at the Integration of the Fortinet’s FortiGate to Nozomi Networks’ SCADAguardian appliance, to bring the power of the Security Fabric to the Industrial Control Systems.

DEPLOYMENT PREREQUISITES

1. FortiGate
2. FortiSwitch
3. Nozomi ScadaGuardian
4. An ICS environment with IT and OT Networks

VERSION COMPATIBILITY

This Deployment and Integration guide applies to FortiGates with FortiOS v5.6, v6.0 and above, and with Nozomi SCADAGuardian v18.0 and above. This guide will assume the integration with FortiOS 5.6.

LICENSING

For licenses to Nozomi ScadaGuardian, please contact Nozomi’s respective sales team.

DEPLOYMENT

ARCHITECTURE OVERVIEW

This is an example of what a SCADA Network may look like. The diagram denotes potential topological locations for where the FortiGate, FortiSwitch, FortiSIEM and the SCADAGuardian are may reside, in between the IT and the OT Networks (and/or the Process and Control Networks).
The FortiGate sits in-line between the IT and the OT Networks, and within the local environments of each OT Networks themselves – actively controlling traffic between the IT Network and the OT Network. The Nozomi SCADAGuardian is connected in SPAN/Port Mirroring mode behind the respective switches, having visibility of network traffic of both the networks.

For the purpose of this Integration guide, we will focus on a single segment.

Specifically, The communication between the FortiGate and the SCADAGuardian occurs over the Security Fabric via the Management Network.

**FORTIGATE CONFIGURATION**

On the FortiGate, there are 3 basic requirements that are required for FortiGate to be in-line between the IT Network and the OT Network, and to be integrated with the SCADAGuardian. There are three Interfaces to be configured, one Service and one Policy.

**INTERFACES**
a) IT Network

A port on the FortiGate is required to be configured for the IT Network on a dedicated subnet. Ensure that no Administrator Access options are enabled for this port. ICS Environments require tightly secured networks, as such it is recommended for least possible administrative access to the interface.

Also ensure that "Active Scanning" option is disabled, as this creates unnecessary noise on the network that may impede the integration with SCADAGuardian.

This port will act as the Gateway of the IT Network.

b) OT Network

Similarly, a port on the FortiGate is required to be configured for the OT Network on a dedicated subnet. Ensure that no Administrator Access options are enabled for this port. ICS Environments require tightly secured networks, as such it is recommended for least possible administrative access to the interface.
Also ensure that “Active Scanning” option is disabled, as this creates unnecessary noise on the network that may impede the integration with SCADAGuardian.

This port will act as the Gateway of the OT Network.

c) Management Network

A management network needs to be created via which the FortiGate will communicate with the SCADAGuardian and can be managed from.
PROCOTOL SERVICE

Create Services for your environment’s required protocols.

Typically, these are SCADA oriented protocols such as MODBUS, DNP3, Profibus, FIP, etc. In this example we are creating a service for the MODBUS protocol.

![Protocol Service Configuration]

Name this service ‘Modbus’ and Select Protocol type as TCP/UDP/SCTP and Destination port as ‘TCP’ and port 502. Click OK.

POLICY

Creation of one Policy is required for traffic coming in from IT Network to OT Network allowing only the Protocol Services created from the previous step. Ensure that NAT is disabled, and for the purpose of analysis of incidents, enable all logging.
Please follow the screenshot for the settings for the policy.
CREATE APPROPRIATE USER FOR NOZOMI SCADAGUARDIAN

Create a New user for the Nozomi SCADAGuardian to access the FortiGate for the integration.

Go to System -> Administrators and Click on “Create New”. Enter the details for the user account and enter the details as shown in the screenshot below.

1. Enter the Username, Password and the comments.
2. Select the Type of the user to be “Local User”.
3. Set Administrator Profile to “super_admin”.
4. Enable Restrict login to trusted hosts, and put in the IP of the Nozomi SCADAGuardian.
5. Click OK.

NOZOMI CONFIGURATION

The configuration on the SCADAGuardian requires connectivity to the Management interface and all the security integration options enabled.

Ensure that the management interface of Nozomi SCADAGuardian can reach using protocol ssh on port 22 the management interface of the Fortigate.

Ensure that the SCADAGuardian is connected to a switch for IT Network and the OT Network in SPAN/Mirrored ports. This gives SCADAGuardian visibility of the SCADA traffic between the networks.
ENABLE FORTIGATE + NOZOMI CONFIGURATION:

1. Under Settings->Firewall Integration choose “Fortinet FortiGate”

2. Insert the IP address of the management interface of the Fortigate and the user with the password created on the Fortigate for the integration

3. Make sure that the status is updated to “Connected to Fortinet FortiGate <ip address>” in green. This ensures that the connectivity between the FortiGate and the SCADAGuardian is enabled.

PREPARING THE INTEGRATION FOR TESTING AND DEPLOYMENT

Nozomi SCADAGuardian works on the basis of behavioral analysis and machine learning. When a SCADAGuardian is placed in a new environment, the appliance has to be put in the “Learning” state, prior to live production deployment, for a designated amount of time prior to enabling Protection mode.

Placing SCADAGuardian in Learning mode

To ensure that the SCADAGuardian is in Learning Mode, all prior data must be first reset to a clean state:

1. Log in to the SCADAGuardian
2. Go to System -> Data
3. Clear all settings by clicking on “Select All”
4. Click on“Reset” and enter your password.
This will ensure that the appliance is start from a clean state with no prior learning.

To ensure that the system is in Learning Mode:

1. Click on “Settings” and go to “Learning”
2. Ensure that both the Network and Processes section have “Learning” selected. Here, you will be able to see the amount of time since which the system has been in Learning mode.
PLACING THE SYSTEM IN PROTECTING MODE

Once the SCADAGuardian has been in Learning mode for an appropriate amount of time, it can now be put into “Protecting” mode to begin actively monitoring the ICS environment.

To put the system into Protect mode:

1. Click on “Settings” and go to “Learning”
2. Under the “Network” section, click on “Protecting”.

TESTING THE INTEGRATION AND DEPLOYMENT

Before testing the integration, you should ensure that SCADAgurdian’s baseline and the learning phase is completed.

To test the Integration, please refer to the Nozomi Integration Video to replicate the scenarios.

REFERENCES

- FortiGate/FortiOS Admin Guides
  - [http://docs.fortinet.com/fortigate/admin-guides](http://docs.fortinet.com/fortigate/admin-guides)
- Nozomi Networks SCADAGuardian Resources
  - [http://www.nozominetworks.com/resources.html](http://www.nozominetworks.com/resources.html)
- Fortinet User Community
  - [https://fuse.fortinet.com](https://fuse.fortinet.com)
- Nozomi Networks