DEPLOYMENT GUIDE

Fortinet FortiGate and Nozomi Networks Guardian

Fortinet FortiGate and Nozomi Networks Guardian

Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Nozomi

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 control systems (ICS) and network security expertise, Nozomi Networks' Guardian appliances and software inspect industrial networks non-intrusively and apply machine-learning (ML) with Artificial Intelligence (AI) technology to provide unique insight into the topology, devices, and behaviors present in it.

Deployment Prerequisites

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

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 Fortinet's FortiGate to Nozomi Networks' Guardian appliance, to bring the power of the Security Fabric to the industrial control systems.

Version Compatibility

This Deployment and Integration Guide applies to FortiGates with FortiOS v5.4 and 5.6, and with Nozomi Networks' Guardian v17.0.0. This guide will assume the integration with FortiOS 5.6.

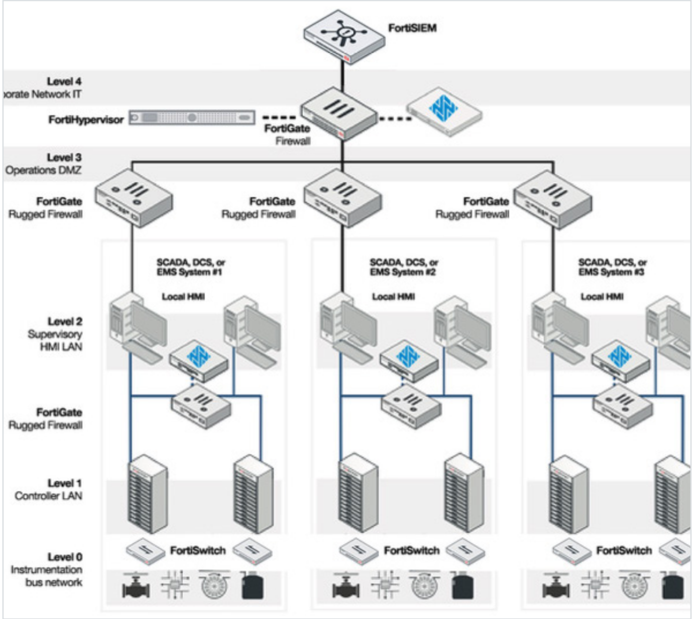
Licensing

For licenses to the Nozomi Networks' Guardian, please contact Nozomi Networks respective sales team.
http://www. nozominetworks.com/company/contact-us.html

Deployment

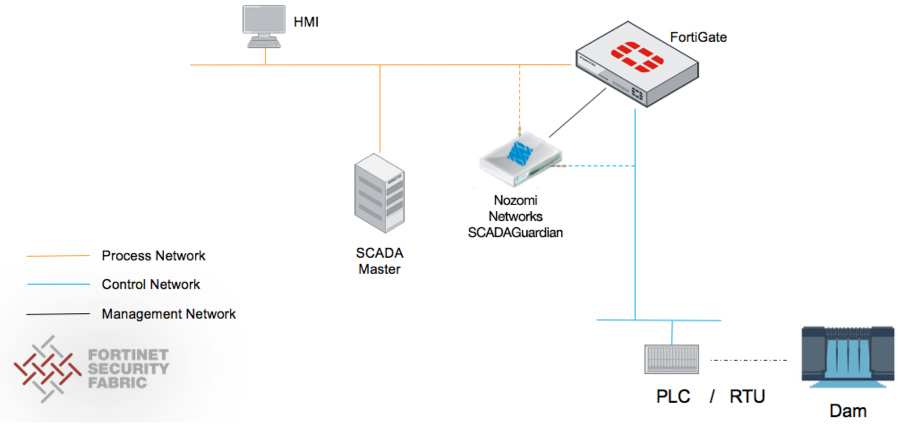
Architecture Overview

This is an example of what a supervisory control and data acquisition (SCADA) network may look like, where the FortiGate and the Guardian are located as a point of convergence between the IT and the OT networks (and/or the process and OT networks).



The FortiGate sits in-line between the IT and the OT networks, and within the local environments of each OT network themselves—actively controlling traffic between the IT network and the OT network. The Nozomi Networks' Guardian is connected in SPAN/port mirroring mode behind the respective switches, having visibility of network traffic of both networks.

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

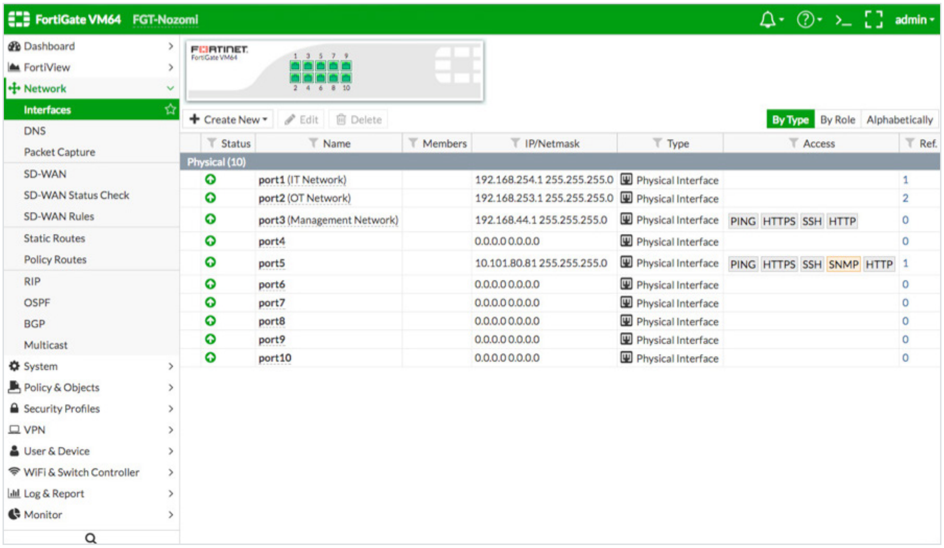


The communication between the FortiGate and the Guardian occurs over the Security Fabric via the management network.

FortiGate Configuration

On the FortiGate, there are three basic requirements for the FortiGate to be in-line between the IT network and the OT network, and to be integrated with the Guardian. There are three interfaces to be configured, one service, and one policy.

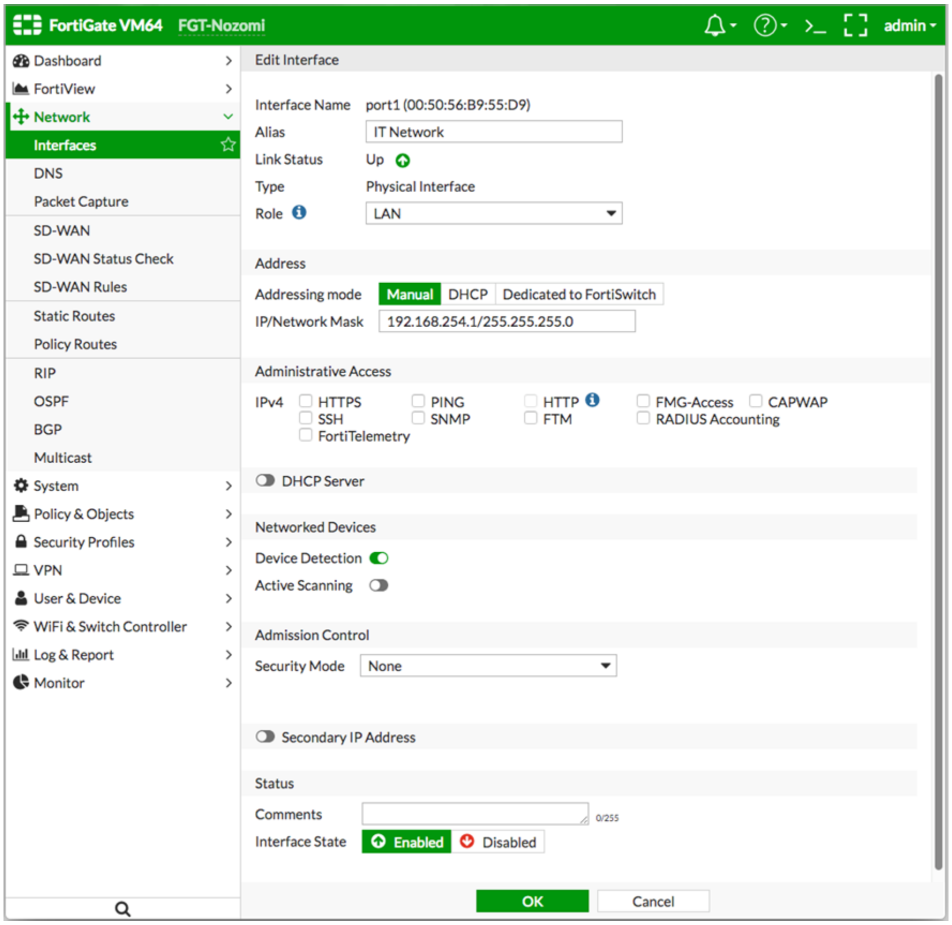
Interfaces



Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)						
●	port1 (IT Network)		192.168.254.1 255.255.255.0	Physical Interface		1
●	port2 (OT Network)		192.168.253.1 255.255.255.0	Physical Interface		2
●	port3 (Management Network)		192.168.44.1 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	0
●	port4		0.0.0.0 0.0.0.0	Physical Interface		0
●	port5		10.101.80.81 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP	1
●	port6		0.0.0.0 0.0.0.0	Physical Interface		0
●	port7		0.0.0.0 0.0.0.0	Physical Interface		0
●	port8		0.0.0.0 0.0.0.0	Physical Interface		0
●	port9		0.0.0.0 0.0.0.0	Physical Interface		0
●	port10		0.0.0.0 0.0.0.0	Physical Interface		0

1. IT Network

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



Edit Interface

Interface Name port1 (00:50:56:B9:55:D9)
Alias IT Network
Link Status Up
Type Physical Interface
Role LAN

Address

Addressing mode [✓ Manual] DHCP Dedicated to FortiSwitch
IP/Network Mask 192.168.254.1/255.255.255.0

Administrative Access

IPv4 □ HTTPS □ PING □ HTTP □ FMG-Access □ CAPWAP
□ SSH □ SNMP □ FTM □ RADIUS Accounting
□ FortiTelemetry

DHCP Server

Networked Devices

Device Detection ●
Active Scanning ○

Admission Control

Security Mode None

Secondary IP Address

Status

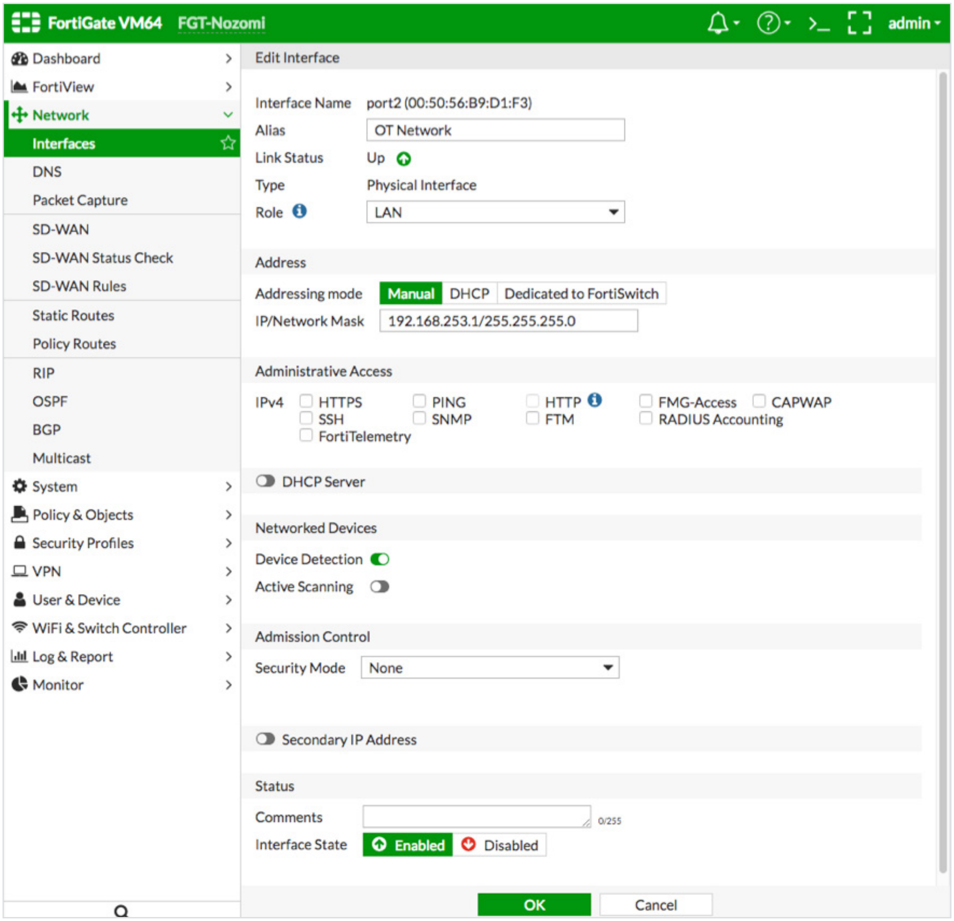
Comments 0/255
Interface State [✓ Enabled] Disabled

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

This port will act as the gateway of the IT network.

2. OT Network

Similarly, a port on the FortiGate is required to be configured for the OT network on a dedicated subnet. Ensure that no Administrative Access options are enabled for this port. ICS environments require tightly secured networks. As such, the least possible administrative access to the interface is recommended.



Edit Interface

Interface Name port2 (00:50:56:B9:D1:F3)
Alias OT Network
Link Status Up
Type Physical Interface
Role LAN

Address

Addressing mode [✓ Manual] DHCP Dedicated to FortiSwitch
IP/Network Mask 192.168.253.1/255.255.255.0

Administrative Access

IPv4 □ HTTPS □ PING □ HTTP □ FMG-Access □ CAPWAP
□ SSH □ SNMP □ FTM □ RADIUS Accounting
□ FortiTelemetry

DHCP Server (off)

Networked Devices

Device Detection (on)
Active Scanning (off)

Admission Control

Security Mode None

Secondary IP Address (off)

Status

Comments 0/255
Interface State [✓ Enabled] Disabled

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

This port will act as the gateway of the OT network.

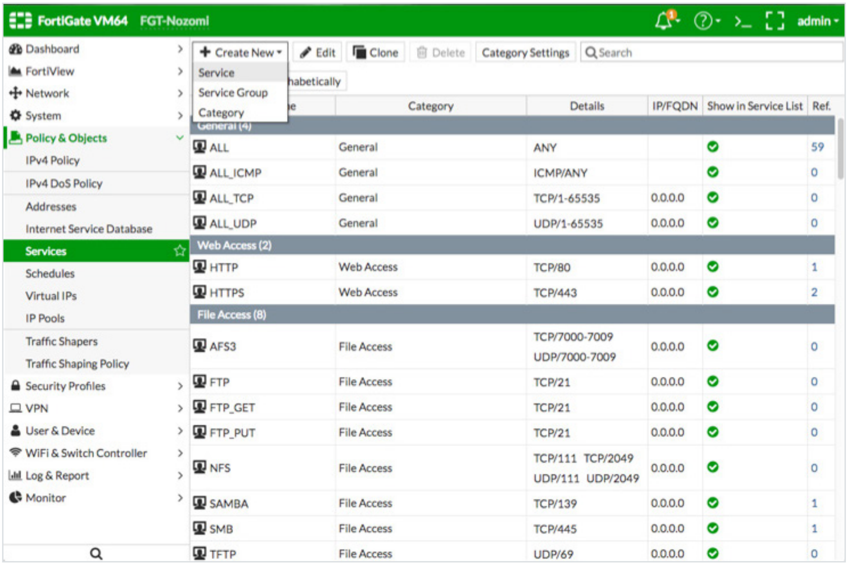
3. Management Network

A management network needs to be created on which the FortiGate will communicate with the Guardian and from which it can be managed.

Protocol Service

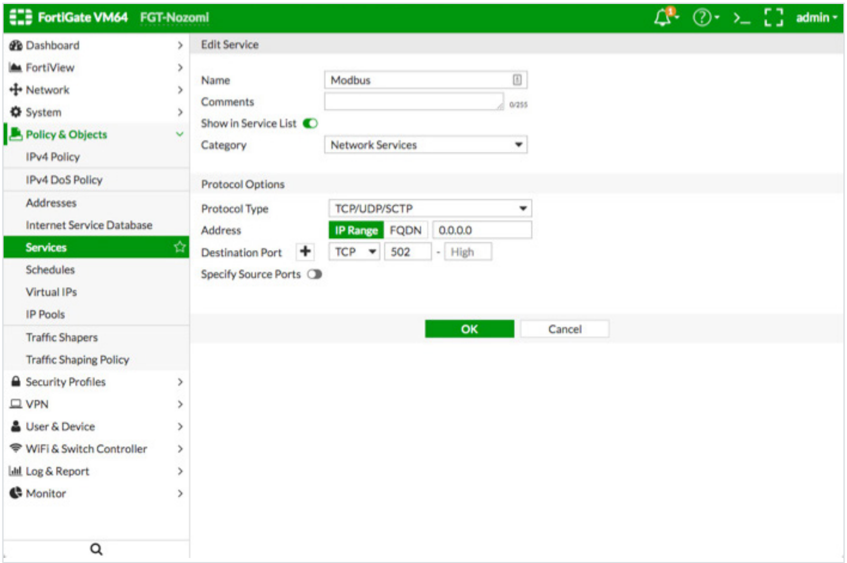
Create services for your environment's required protocols.

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.



e	Category	Details	IP/FQDN	Show in Service List	Ref.
General (4)					
ALL	General	ANY		✓	59
ALL_ICMP	General	ICMP/ANY		✓	0
ALL_TCP	General	TCP/1-65535	0.0.0.0	✓	0
ALL_UDP	General	UDP/1-65535	0.0.0.0	✓	0
Web Access (2)					
HTTP	Web Access	TCP/80	0.0.0.0	✓	1
HTTPS	Web Access	TCP/443	0.0.0.0	✓	2
File Access (8)					
AFS3	File Access	TCP/7000-7009 UDP/7000-7009	0.0.0.0	✓	0
FTP	File Access	TCP/21	0.0.0.0	✓	0
FTP_GET	File Access	TCP/21	0.0.0.0	✓	0
FTP_PUT	File Access	TCP/21	0.0.0.0	✓	0
NFS	File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	✓	0
SAMBA	File Access	TCP/139	0.0.0.0	✓	1
SMB	File Access	TCP/445	0.0.0.0	✓	1
TFTP	File Access	UDP/69	0.0.0.0	✓	0

Name this service "Modbus" and select Protocol Type as TCP/UDP/SCTP and Destination Port as "TCP" and port 502. Click OK.



Edit Service

Name: Modbus

Comments: 0/255

Show in Service List ●

Category: Network Services

Protocol Options

Protocol Type: TCP/UDP/SCTP

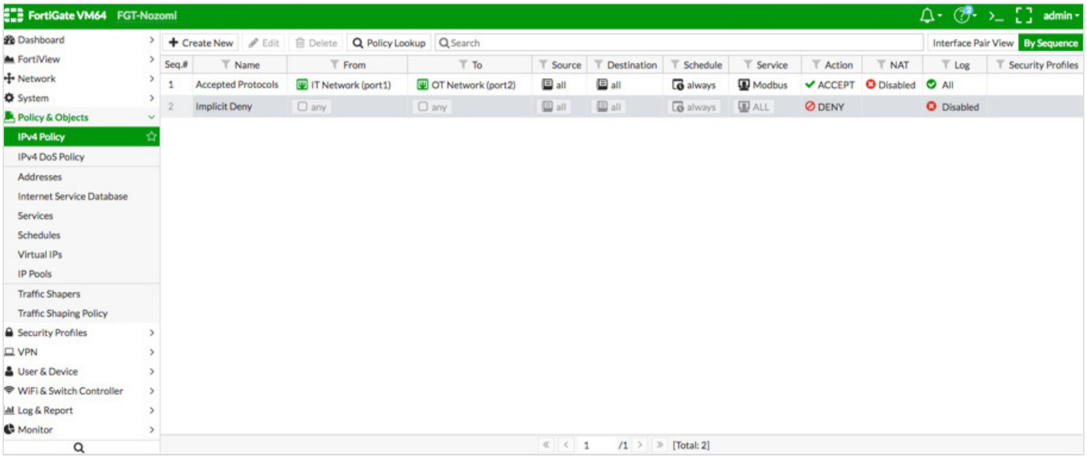
Address: IP Range FQDN 0.0.0.0

Destination Port: TCP 502 - High

Specify Source Ports ○

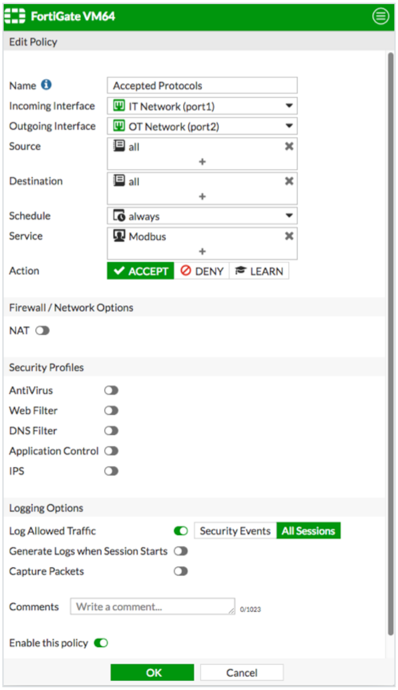
Policy

Creation of one policy is required for traffic coming in from the IT network to the 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.



Seq.#	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Log	Security Profiles
1	Accepted Protocols	IT Network (port1)	OT Network (port2)	all	all	always	Modbus	✓ ACCEPT	Disabled	All	
2	Implicit Deny	any	any	all	all	always	ALL	DENY		Disabled	

Please follow the screenshot for the settings for the policy.



Name	Accepted Protocols
Incoming Interface	IT Network (port1)
Outgoing Interface	OT Network (port2)
Source	all
Destination	all
Schedule	always
Service	Modbus
Action	✓ ACCEPT / DENY / LEARN

Firewall / Network Options

NAT	○

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○

Logging Options

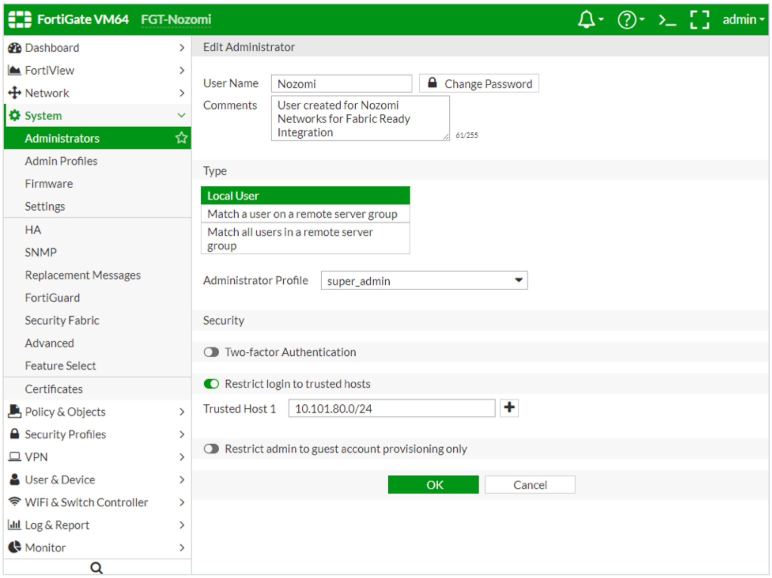
Log Allowed Traffic	● Security Events / All Sessions
Generate Logs when Session Starts	○
Capture Packets	○
Comments	Write a comment... 0/1023
Enable this policy	●

Create User for Nozomi Networks' Guardian

Create a new user for the Nozomi Networks' Guardian 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 User Name, Password, and 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 Networks' Guardian.
5. Click **OK.**



Edit Administrator

User Name: Nozomi
Change Password
Comments: User created for Nozomi Networks for Fabric Ready Integration
61/255

Type
- [✓ Local User]
- Match a user on a remote server group
- Match all users in a remote server group

Administrator Profile: super_admin

Security
- ○ Two-factor Authentication
- ● Restrict login to trusted hosts
- Trusted Host 1: 10.101.80.0/24
- ○ Restrict admin to guest account provisioning only

OK Cancel

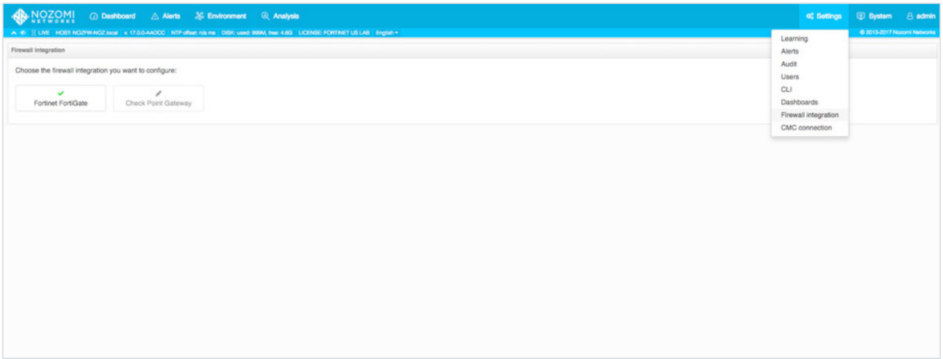
Nozomi Networks Configuration

The configuration on the Guardian requires connectivity to the management interface and all the security integration options enabled. Ensure that the management interface of the Nozomi Networks' Guardian can reach using protocol ssh on port 22 the management

Ensure that the Guardian is connected to a switch for the IT network and the OT network in SPAN/mirrored ports. This gives the Guardian visibility of the SCADA traffic between the networks.

Enable FortiGate + Nozomi Networks Configuration

1. Under Settings > Firewall Integration, choose "Fortinet FortiGate."

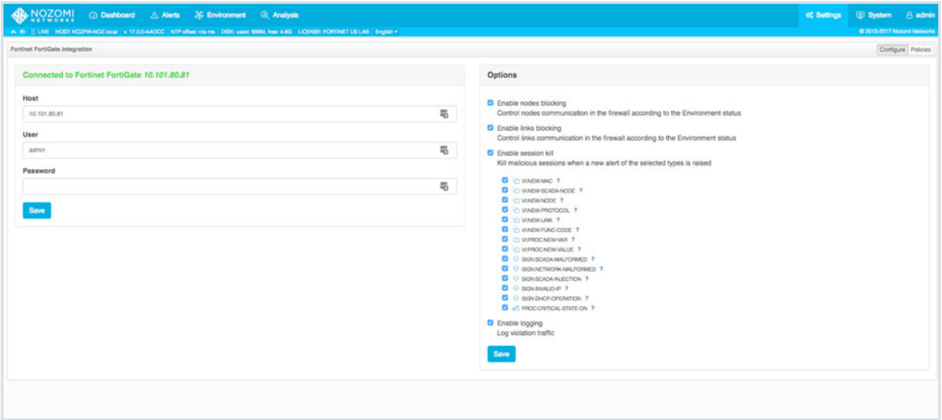

NOZOMI NETWORKS
Dashboard
Alerts
Environment
Analysis
Settings
System
admin
LIVE HOST: NOZFW-NOZ.local v. 17.0.0-AADCC NTP offset: n/a ms DISK: used: 999M, free: 4.6G LICENSE: FORTINET US LAB English
© 2013-2017 Nozomi Networks
Learning
Alerts
Audit
Users
CLI
Dashboards
Firewall integration
CMC connection

Firewall integration

Choose the firewall integration you want to configure:

✓ Fortinet FortiGate | Check Point Gateway

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


NOZOMI NETWORKS
Dashboard
Alerts
Environment
Analysis
Settings
System
admin
LIVE HOST: NOZFW-NOZ.local v. 17.0.0-AADCC NTP offset: n/a ms DISK: used: 999M, free: 4.6G LICENSE: FORTINET US LAB English
© 2013-2017 Nozomi Networks
Configure
Policies

Fortinet FortiGate Integration

Connected to Fortinet FortiGate *10.101.80.81*

Host: 10.101.80.81
User: admin
Password:
Save

Options

- ☑ Enable nodes blocking
  Control nodes communication in the firewall according to the Environment status
- ☑ Enable links blocking
  Control links communication in the firewall according to the Environment status
- ☑ Enable session kill
  Kill malicious sessions when a new alert of the selected types is raised
  - ☑ VI:NEW-MAC ?
  - ☑ VI:NEW-SCADA-NODE ?
  - ☑ VI:NEW-NODE ?
  - ☑ VI:NEW-PROTOCOL ?
  - ☑ VI:NEW-LINK ?
  - ☑ VI:NEW-FUNC-CODE ?
  - ☑ VI:PROC:NEW-VAR ?
  - ☑ VI:PROC:NEW-VALUE ?
  - ☑ SIGN:SCADA-MALFORMED ?
  - ☑ SIGN:NETWORK-MALFORMED ?
  - ☑ SIGN:SCADA-INJECTION ?
  - ☑ SIGN:INVALID-IP ?
  - ☑ SIGN:DHCP-OPERATION ?
  - ☑ PROC:CRITICAL-STATE-ON ?
- ☑ Enable logging
  Log violation traffic

Save

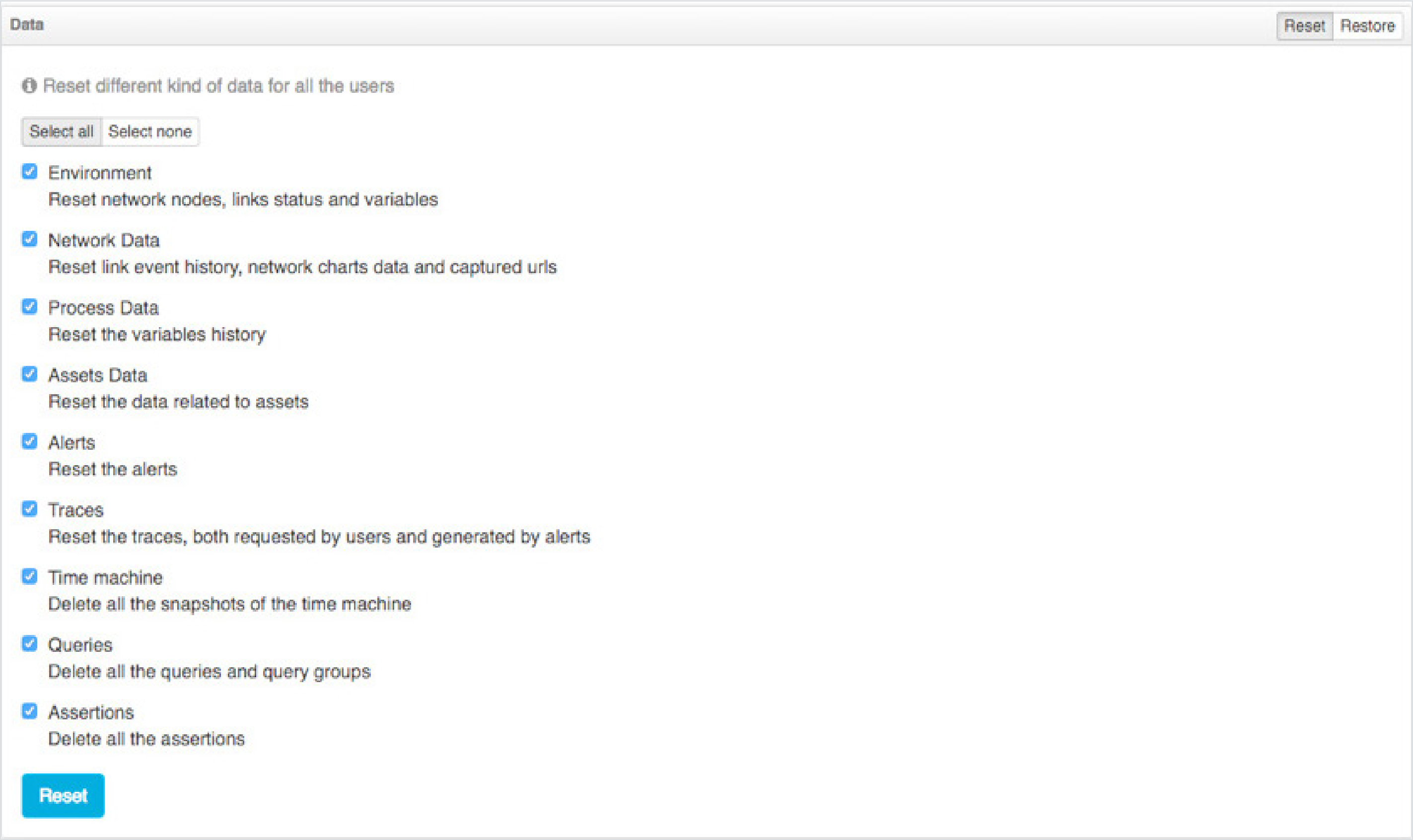
Preparing the Integration for Testing and Deployment

The Nozomi Networks' Guardian works on the basis of behavioral analysis and machine learning. When a Guardian 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 Protecting mode.

Placing Guardian in Learning Mode

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

1. Log in to the Guardian.
2. Go to System -> Data.
3. Clear all settings by clicking on "Select all."
4. Click on "Reset" and enter your password.



Reset different kind of data for all the users

☑ Environment
Reset network nodes, links status and variables

☑ Network Data
Reset link event history, network charts data and captured urls

☑ Process Data
Reset the variables history

☑ Assets Data
Reset the data related to assets

☑ Alerts
Reset the alerts

☑ Traces
Reset the traces, both requested by users and generated by alerts

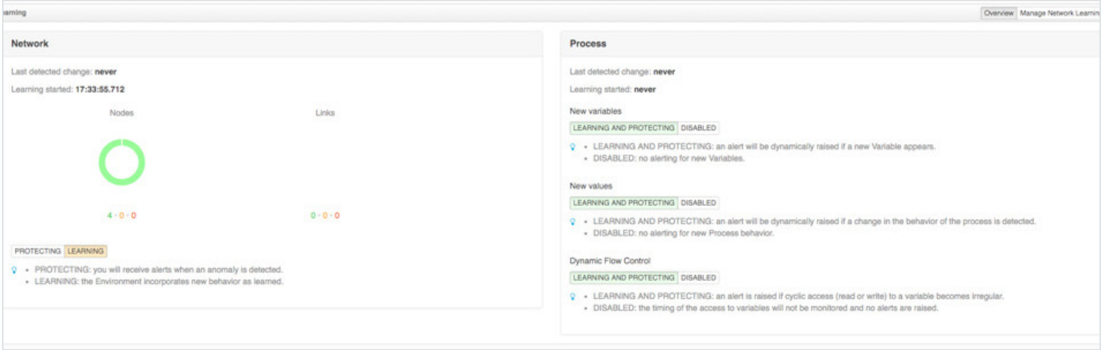
☑ Time machine
Delete all the snapshots of the time machine

☑ Queries
Delete all the queries and query groups

☑ Assertions
Delete all the assertions

This will ensure that the appliance is started from a clean state with no prior learning.

To ensure that the system is in Learning mode:



Network

Last detected change: **never**

Learning started: **17:33:55.712**

- PROTECTING: you will receive alerts when an anomaly is detected.
- LEARNING: the Environment incorporates new behavior as learned.

Process

Last detected change: **never**

Learning started: **never**

New variables

- LEARNING AND PROTECTING: an alert will be dynamically raised if a new Variable appears.
- DISABLED: no alerting for new Variables.

New values

- LEARNING AND PROTECTING: an alert will be dynamically raised if a change in the behavior of the process is detected.
- DISABLED: no alerting for new Process behavior.

Dynamic Flow Control

- LEARNING AND PROTECTING: an alert is raised if cyclic access (read or write) to a variable becomes irregular.
- DISABLED: the timing of the access to variables will not be monitored and no alerts are raised.

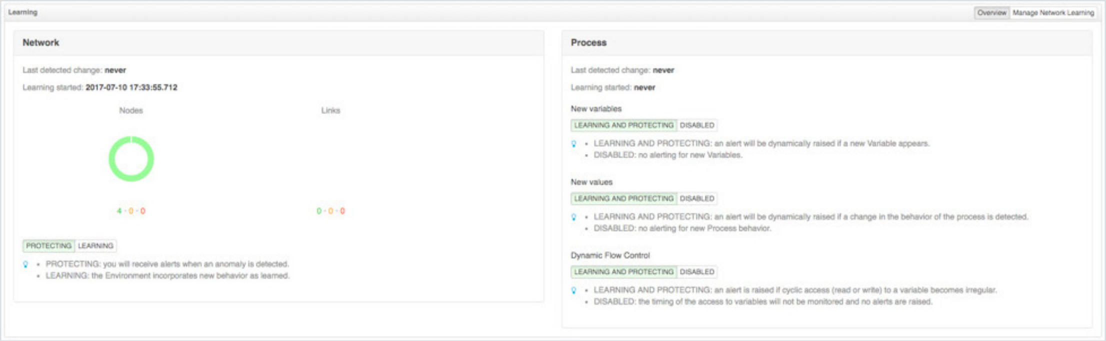
1. Log in to the Guardian.
2. Ensure that both the Network and Process sections have “Learning” selected. Here, you will be able to see the amount of time since the system has been in Learning mode.

Placing the System in Protecting Mode

Once the Guardian 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 Protecting mode:

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



Network

Last detected change: **never**

Learning started: **2017-07-10 17:33:55.712**

- PROTECTING: you will receive alerts when an anomaly is detected.
- LEARNING: the Environment incorporates new behavior as learned.

Process

Last detected change: **never**

Learning started: **never**

New variables

- LEARNING AND PROTECTING: an alert will be dynamically raised if a new Variable appears.
- DISABLED: no alerting for new Variables.

New values

- LEARNING AND PROTECTING: an alert will be dynamically raised if a change in the behavior of the process is detected.
- DISABLED: no alerting for new Process behavior.

Dynamic Flow Control

- LEARNING AND PROTECTING: an alert is raised if cyclic access (read or write) to a variable becomes irregular.
- DISABLED: the timing of the access to variables will not be monitored and no alerts are raised.

Testing the Integration and Deployment

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

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

References

1. FortiGate/FortiOS Admin Guides
   http://docs.fortinet.com/fortigate/admin-guides
2. Nozomi Networks Guardian Data Sheet
   http://www.nozominetworks.com/downloads/US/Nozomi-Networks-SG-Data-Sheet.pdf
3. Nozomi Networks Guardian Resources
   http://www.nozominetworks.com/resources.html
4. Fortinet User Community
   https://fuse.fortinet.com
5. Nozomi Networks
   http://www.nozominetworks.com/

November 20, 2019 1:42 PM
C:\Users\cyan\Documents\AEM\2019-11-20\DG-Fortinet and Nozomi Guardian\DG-Fortinet and Nozomi Guardian\dg-fortinet-nozomi-guardian