

DEPLOYMENT GUIDE

Fortinet FortiGate and Nozomi Networks Guardian



Table of Contents

Overview
Deployment Prerequisites 3
Version Compatibility 3
Licensing 3
Deployment 3
Architecture Overview
FortiGate Configuration 4
Interfaces 4
Protocol Service
Policy
Create User for Nozomi Network's Guardian
Nozomi Networks Configuration
Enable FortiGate + Nozomi Networks Configuration 9
Preparing the Integration for Testing and Deployment
Placing Guardian in Learning Mode10
Placing the System in Protecting Mode11
Testing the Integration and Deployment11
References

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

- FortiGate
- FortiSwitch
- Nozomi Networks' Guardian
- 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. <u>http://www.nozominetworks.com/company/contact-us.html</u>

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

፼ Dashboard ■ FortiView + Network	> FORTION forficing VMail						
Interfaces	🔅 🛨 Create	Neur & Edit ID Delete		-		DuTure Du Pole Ale	da batte alla
DNS Packet Capture	T Sta	tus T Name	T Members	T IP/Netmask	⊤ Туре	T Access	T Re
SD-WAN SD-WAN Status Check SD-WAN Rules	Physical (1	o) port1 (IT Network) port2 (OT Network) port3 (Management Network)		192.168.254.1 255.255.255.0 192.168.253.1 255.255.255.0 192.168.44.1 255.255.255.0	 Physical Interface Physical Interface Physical Interface 	PING HTTPS SSH HTTP	1 2 0
Static Routes Policy Routes	0	port4 port5		0.0000000 10.101.80.81 255.255.255.0	Physical Interface Physical Interface	PING HTTPS SSH SNMP HT	O TP 1
RIP OSPF BGP Multicast	0000	port6 port7 port8 port9		0.0.0.0.0.0.0 0.0.0.0.0.0.0 0.0.0.0.0.0	 Physical Interface Physical Interface Physical Interface Physical Interface 		0
 System Policy & Objects Security Profiles 	>	port10		0000000	Physical Interface		0
□ VPN User & Device WiFi & Switch Controller	>						
Monitor	>						

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.

FortiGate VM64 FGT-N	ozomi			۵.	0.)	- 53	admin -
Dashboard FortiView	Edit Interface Interface Name port1	100:50:56:89:5	5:D9)				
Network Identifices DNS Packet Capture SD-WAN SD-WAN Status Check SD-WAN Rules Static Routes	Alias IT Ne Link Status Up C Type Physic Role D LAN Address Addressing mode Mai IP/Network Mask 199	al Interface	Pedicated to Fort15	witch			
Policy Routes RIP OSPF BGP Multicast System Policy & Objects Security Profiles	Administrative Access IPv4 HTTP5 SSH FortiTelemetry Dir DHCP Server Networked Devices Device Detection	PING SNMP	HTTP 0	PMG-Access RADIUS Accost	CAPW.	A₽	
User & Device WiFi & Switch Controller Use & Report Monitor	Active Scanning Active Scanning Active Scanning Active Scanning Active Scanning Security Mode None Security Mode None Security IP Addrese	55					
0	Status Comments Interface State	nabled 🙂 Di	assisted	Cancel			

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.

FortiGate VM64 FGT-N	lozomi	Ω٠	· >_	13	admin
B Dashboard FortiView the Network	Edit Interface Interface Name port2 (00:50:56:B9:D1:F3)				
Interfaces DNS Packet Capture SD-WAN SD-WAN Status Check SD-WAN Rules Static Routes Policy Routes RIP OSPF	Alias OT Network Link Status Up Type Physical Interface Role LAN Address Address Addressing mode Manual DHCP Dedicated to FortiSwib IP/Network Mask 192.168.253.1/255.255.255.0 Administrative Access IPv4 HTTP5 PING HTTP	ch FMG-Access	CAPWAP		
BGP Multicast ♦ System ♦ Policy & Objects ♦ Security Profiles ↓ VPN ♦ User & Device ♥ WIFI & Switch Controller Intil Log & Report ♦ Monitor	SSH SNMP FTM FortiTelemetry Networked Devices Device Detection Active Scanning Active Scanning Active Scanning Security Mode None Security Mode None Security Mode None Security Address	RADIUS Accor	unting		
0	Status Comments acass Interface State C Enabled Disabled OK C	ancel			

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.

FortiGate VM64 FGT	T-Nozomi			<u>ц</u> . (D• ≻_ [] •	dmin •
😰 Dashboard 🖮 FortiView	Create New Service Service	P Edit Clone 🕆 Delete	Category Settings Q Search			
O System	> Category	e Category	Details	IP/FQDN	Show in Service List	Ref
Policy & Objects IPv4 Policy IPv4 DoS Policy Addresses Internet Service Database Schedules Schedules Virtual IPs IP Produ	Conner al (4) Q ALL Q ALL CP Q ALL JCMP Q ALL JCMP Q ALL JCP Q ALL UDP Web Access (2) Web Access (2) Q HTTP Q HTTPS File Access (8)	General General General General Web Access Web Access	ANY ICMP/ANY TCP/1-65535 UDP/1-65535 TCP/80 TCP/443	0000 0000 0000 0000	0 0 0 0	59 0 0 1 2
Traffic Shapers Traffic Shaping Policy	AFS3	File Access	TCP/7000-7009 UDP/7000-7009	0.000	•	0
Security Profiles	> EFTP	File Access	TCP/21	0.0.0.0	•	0
D VPN	> FTP_GET	File Access	TCP/21	0.0.0.0	۲	0
🛔 User & Device	> EFTP_PUT	File Access	TCP/21	0.0.0.0	0	0
♥ WIFI & Switch Controller		File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	•	0
C Monitor	SAMBA	File Access	TCP/139	0.0.0.0	0	1
	SMB	File Access	TCP/445	0.0.0.0	0	1
Q	TETP	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.

FortiGate VM64 FG	[-Nozom]	admin•
2 Dashboard	> Edit Service	
FortiView Network System Policy & Objects IPv4 Policy IPv4 DoS Policy Addresses Internet Service Database Service	Name Modbus Comments Show in Service List Category Protocol Options Protocol Type TCP/UDP/SCTP Address IP Range FQDN 0.0.0.0 Destination Port CF V 502 Hith	
Schedules Virtual IPs IP Pools	Specify Source Ports OK Cancel	
Traffic Shapers Traffic Shaping Policy		
Security Profiles VPN User & Device VIFI & Switch Controller Log & Report Minitor	> > > >	
Q		

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.

FortiGate VM64 FG1	r-Noz	tomi										3	∆ • <i>®</i> •	>_ [] admin-
2 Dashboard	>	+0	reate New 🥜 Edit	🖹 Delete 🔍	Policy Lookup	Q Search							Interface Pa	ir View By Sequence
FortiView	>	Seq.#	T Name	T From		T To	T Source	T Destination	T Schedule	T Service	T Action	T NAT	T Log	T Security Profiles
+ Network	>	1	Accepted Protocols	IT Network (g	port1)	OT Network (port2)	🔲 all	🗉 all	G always	Modbus	✓ ACCEPT	O Disabled	IIA 🕲	
System	>	2	Implicit Denv			anv	(II) at		Co alurante		ODENY			
Policy & Objects	~	10	implicit o eriy	C) any		unty	388 111	- 100 (111)	LQ arrays	The Mark	DENT		UISabled	
IPv4 Policy	台													
IPv4 DoS Policy														
Addresses Internet Service Database														
Services Schedules														
Virtual IPs IP Pools														
Traffic Shapers Traffic Shaping Policy														
Security Profiles	>													
U VPN	>													
🛔 User & Device	>													
ViFi & Switch Controller	>													
Al Log & Report	>													
C Monitor	>													
Q							≪ < :	1 /1 > >	[Total: 2]					

Please follow the screenshot for the settings for the policy.

	Accepted Prot	ocols		
coming interface	IT Notwork	(nort1)		
uteoing Interface	CT Network	the (nort 2)		
ource	all	+	,	ĸ
estination	🗐 all	+	3	¢
chedule	Co always			•
ervice	Modbus	+	3	¢
ction	✓ ACCEPT	O DENY	E LEARN	
ecurity Profiles ntiVirus /eb Filter	0			
ecurity Profiles ntiVirus Veb Filter NS Filter	0			
ecurity Profiles ntiVirus Jeb Filter NS Filter pplication Control PS				
ecurity Profiles ntiVirus Veb Filter NS Filter pplication Control PS ogging Options				
ecurity Profiles ntiVirus Veb Filter NS Filter pplication Control PS ogging Options og Allowed Traffic	3	D Securi	ty Events A	II Sessi
ecurity Profiles ntiVirus Veb Filter NS Filter pplication Control PS ogging Options og Allowed Traffic enerate Logs when	Session Starts	D Securi	ty Events	II Sessio
ecurity Profiles nt/Virus Veb Filter NS Filter pplication Control 95 seging Options 35 Allowed Traffic enerate Logs when apture Packets	Session Starts	D Securi	ty Events	II Sessio

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.

FortiGate VM64 FG1	r-Nozomi			Δ · ⑦·	>_ [] admin→
Dashboard EartiView	> Edit Admini	strator	e 6266X 986		Prince P
Vetwork System	Comments	Nozomi User created for Nozomi Networks for Fabric Ready Intervention	Change Password		
Administrators Admin Profiles Firmware	Type Local User	integration	= =1:255		
HA HA SNMP Replacement Messages FortiGuard Security Fabric Advanced	Match aus Match all u group Administra Security	er on a remote server group sers in a remote server tor Profile super_admin	•		
Feature Select	C Restric	t login to trusted hosts			
Policy & Objects Security Profiles VPN	> Trusted Ho	t admin to guest account provi	+		
 ▲ User & Device ♥ WiFi & Switch Controller ▲ Log & Report 	>		OK Cancel		
C Monitor	>				

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."



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.

NOZOMI () Deathcard () Alarta () Environment (), Analysis			Bill System (3) edmin
Patine Politik Integration			Covigure Policies
Connected to Fortilett FortilGate 10.101.00.81		Options	
HER HEREAL Des Jahan Paramet	ष २ व	Control tools sounding Control tools sounding to the Control tools Control tools sounding to the Control tools Control Control tools Control Cont	

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 \rightarrow Data.
- 3. Clear all settings by clicking on "Select all."
- 4. Click on "Reset" and enter your password.

Deta	Reset	Restore
Reset different kind of data for all the users		
Select all Select none		
C 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		
Z Traces		
Reset the traces, both requested by users and generated by alerts		
Z Time machine		
Delete all the snapshots of the time machine		
Queries		
Delete all the queries and query groups		
Assertions		
Delete all the assertions		
Devel		
HUSA		

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:

ming	Overview Manage Network Learn
Network	Process
Lait detected changes never Learning stanist: 17:33:55.712 Nodes Links 4 - 0 0 · 0 - 0	Last detected change: never Lasming stands: never Nev valiables LEARNING AND PROTECTING an alert will be dynamically raised if a new Variable appears.
PROTECTING: LEARNING PROTECTING: you will receive alerts when an anomaly is detected. EARNING: the Environment incorporates new behavior as learned.	DISABLED: no alerting for new Process behavior. Dynamic Flow Control (EXAMINIA AND PROTECTING) DISABLED V = LEARNING AND PROTECTING: an alert is raised if cyclic access (read or write) to a variable becomes irregular. OISABLE: the terring 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."

aming	Overview Manage Network Learning
Network	Process
Laid detected charge: never Learning stands: 2017-07-10 17:33:55:712 Nodes Links	Last detected change: never Learning starticit never Nerv vasibles [EXPRING AND PROTECTING] Disket.KD [2] LEARNING AND PROTECTING: an alert will be dynamically raised if a new Variable appears. - DISABLED: no alerting for new Variables.
4.0.0	New values [LEARING AND PROTECTING] DISABLED
PROTECTING: LAANNA PROTECTING: you will nooelve allerts when an anomaly is detected. ELAANNAG: the Environment Incorporates new behavior as learned.	Dynamic Flow Control [EAMINIG AND PROTECTING] DISALED 9 LEAMINIG AND PROTECTING and and it is raised if cyclic access (read or write) to a variable becomes irregular. • DISALED The time into the access to variables will not be monitored and no allerts 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

- FortiGate/FortiOS Admin Guides <u>http://docs.fortinet.com/fortigate/admin-guides</u>
- 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



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, FortiCare* and FortiGuard*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warrantes, wether express or implied, except to the extent Fortine enternes a binding written contract, signal commitment by Fortinet; and Fortinet disclaims all warrantes, wether express or implied, except to the extent Fortine enternes a binding written contract, signal constants, and purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance in the same ideal conditions as in Fortinet is disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this building uncleanted in the exame ideal conditions hall be applicable.