

iROC FortiGate NGFW User Manual



Intelligent Cyber Secure Platform



Version: 1.0.3, Date: Sept 2021



© 2021 i5 Communications Inc. All rights reserved.

Copyright Notice

© 2021 iS5 Communications Inc. All rights reserved.

No Part of this publication may be reproduced in any form without the prior written consent of iS5 Communications Inc. (iS5).

Trademarks

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the Technical Specifications.

Warranty

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident. Refer to the Technical Specifications for the actual warranty period(s) of the product(s) associated with this publication. Warranty certificate available at: <https://is5com.com/warranty>

Disclaimer

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

Contact Information

iS5 Communications Inc. 5895 Ambler Dr., Mississauga, Ontario, L4W 5B7 Tel: 1+ 905-670-0004 // Fax: 1+ 289-401-5206 Website: <http://www.is5com.com/> Technical Support: E-mail: support@is5com.com
Sales Contact: E-mail: sales@is5com.com

TERMS AND CONDITIONS FOR SOFTWARE PROGRAMS AND EMBEDDED SOFTWARE IN PRODUCTS

1) EULA

All products which consist of or include software (including operating software for hardware supplied by Supplier and software in object code format that is embedded in any hardware) and/or any documentation shall be subject to the End User License Agreement (“EULA”) attached hereto as Exhibit A. Buyer shall be deemed to have agreed to be bound by all of the terms, conditions and obligations therein and shall ensure that all subsequent purchasers and licensees of such products shall be further bound by all of the terms, conditions and obligations therein. For software and/or documentation delivered in connection with these Terms and Conditions, that is not produced by Supplier and which is separately licensed by a third party, Buyer’s rights and responsibilities with respect to such software or documentation shall be governed in accordance with such third party’s applicable software license. Buyer shall, on request, enter into one or more separate “click-accept” license agreements or third party license agreements in respect thereto. Supplier shall have no further obligations with respect to such products beyond delivery thereof. Where Buyer is approved by Supplier to resell products, Buyer shall provide a copy of the EULA and applicable third party license agreements to each end user with delivery of such products and prior to installation of any software. Buyer shall notify Supplier promptly of any breach or suspected breach of the EULA or third party license agreements and shall assist Supplier in efforts to preserve Supplier’s or its supplier’s intellectual property rights including pursuing an action against any breaching third parties. For purposes of these terms and conditions: “software” shall mean scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language (“html”) and other computer mark-up languages; “hardware” shall mean mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment; and “documentation” shall mean documentation supplied by Supplier relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of any software.

2) INTELLECTUAL PROPERTY

Buyer shall not alter, obscure, remove, cancel or otherwise interfere with any markings (including without limitation any trademarks, logos, trade names, or labelling applied by Supplier). Buyer acknowledges that Supplier is the sole owner of the trademarks used in association with the products and that Buyer has no right, title or interest whatsoever in such trademarks and any goodwill associated therewith and that all goodwill associated with such trademarks is owned by and shall enure exclusively to and for the benefit of Supplier. Further, Buyer shall not represent in any manner that it has acquired any ownership rights in such trademarks or other intellectual property of Supplier. Supplier will defend any claim against Buyer that any iS5Com branded product supplied under these Terms and Conditions infringes third party patents or copyrights (a “Patent Claim”) and will indemnify Buyer against the final judgment entered by a court of competent jurisdiction or any settle-

ments arising out of a Patent Claim, provided that Buyer: (1) promptly notifies Supplier in writing of the Patent Claim; and (2) cooperates with Supplier in the defence of the Patent Claim, and grants Supplier full and exclusive control of the defence and settlement of the Patent Claim and any subsequent appeal. If a Patent Claim is made or appears likely, Buyer agrees to permit Supplier to procure for Buyer the right to continue using the affected product, or to replace or modify the product with one that is at least functionally equivalent. If Supplier determines that none of those alternatives is reasonably available, then Buyer will return the product and Supplier will refund Buyer's remaining net book value of the product calculated according to generally accepted accounting principles. Supplier has no obligation for any Patent Claim related to: (1) compliance with any designs, specifications, or instructions provided by Buyer or a third party on Buyer's behalf; (2) modification of a product by Buyer or a third party; (3) the amount or duration of use which Buyer makes of the product, revenue earned by Buyer from services it provides that use the product, or services offered by Buyer to external or internal Buyers; (4) combination, operation or use of a product with non-Supplier products, software or business processes; or (5) use of any product in any country other than the country or countries specifically authorized by Supplier.

3) **EXPORT CONTROLS AND SANCTIONS**

- a) In these Term and Conditions, "**Export Controls and Sanctions**" means the export control and sanctions laws of each of Canada, the US and any other applicable country, territory or jurisdiction including the United Nations, European Union and the United Kingdom, and any regulations, orders, guides, rules, policies, notices, determinations or judgements issued thereunder or imposed thereby.
- b) Supplier products, documentation and services provided under these Terms and Conditions may be subject to Canadian, U.S. and other country Export Controls and Sanctions. Buyer shall accept and comply with all applicable Export Control and Sanctions in effect and as amended from time to time pertaining to the export, re-export and transfer of Supplier's products, documentation and services. Buyer also acknowledges and agrees that the export, re-export or transfer of Supplier products, documentation and services contrary to applicable Export Controls and Sanctions may be a criminal offence.
- c) For greater certainty, Buyer agrees that (i) it will not directly or indirectly export, re-export or transfer Supplier products, documentation and services provided under these Terms and Conditions to any individual or entity in violation of any aforementioned Export Controls and Sanctions; (ii) it will not directly or indirectly export, re-export or transfer any such products, documentation and services to any country or region of any country that is prohibited by any applicable Export Controls and Sanctions or for any of the following end-uses, or in any of the following forms unless expressly authorized by any applicable government permit issued under or otherwise expressly permitted by applicable Export Controls and Sanctions:
 - i) For use that is directly or indirectly related to the research, design, handling, storage, operation, detection, identification, maintenance, development, manufacture, production or dissemination of chemical, biological or nuclear weapons, or any missile or other delivery systems for such weapons, space launch vehicles, sounding rockets or unmanned air vehicle systems;
 - ii) Technical information relating to the design, development or implementation of the cryptographic components, modules, interfaces, or architecture of any software; or

- iii) Source code or pseudo-code, in any form, of any of the cryptographic components, modules, or interfaces of any software.
- d) Buyer confirms that it is not (i) listed as a sanctioned person or entity under any Export Controls and Sanctions list of designated persons, denied persons or specially designated nationals maintained by the Canadian Department of Foreign Affairs, Trade and Development, the Canadian Department of Public Safety and Emergency Preparedness, the U.S. Office of Foreign Assets Control of the U.S. Department of the Treasury, the U.S. Department of State, the U.S. Department of Commerce, United Nations Security Council, the European Union or any EU member state, HM's Treasury, or any other department or agency of any of the aforementioned countries or territories, or the United Nations or any other country's sanctions-related list; (ii) owned or controlled by such person or entity; or (iii) acting in any capacity on behalf of or for the benefit of such person or entity. Buyer also confirms that this applies equally to any of its affiliates, joint venture partners, subsidiaries and to the best of Buyer's knowledge, any of its agents or representatives.

Exhibit A: End User License Agreement

IMPORTANT – READ CAREFULLY: iS5 Communications Inc. (“**iS5Com**”) licenses the iS5Com Materials (as defined below) subject to the terms and conditions of this end user license agreement (the “**EULA**”). BY SELECTING “ACCEPT” OR OTHERWISE EXPRESSLY AGREEING TO THIS EULA, BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, OR BY USING THE HARDWARE (AS DEFINED BELOW), ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS EULA BECOME LEGALLY BINDING ON THE CUSTOMER. This End User License Agreement (the “**EULA**”) supplements the Terms and Conditions or such other terms and conditions between iS5Com or, if applicable, a reseller for iS5Com, and the Customer (as defined below) (in either case, the “**Contract**”).

1) DEFINITIONS

*“**Confidential Information**” means all data and information relating to the business and management of iS5Com, including iS5Com Materials, trade secrets, technology and records to which access is obtained hereunder by the Customer, and any materials provided by iS5Com to the Customer, but does not include any data or information which: (a) is or becomes publicly available through no fault of the Customer; (b) is already in the rightful possession of the Customer prior to its receipt from iS5Com; (c) is already known to the Customer at the time of its disclosure to the Customer by iS5Com and is not the subject of an obligation of confidence of any kind; (d) is independently developed by the Customer; (e) is rightfully obtained by the Customer from a third party; (e) is disclosed with the written consent of iS5Com; or (f) is disclosed pursuant to court order or other legal compulsion.*

- “**Customer**” means the licensee of the iS5Com Software pursuant to the Contract.
- “**iS5Com Documentation**” means Documentation supplied by or on behalf of iS5Com under the Contract relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of iS5Com Software, or iS5Com Firmware.
- “**iS5Com Firmware**” means iS5Com Software in object code format that is embedded in iS5Com Hardware.
- “**iS5Com Hardware**” means Hardware supplied by or on behalf of iS5Com under the Contract.

- **“i5Com Materials”** means, collectively, the i5Com Software and the i5Com Documentation.
- **“i5Com Software”** means Software supplied by or on behalf of i5Com under the Contract. For greater certainty, i5Com Software shall include all operating Software for i5Com Hardware, and i5Com Firmware.
- **“Documentation”** means written instructions and manuals of a technical nature.
- **“EULA”** means this End User License Agreement.
- **“Hardware”** means hardware, mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment.
- **“Intellectual Property Rights”** means any and all proprietary rights provided under: (i) patent law; (ii) copyright law (including moral rights); (iii) trade-mark law; (iv) design patent or industrial design law; (v) semi-conductor chip or mask work law; or (vi) any other statutory provision or common law principle applicable to this EULA, including trade secret law, which may provide a right in either Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how generally, or the expression or use of such Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how trade secret law; any and all applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing; and all licenses and waivers and benefits of waivers of the intellectual property rights set out herein, all future income and proceeds from the intellectual property rights set out herein, and all rights to damages and profits by reason of the infringement of any of the intellectual property rights set out herein.
- **“Software”** means scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language (“html”) and other computer mark-up languages.
- **“Third Party License Terms”** means additional terms and conditions that are applicable to Third Party Software.
- **“Third Party Software”** means Software owned by any third party, licensed to i5Com and sublicensed to the Customer.
- **“Update”** means a supplemented or revised version of i5Com Software which rectifies bugs or makes minor changes or additions to the functionality of i5Com Software and is designated by i5Com as a higher release number from, for example, 6.06 to 6.07 or 6.1 to 6.2.

2) LICENSE

– 2.1 License Grant

The i5Com hereby grants to the Customer, subject to any Third Party License Terms, a non-exclusive, non-transferable, non-sublicensable right and licence to use i5Com Materials solely in object code format, solely for the Customer’s own business purposes, solely in accordance with this EULA (including, for greater certainty, subject to Section 6.1 of this EULA) and the applicable i5Com Documentation, and, in the case of i5Com Firmware, solely on i5Com Hardware on which i5Com Firmware was installed, provided that Customer may only install i5Com Software on such number of nodes expressly set out in the Contract.

– **2.2 License Restrictions**

Except as otherwise provided in Section 2.1 above, the Customer shall not: (a) copy iS5Com Materials for any purpose, except for the sole purpose of making an archival or back-up copy; (b) modify, translate or adapt the iS5Com Materials, or create derivative works based upon all or part of such iS5Com Materials; (c) assign, transfer, loan, lease, distribute, export, transmit, or sublicense iS5Com Materials to any other party; (d) use iS5Com Materials for service bureau, rent, timeshare or similar purposes; (e) decompile, disassemble, decrypt, extract, or otherwise reverse engineer, as applicable, iS5Com Software or iS5Com Hardware; (f) use iS5Com Materials in a manner that uses or discloses the Confidential Information of iS5Com or a third party without the authorization of such person; (g) permit third parties to use iS5Com Materials in any way that would constitute breach of this EULA; or (h) otherwise use iS5Com Materials except as expressly authorized herein.

– **2.3 Updates and Upgrades**

The license granted hereunder shall apply to the latest version of iS5Com Materials provided to the Customer as of the effective date of this EULA, and shall apply to any Updates and Upgrades subsequently provided to the Customer by iS5Com pursuant to the terms of this EULA. Customer shall only be provided with Updates and/or Upgrades if expressly set out in the Contract.

– **2.4 Versions**

In the event any Update or Upgrade includes an amended version of this EULA, Customer will be required to agree to such amended version in order to use the applicable iS5Com Materials and such amended EULA shall be deemed to amend the previously effective version of the EULA.

– **2.5 Third Party Software**

Customer shall comply with any Third Party License Terms.

3) **OWNERSHIP**

– **3.1 Intellectual Property**

Notwithstanding any other provision of the Contract, iS5Com and the Customer agree that iS5Com is and shall be the owner of all Intellectual Property Rights in iS5Com Materials and all related modifications, enhancements, improvements and upgrades thereto, and that no proprietary interests or title in or to the intellectual property in iS5Com Materials is transferred to the Customer by this EULA. iS5Com reserves all rights not expressly granted to the Customer under Section 2.1.

– **3.2 Firmware**

iS5Com and the Customer agree that any and all iS5Com Firmware in or forming a part of iS5Com Hardware is being licensed and not sold, and that the words “purchase,” “sell” or similar or derivative words are understood and agreed to mean “license,” and that the word “Customer” as used herein are understood and agreed to mean “licensee,” in each case in connection with iS5Com Firmware.

– **3.3 Third Party Software**

Certain of iS5Com Software provided by iS5Com may be Third Party Software owned by one or more third parties and sublicensed to the Customer. Such third parties retain ownership of and

title to such Third Party Software, and may directly enforce the Customer's obligations hereunder in order to protect their respective interests in such Third Party Software.

4) **CONFIDENTIALITY**

– **4.1 Confidentiality**

The Customer acknowledges that i55Com Materials contain Confidential Information of i55Com and that disclosure of such Confidential Information to any third party could cause great loss to i55Com. The Customer agrees to limit access to i55Com Materials to those employees or officers of the Customer who require access to use i55Com Materials as permitted by the Contract and this EULA and shall ensure that such employees or officers keep the Confidential Information confidential and do not use it otherwise than in accordance with the Contract and this EULA. The obligations set out in this Section 4 shall continue notwithstanding the termination of the Contract or this EULA and shall only cease to apply with respect to such part of the Confidential Information as is in, or passes into, the public domain (other than in connection with the Customer's breach of this EULA) or as the Customer can demonstrate was disclosed to it by a third person who did not obtain such information directly or indirectly from i55Com.

– **4.2 Irreparable Harm**

Without limiting any other rights or remedies available to i55Com in law or in equity, the Customer acknowledges and agrees that the breach by Customer of any of the provisions of this EULA would cause serious and irreparable harm to i55Com which could not adequately be compensated for in damages and, in the event of a breach by the Customer of any of such provisions, the Customer hereby consents to an injunction against it restraining it from any further breach of such provisions.

– **4.3 Security**

*Any usernames, passwords and/or license keys ("**Credentials**") provided to you by i55Com shall be maintained by the Customer and its representatives in strict confidence and shall not be communicated to or used by any other persons. THE CUSTOMER SHALL BE RESPONSIBLE FOR ALL USE OF CREDENTIALS, REGARDLESS OF THE IDENTITY OF THE PERSON(S) MAKING SUCH USE, AND WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, IS5COM SHALL HAVE NO RESPONSIBILITY OR LIABILITY IN CONNECTION WITH ANY UNAUTHORIZED USE OF CREDENTIALS.*

5) **LIMITATION OF LIABILITY**

– **5.1 Disclaimer**

EXCEPT FOR THE EXPRESS WARRANTIES MADE BY IS5COM IN THE CONTRACT, (A) IS5COM MAKES NO AND HEREBY EXPRESSLY DISCLAIMS, AND THE PARTIES HERETO HEREBY EXPRESSLY WAIVE AND EXCLUDE TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, AND THE CUSTOMER AGREES NOT TO SEEK OR CLAIM ANY BENEFIT THEREOF, IN EACH CASE, ALL WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS (AND THERE ARE NO OTHER WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, OF ANY KIND WHATSOEVER SET OUT HEREIN) WITH RESPECT TO THE IS5COM MATERIALS, INCLUDING AS TO THEIR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, DESIGN OR CONDITION, COMPLIANCE WITH THE REQUIREMENTS OF ANY APPLICABLE LAWS, CONTRACT OR SPECIFICATION, NON- INFRINGE-

MENT OF THE RIGHTS OF OTHERS, ABSENCE OF LATENT DEFECTS, OR AS TO THE ABILITY OF THE IS5COM MATERIALS TO MEET CUSTOMER'S REQUIREMENTS OR TO OPERATE OF ERROR FREE; AND (B) THE IS5COM MATERIALS ARE PROVIDED "**AS IS**" WITHOUT WARRANTY OR CONDITION OF ANY KIND.

– **5.2 Limitation of Liability**

EXCEPT AS EXPRESSLY PROVIDED IN THE CONTRACT, IN NO EVENT SHALL IS5COM BE LIABLE TO THE CUSTOMER OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING UNDER OR IN CONNECTION WITH THIS EULA EVEN IF ADVISED OF THE POSSIBILITY THEREOF. THIS LIMITATION SHALL APPLY IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND OR CLAIM, INCLUDING BREACH OF CONTRACT, NEGLIGENCE, TORT OR ANY OTHER LEGAL THEORY, AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES AND/OR FAILURE OF THE ESSENTIAL PURPOSE OF THIS EULA.

6) **TERM**

– **6.1 Term**

Customer's right to use i55Com Materials shall terminate at such time as set out in the Contract or upon termination or expiration of the Contract, in each case at which time this EULA shall be deemed to terminate.

– **6.2 Survival**

Each of Sections 1, 2.4, 3, 4, 5, 6.2, and 7 shall survive termination of the EULA.

7) **MISCELLANEOUS**

– **7.1 Miscellaneous**

This EULA is (together with, as applicable, any click-wrap license agreement or Third Party License Terms pertaining to the use of i55Com Materials) the entire agreement between the Customer and i55Com pertaining to the Customer's right to access and use i55Com Materials, and supersedes all prior or collateral oral or written representations or agreements related thereto. Notwithstanding anything to the contrary contained in the Contract, to the extent of any inconsistency between this EULA and the Contract, or any such applicable click-wrap agreement, this EULA shall take precedence over the Contract and such click-wrap agreement. In the event that one or more of the provisions is found to be illegal or unenforceable, this EULA shall not be rendered inoperative but the remaining provisions shall continue in full force and effect. The parties expressly disclaim the application of the United Nations Convention for the International Sale of Goods. This EULA shall be governed by the laws of the Province of Ontario, Canada, and federal laws of Canada applicable therein. In giving effect to this EULA, neither party will be or be deemed an agent of the other for any purpose and their relationship in law to the other will be that of independent contractors. Any waiver of any terms or conditions of this EULA: (a) will be effective only if in writing and signed by the party granting such waiver, and (b) shall be effective only in the specific instance and for the specific purpose for which it has been given and shall not be deemed or constitute a waiver of any other provisions (whether or not similar) nor shall such waiver constitute a continuing waiver unless otherwise expressly provided. The failure of either party to exercise, and any delay in exercising, any of its rights hereunder, in whole or in part, shall not constitute or be deemed a waiver or forfeiture of such rights, neither in the specific instance nor on a continuing basis. No single or partial exercise of any such right shall preclude any other or further exercise of such right

or the exercise of any other right. Customer shall not assign or transfer this EULA or any of its rights or obligations hereunder, in whole or in part, without the prior written consent of iS5Com. The division of this EULA into sections and the insertion of headings are for convenience of reference only and shall not affect the construction or interpretation of this EULA. References herein to Sections are to sections of this Agreement. Where the word “include”, “includes” or “including” is used in this EULA, it means “include”, “includes” or “including”, in each case, “without limitation”. All remedies provided for iS5Com under this EULA are non-exclusive and are in addition, and without prejudice, to any other rights as may be available to of iS5Com, whether in law or equity. By electing to pursue a remedy, of iS5Com does not waive its right to pursue any other available remedies. The parties acknowledge that they have required this Agreement to be written in English. Les parties aux présentes reconnaissent qu’elles ont exigé que la présente entente soit rédigée en anglais.

– **7.2 Subject to Change**

Terms and Conditions are subject to change. For the latest information please visit:
<https://is5com.com/terms-and-conditions/>

Contents

	iROC FortiGate NGFW User Manual	i
	Copyright Notice	ii
	TERMS AND CONDITIONS FOR SOFTWARE PROGRAMS AND EMBEDDED SOFTWARE IN PRODUCTSiii
Chapter: 1	Introduction	1
	Purpose and Scope	1
	FortiGate-VM Summary	1
	iROC Module	2
Chapter: 2	FortiGate Architecture with iROC Module	5
	iROC System Configuration	5
Chapter: 3	Registering FortiGate-VM Virtual Appliance	6
Chapter: 4	Installation and Configuration of FortiGate License	7
	Configuring of IP manually for a Connection to Internet	7
	System IP Change	7
	FortiGate-VM IP Change	9
	Configuring New IP Address for the PC13
	Checking Connectivity14
	Uploading, Validating and Configuring FortiGate License14
	Changing System (Linux) Password (Recommended)17

INTRODUCTION

1. Introduction

Fortinet's FortiGate-VM product is a Next-Generation Firewall (NGFW) that provides the ability to identify attacks, malware, and other threats and blocks threats. By extending beyond stateful firewall capabilities, NGFWs provide SSL inspection, applications control, and deep packet inspection (DPI) and identify threats across multiple attacks surfaces specific to OT environments.

Combined with the FortiGate-VM®, the iROC module of the i5Com's RAPTOR platform enables industrial applications to have "best in breed" security solutions for their OT applications. The integration of FortiGate-VM into i5Com's leading-edge RAPTOR® iMX350 & iMX950 models offers a cost-effective and flexible option as well.

By integrating the Fortinet with the iROC module into the RAPTOR platform with the iROC module, i5Com offers an industrial-grade NGFW solution that reduces the cost, space, complexity, and time to deploy the solution.

1.1. Purpose and Scope

This document provides the initial guidance on how to set up an iROC and FortiGate Firewall.

Users are highly recommended to change the iROC OS(Linux) password. iROC System password change procedures are provided in this document.

FortiGate Firewall will be forced to change the password for first time login.

1.2. FortiGate-VM Summary

The FortiGate-VM on Linux KVM delivers Next-Generation Firewall (NGFW) capabilities for organizations of all sizes. It protects against cyber threats with high performance, security efficacy, and deep visibility.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevents and detects known and unknown attacks using continuous threat intelligence from Artificial Intelligence (AI)-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology with DPDK (Data Plane Development Kit) and vNP offloading and SR-IOV (Single Root I/O Virtualization) technologies
- Provides industry-leading performance and protection for SSL encrypted traffic
- Supports Intel QuickAssist Technology (QAT) acceleration for throughput improvements on IPsec VPN

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources (only BYOL supports VDOM)
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

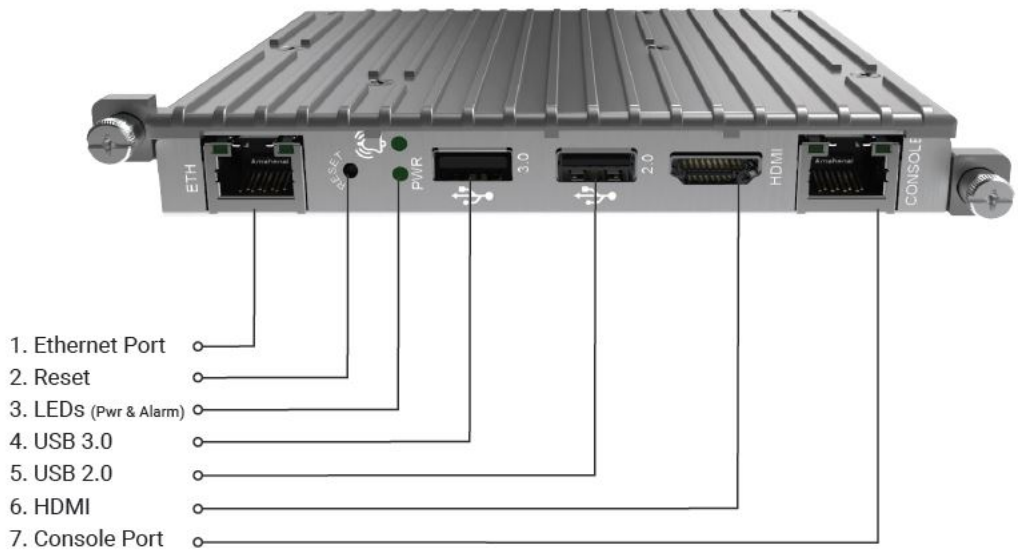
Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
- Out-of-the-box integration and orchestration with leading SDN platforms

1.3. iROC Module

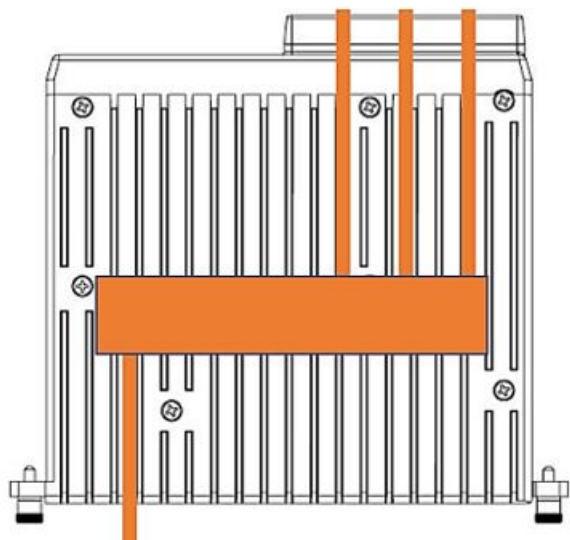
The iROC computing module is a hot-swappable industrial computing module that can be inserted into slots 1 through 4 of the RAPTOR iMX350.

Figure 1: Front View of the iROC Module



The iROC module supports up to three network connections through its backplane and one on its faceplate. The interfaces are 1 Gbps; however, they have an effective throughput of less than 1 Gbps based on factors such as CPU load, operating system, and other system demands.

Figure 2: iROC Backplane Interfaces



The three backplane ports of the iROC are connected to the switch fabric internal ports. The table below shows the mapping between the iROC module ports and the switch fabric based on the slot number where the iROC is inserted.

Table 1: Network Interface Availability

iROC Location	Port 1	Port 2	Port 2
Line Module 1	Gi 0/1	Gi 0/5	
Line Module 2	Gi 0/9	Gi 0/13	
Line Module 3	Gi 0/17	Gi 0/21	
Line Module 4	Ex 0/1	Ex 0/3	Ex 0/4

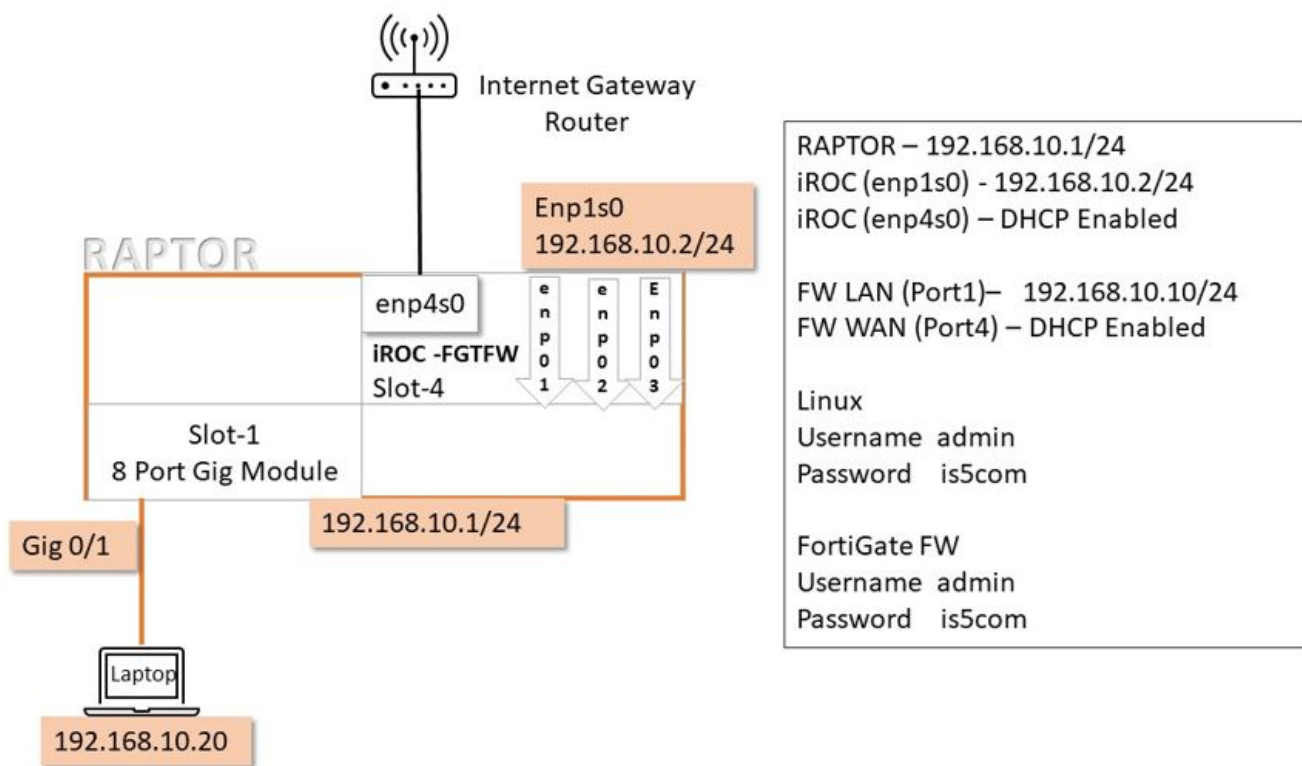
2. FortiGate Architecture with iROC Module

2.1. iROC System Configuration

- iROC with 8 GB RAM and 512 GB HD
- OS CentOS 7 (customized installation with virtualization server only)
- iROC module is to be installed in slot 4. It is recommended to use slot 4 to populate all four network interfaces; if a 10g module has already been installed in slot 4, then use slot 3.
- Enp1s0 – for internal connectivity with RAPTOR (internal interface)
- Enp4s0 – for external connectivity with iROC/FW (iROC MGMT physical network interface)

The figure below represents the initial IP configuration and credentials of the iROC FortiGate Firewall in the RAPTOR.

Figure 1: Internal Architecture of RAPTOR with iROC in Slot 4



3. Registering FortiGate-VM Virtual Appliance

Registering the FortiGate-VM virtual appliance with Customer Service & Support allows you to obtain the FortiGate- VM virtual appliance license file.

To register the FortiGate-VM virtual appliance:

- Log in to the Fortinet Customer Service & Support site at <https://support.fortinet.com/> using a support account or select **Sign Up** to create an account.
- On the main page, under **Asset**, select **Register / Renew**.
- On the Registration Page, enter the registration code emailed to you and select **Register** to access the registration form.
- Complete and submit the registration form.
- On the Registration Acknowledgment page, click **License File Download** link.
- Save the license file (.lic) to your local computer.

4. Installation and Configuration of FortiGate License

The FortiGate Firewall comes preinstalled in the iROC module. This section will document how to activate the license.

PREREQUISITE:

- 1) To validate the FortiGate License, an Internet connection to iROC and Fortinet is needed.
- 2) Both iROC MGMT (Faceplate NIC) and FortiGate WAN Port (Port 4) should have DHCP enabled.
- 3) There should be a connection to the Internet using IP from DHCP Server of your company network, or
- 4) An IP should be configured manually for a connection to Internet.

4.1. Configuring of IP manually for a Connection to Internet

1. The following steps are required for configuring manually an IP for a connection to Internet - **System IP Change** and **FortiGate-VM IP Change**.

System IP Change

1. Connect Keyboard Mouse and Monitor to iROC.
2. Login to CentOS 7. The username is **admin** and the password is **is5com**.
3. Step 1 - Change the System IP (Ethernet (enp4s0)) as shown on the figures below. Click where indicated by the arrows.

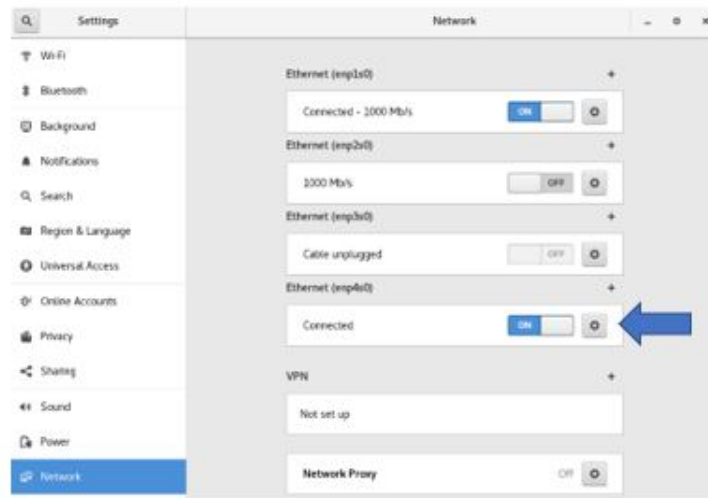
STEP RESULT: The following screen will appear.

Figure 1: Step 1



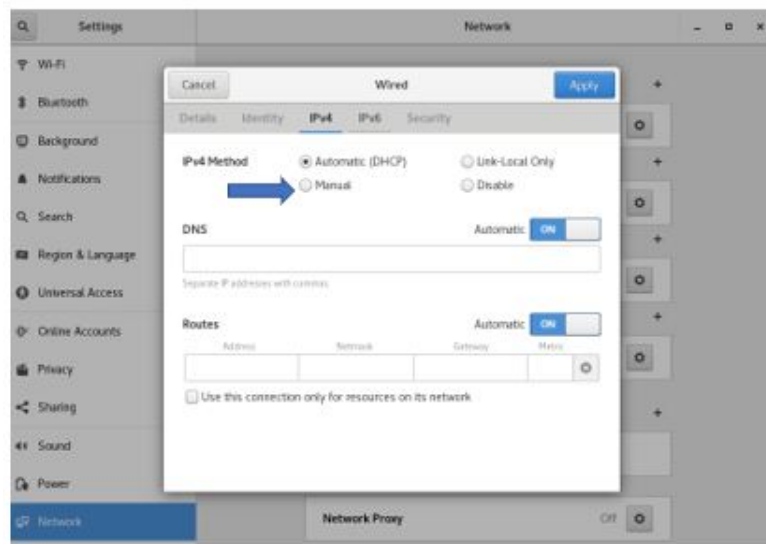
4. Step 2 - Click the indicated by an arrow icon.

STEP RESULT: The following screen will appear.

Figure 2: Step 2

5. Step 3- Click the indicated by an arrow icon.

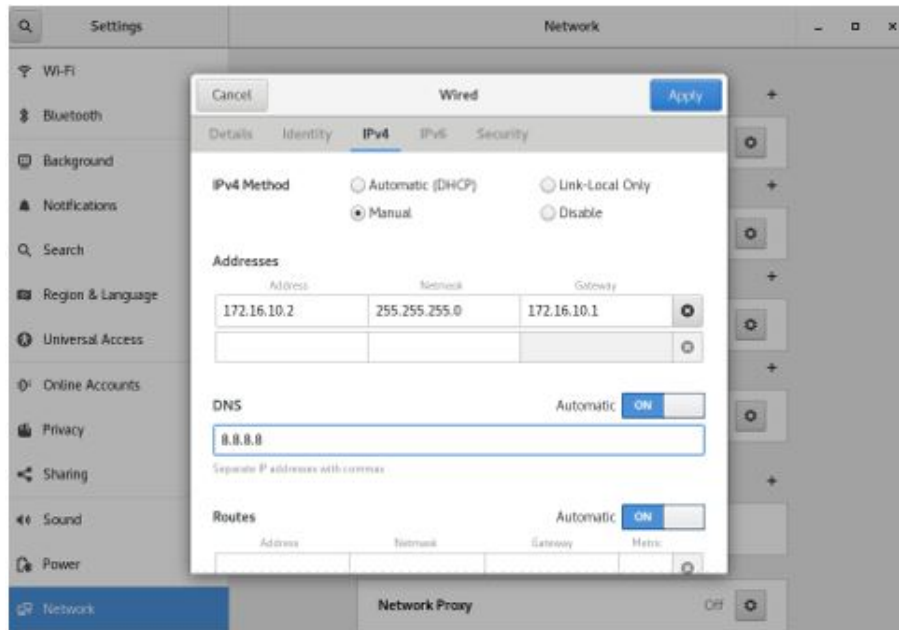
STEP RESULT: The following screen will appear.

Figure 3: Step 3

6. Step 4 - Configure the System IP (Ethernet (enp4s0)) and DNS for Internet connection (see above for an example IP configuration), and then click **Apply**.

STEP RESULT: The following screen will appear.

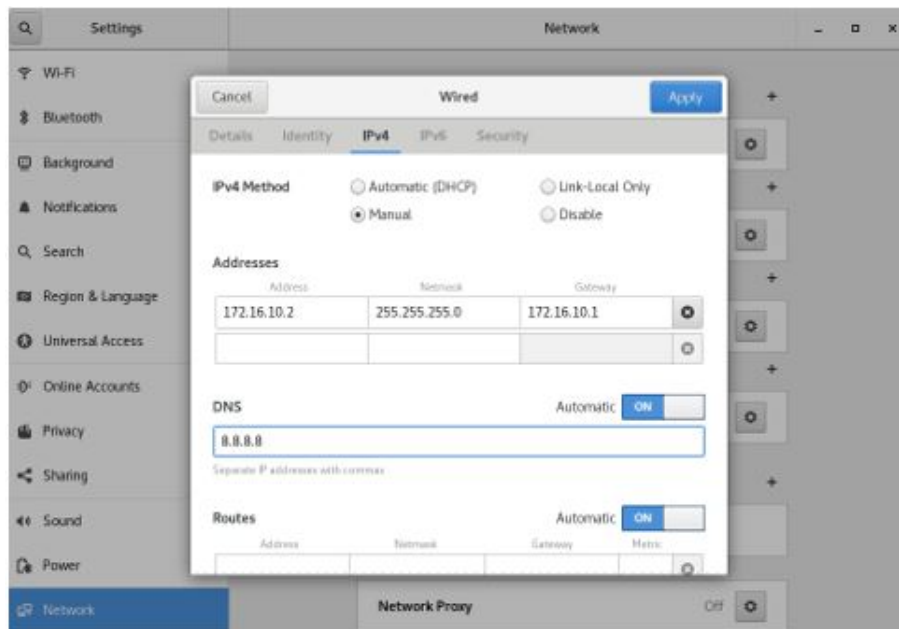
Figure 4: Step 4



- Step 5 - Restart the interface using the ON/OFF button. See where indicated by an arrow.

STEP RESULT: The following screen will appear.

Figure 5: Step 5

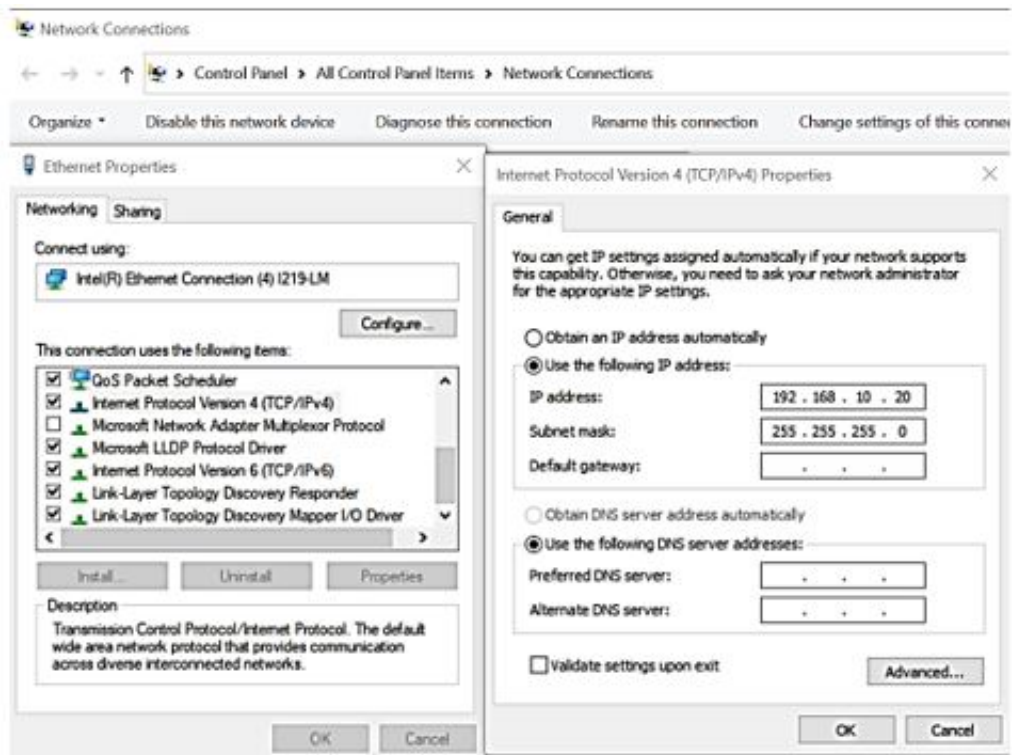


- Step 6 - in a web browser, go to **Application > Favourites** and verify the Internet connection.

FortiGate-VM IP Change

- Configure the PC to have **IP Address** 192.168.10.20 and **Subnet Mask** 255.255.255.0.

STEP RESULT: Enter the information in the following screen.

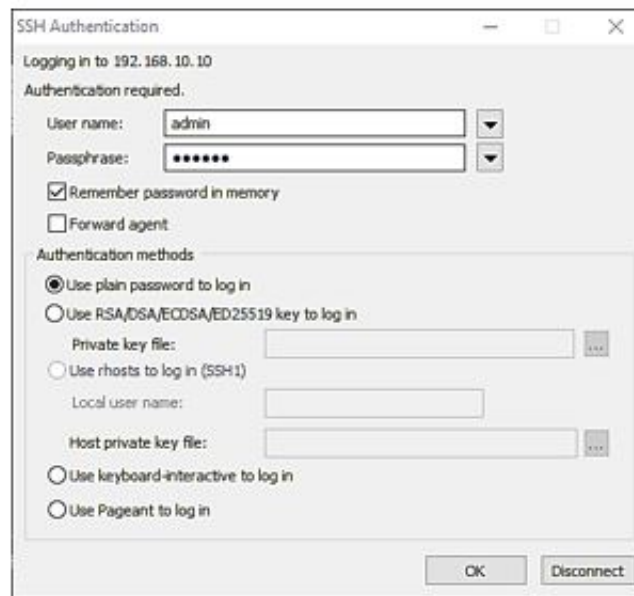
Figure 6: Network Connection

2. Connect one end of the 5' Ethernet cable to the PC network port. Connect the other end to the RAPTOR Gig Port.
3. Now ping the following IP addresses from your PC to check the connectivity.

FOR EXAMPLE: Ping the following:

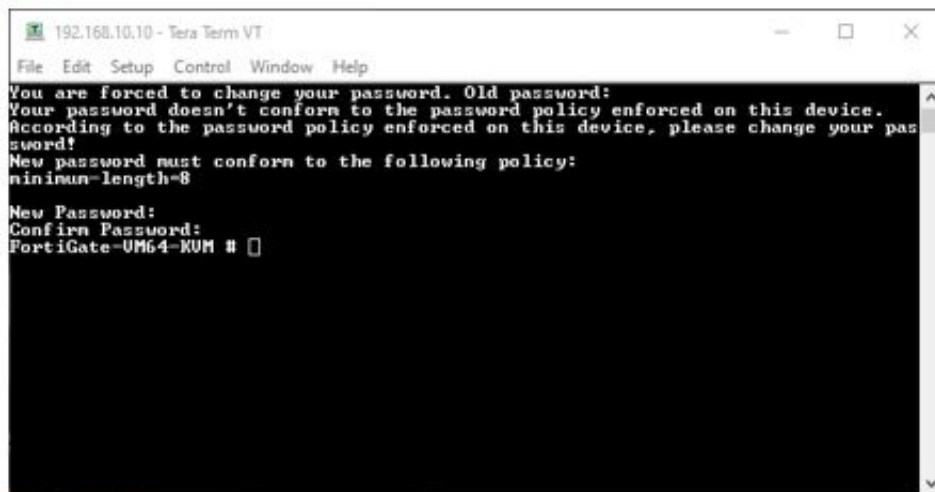
- a. RAPTOR IP 192.168.10.1
 - b. iROC preconfigured IP 192.168.10.2
 - c. FortiGate Firewall IP 192.168.10.10
4. For SSH to iROC FortiGate FW - 192.168.10.10:

STEP RESULT: Enter username **admin** and password **is5comin** in the following screen.

Figure 7: SSH Authentication

5. During first time login, the password must be changed.

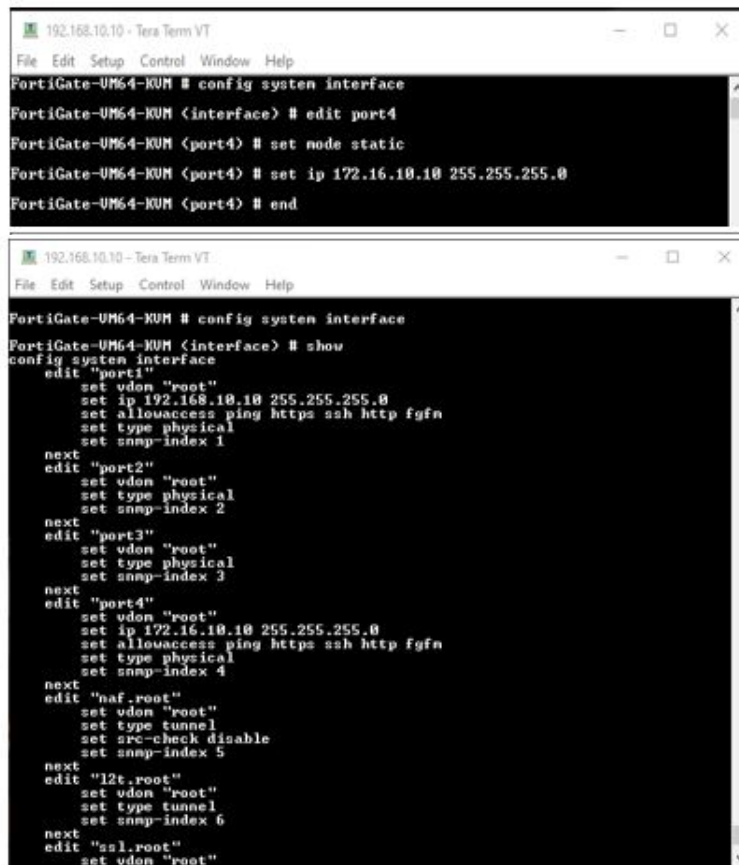
STEP RESULT: Start a Tera Term session and change the password as follows.

Figure 8: Tera Term- Change Password during First Time Login

6. Configure the port4 IP address.

FOR EXAMPLE: Start a Tera Term session and use an IP address of 172.16.10.10.

```
config system interface
edit port4
set mode static
set ip 172.16.10.10 255.255.255.0
end
```

Figure 9: Tera Term- Configuring of port4 IP address

```
192.168.10.10 - Tera Term VT
File Edit Setup Control Window Help
FortiGate-UM64-KUM # config system interface
FortiGate-UM64-KUM <interface> # edit port4
FortiGate-UM64-KUM <port4> # set mode static
FortiGate-UM64-KUM <port4> # set ip 172.16.10.10 255.255.255.0
FortiGate-UM64-KUM <port4> # end

192.168.10.10 - Tera Term VT
File Edit Setup Control Window Help
FortiGate-UM64-KUM # config system interface
FortiGate-UM64-KUM <interface> # show
config system interface
edit "port1"
    set vdon "root"
    set ip 192.168.10.10 255.255.255.0
    set allowaccess ping https ssh http fgfn
    set type physical
    set snmp-index 1
next
edit "port2"
    set vdon "root"
    set type physical
    set snmp-index 2
next
edit "port3"
    set vdon "root"
    set type physical
    set snmp-index 3
next
edit "port4"
    set vdon "root"
    set ip 172.16.10.10 255.255.255.0
    set allowaccess ping https ssh http fgfn
    set type physical
    set snmp-index 4
next
edit "haf.root"
    set vdon "root"
    set type tunnel
    set src-check disable
    set snmp-index 5
next
edit "l2t.root"
    set vdon "root"
    set type tunnel
    set snmp-index 6
next
edit "ssl.root"
    set vdon "root"
```

7. Configure the default gateway.

FOR EXAMPLE: In a Tera Term session, enter the following CLI commands.

```
config router static
edit 1
    set device port4
    set gateway 172.16.10.1
next
end
```

Figure 10: Tera Term- Configuring of Default Gateway

```

192.168.10.10 - Tera Term VT
File Edit Setup Control Window Help
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM #
FortiGate-UM64-KUM # config router static
FortiGate-UM64-KUM <static> # edit 1
new entry '1' added
FortiGate-UM64-KUM <1> # set device port4
FortiGate-UM64-KUM <1> # set gateway
<class_ip> Class A,B,C ip xxx.xxx.xxx.xxx
FortiGate-UM64-KUM <1> # set gateway 172.16.10.1
FortiGate-UM64-KUM <1> # next
FortiGate-UM64-KUM <static> # end
FortiGate-UM64-KUM #

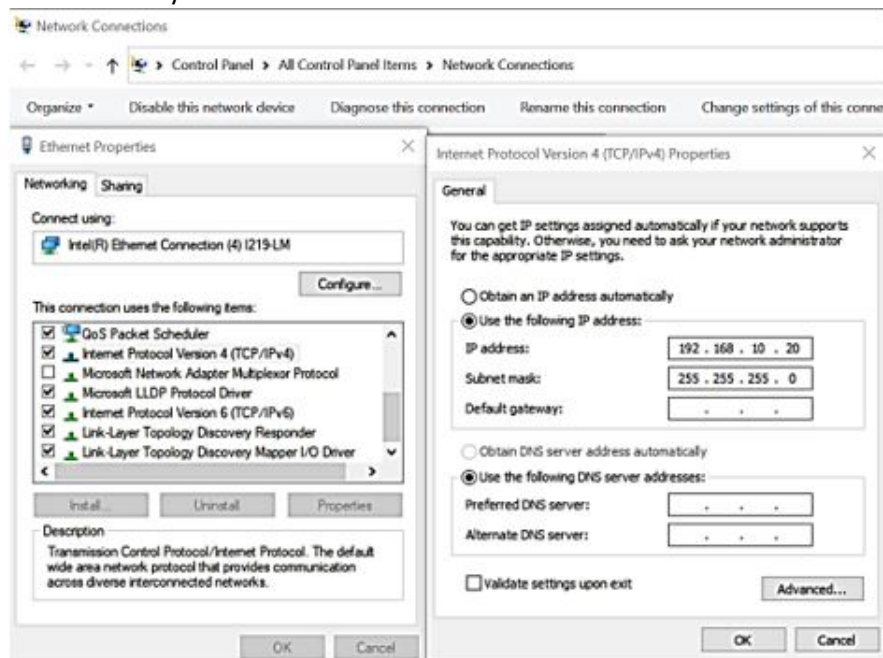
FortiGate-UM64-KUM #
FortiGate-UM64-KUM # config router static
FortiGate-UM64-KUM <static> # show
config router static
edit 1
set gateway 172.16.10.1
set device "port4"
next
end
FortiGate-UM64-KUM <static> #

```

4.2. Configuring New IP Address for the PC

1. After establishing the Internet connectivity to iROC+FortiGate FW, configure the PC IP address and subnet mask.

STEP RESULT: In the **Network Connectivity** screen, enter **IP address** of 192.168.10.20 and **Subnet Mask** of 255.255.255.

Figure 11: Network Connectivity

4.3. Checking Connectivity

1. Connect one end of the Ethernet cable to the PC network port. Connect the other end to the RAPTOR Gigabit Port.

FOR EXAMPLE: To check the connectivity, from your PC, ping the following.

- a. RAPTOR IP 192.168.10.1
- b. iROC preconfigured IP 192.168.10.2
- c. FortiGate Firewall IP 192.168.10.10

4.4. Uploading, Validating and Configuring FortiGate License

1. To upload and validate the FortiGate License:
 - a. Start the web browser Microsoft Edge.
 - b. Type FortiGate FW WAN IP 192.168.10.10.
 - c. To login, use username **admin** and password **is5com**.

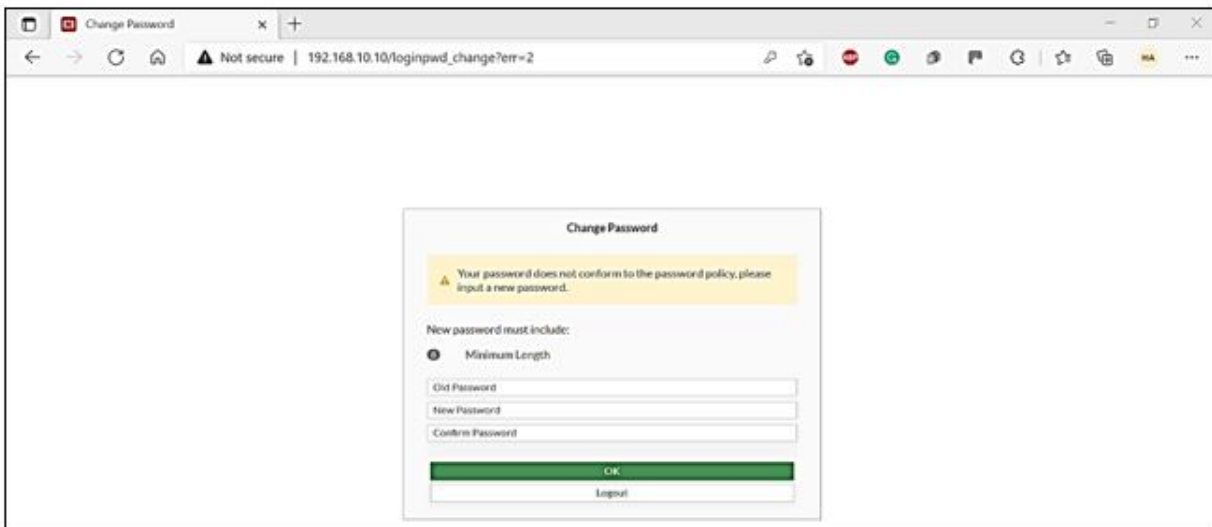
STEP RESULT: Enter the information in the following screen:

Figure 12: Uploading and validating the FortiGate License

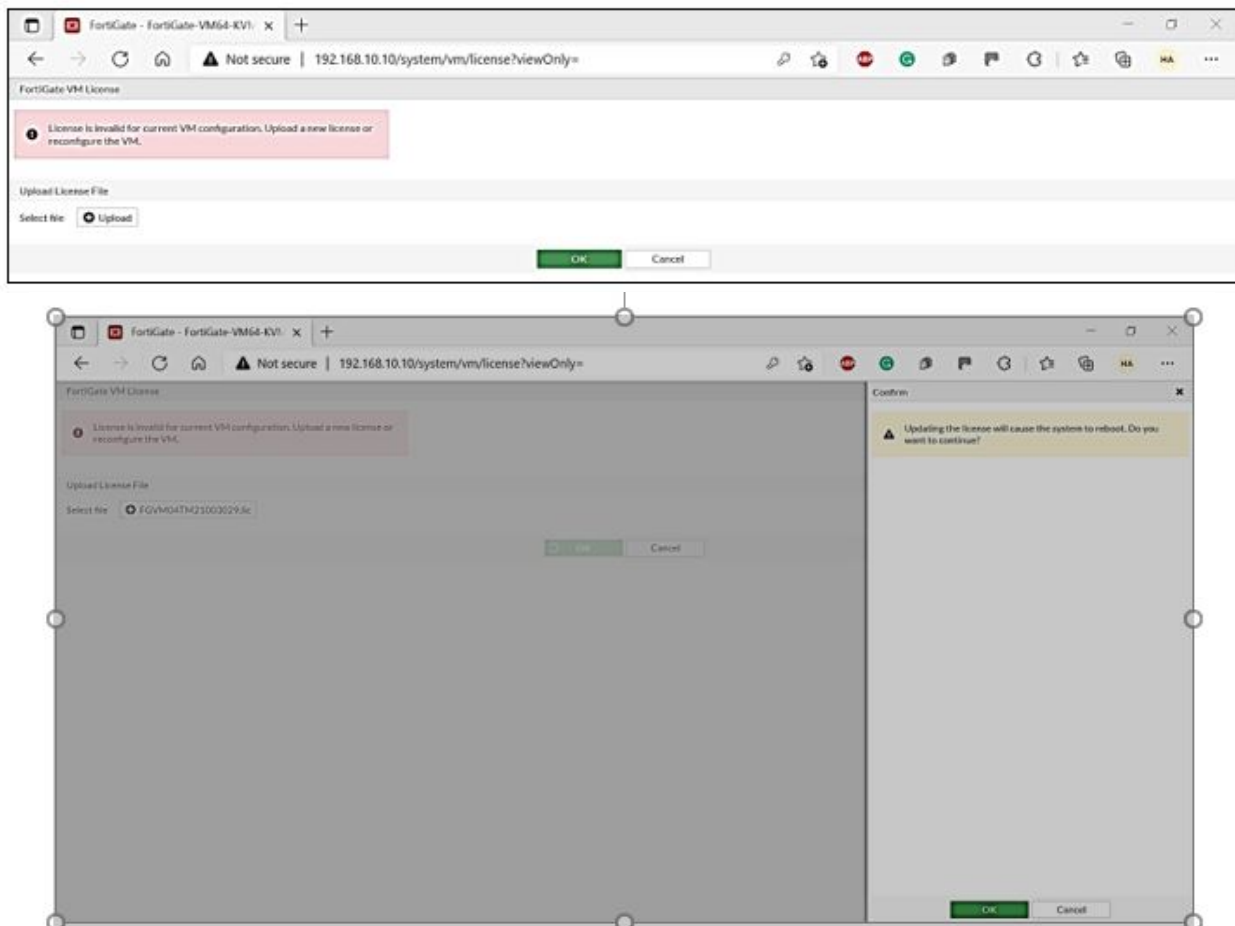


2. After logging in for the first time, there will be a prompt for the password for FortiGate Firewall to be changed (with a minimum length of 8 characters).

FOR EXAMPLE: Change the password in the following screen.

Figure 13: Change of password

STEP RESULT: After successful login, click **Upload** icon in **FortiGate VM License** screen. Upload the license from your computer and click **OK**.

Figure 14: FortiGate VM License Screen

Click **OK** to continue - the Firewall restarts.

3. Login into the Fortinet Firewall Web portal with the new password.

STEP RESULT: The following screen appears.

Figure 15: FortiGate Setup

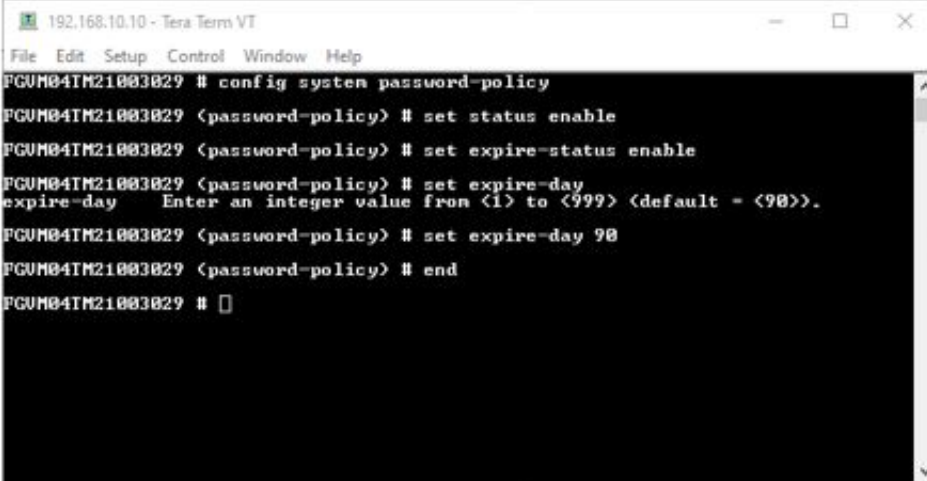


4. For configuring the FortiGate Firewall and its management, refer to the [Fortinet Documentation Library](#).
5. For FortiGate Password Expiry configuration (FortiGate FW factory settings for password policy), perform the following:
 - a. Connect one end of the 5' Ethernet cable to the PC network port. Connect the other end to the RAPTOR Gigabit Port.
 - b. For SSH to iROC FortiGate FW - 192.168.10.10, use username **admin** and password **xxxxxxxx**.
 - c. Configure the FortiGate Firewall for Password Policy.

FOR EXAMPLE: Open a Tera Term session and enter the following CLI commands.

```
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # config system password-policy
FortiGate-VM64-KVM (password-policy) # set status enable
FortiGate-VM64-KVM (password-policy) # set expire-status enable
FortiGate-VM64-KVM (password-policy) # set expire-day 90
FortiGate-VM64-KVM (password-policy) # end
FortiGate-VM64-KVM #
```

RESULT: The following screen appears.

Figure 16: Configuring the FortiGate Firewall for Password Policy

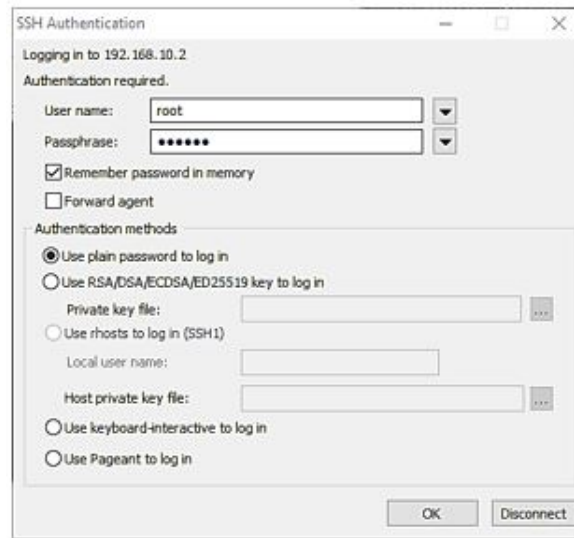
```
192.168.10.10 - Tera Term VT
File Edit Setup Control Window Help
FGUM04TM21003029 # config system password-policy
FGUM04TM21003029 (password-policy) # set status enable
FGUM04TM21003029 (password-policy) # set expire-status enable
FGUM04TM21003029 (password-policy) # set expire-day
expire-day Enter an integer value from <1> to <999> (default = <90>).
FGUM04TM21003029 (password-policy) # set expire-day 90
FGUM04TM21003029 (password-policy) # end
FGUM04TM21003029 #
```

- d. Type *exit* to close the session.

4.5. Changing System (Linux) Password (Recommended)

For security purposes, we highly recommend changing the System (Linux) password.

1. To change the system password, perform the following:
 - a. For SSH to iROC FortiGate FW - 192.168.10.10, use username **root** and Password **xxxxxxxx**.
RESULT: Enter the information in the following screen.

Figure 17: SSH Authentication - username root and Password xxxxxxxx

- b. At the prompt, type the following command in the terminal window to change the password. New password length should be over 7 characters. First, perform the change for the root, and then for the admin user.

- c. For Root user:

FOR EXAMPLE: perform the following:

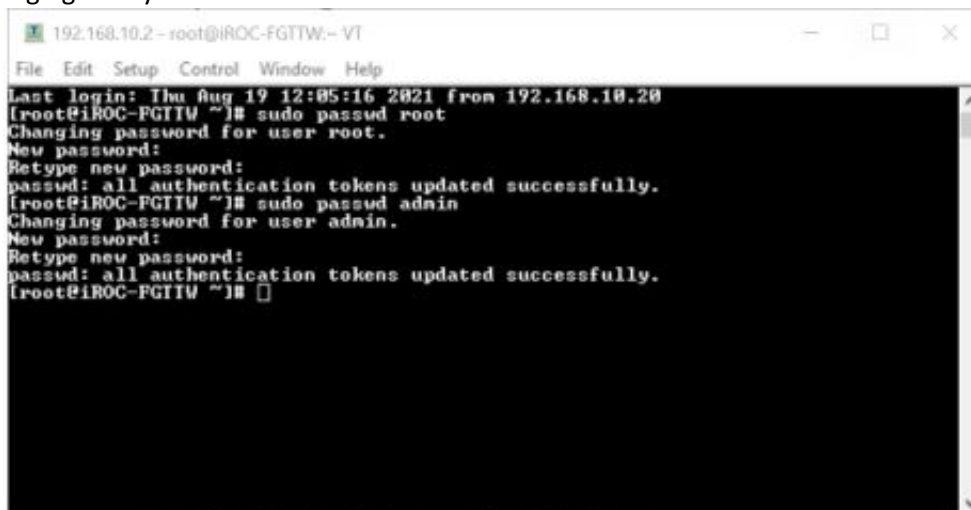
```
[root@iROC-FGTTW ~]# sudo passwd root
Changing password for user root.
New password:
Retype new password:
```

- d. For Admin user:

FOR EXAMPLE: perform the following:

```
[root@iROC-FGTTW ~]# sudo passwd admin
Changing password for user root.
New password:
Retype new password:
```

STEP RESULT: The following screen illustrates the changes.

Figure 18: Changing the System Password

```
192.168.10.2 - root@iROC-FGTTW:~ VT
File Edit Setup Control Window Help
Last login: Thu Aug 19 12:05:16 2021 from 192.168.10.20
[root@iROC-FGTTW ~]# sudo passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@iROC-FGTTW ~]# sudo passwd admin
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@iROC-FGTTW ~]#
```