

Camera access from VPN RUTOS

[Main Page](#) > [General Information](#) > [Configuration Examples](#) > [Camera](#) > **Camera access from VPN RUTOS**



Contents

- [1 Introduction](#)
- [2 Overview](#)
- [3 Step 1: configure VPN](#)
- [4 Step 2: configure the cameras](#)
- [5 Step 3: Configure Port Forwarding](#)
- [6 Step 4: remote access](#)
- [7 Devices used](#)

Introduction

This article is part of a series dedicated to use cases involving RUT routers and **Hikvision** cameras. Here you will find instructions on how to configure a surveillance system that can be managed and controlled remotely via VPN with the help of a single RUT router.

If you're looking for something else that is camera related, you may find the information you need in one of these related articles:

- [Camera access from smartphone](#)
- [Camera access via public IP](#)

Overview

You will need

- a router from the RUT series (except RUT850) or TRB140 and TRB2 series;
- at least one Hikvision IP camera;
- access to or ownership of a VPN network;
- a PoE switch or another type of power supply for the cameras;
- (optional) a Hikvision NVR (Network Video Recorder).

Configuration scheme



Overview

The cameras and the NVR are connected via Ethernet cables to a PoE switch, which is connected to

a RUT router, placing all devices on the same LAN. The RUT router is connected to a VPN making the network reachable to other VPN clients. To reach individual devices in the LAN, Port Forwarding to each device is configured on the RUT.

Step 1: configure VPN

First, we will configure a VPN client on the router. A VPN connection will provide remote access to the router's local network and ensure data security. If your router has a [static public IP address](#), you can access it without the help of a VPN. However, it is not recommended because the absence of a VPN leaves the cameras vulnerable on an unsafe public network with nothing but password protection.

The configuration will depend on the type of VPN that is available to you. You can find various VPN configuration guides [here](#). For this guide, we'll be using OpenVPN ([click here](#) for OpenVPN examples).

Once you set up a VPN connection or if you chose to skip this part and use the router's public IP instead, you can advance on to the next step.

Step 2: configure the cameras

The default IP address for Hikvision cameras is 192.168.1.64. If you plan on using a single camera, you can leave this IP address or change it to whatever suits your needs. But since we'll be configuring 4 cameras and an NVR for this example, we'll need to set up the equipment to have different IP addresses. The setup we'll be using will have the following IPs:



To change the IP address of a Hikvision camera, power it on, connect it to your PC, or an Ethernet port of your RUT router (that is connected to the PC). Type the camera's default IP address (192.168.1.64) into the URL field of your web browser and press "Enter":



If this is the first time that you are connecting to the camera, you will be required to create a user. Just follow the prompts and after you have successfully logged in go to the **Configuration** page (top left corner of the page) and navigate to the **Network → Basic Settings → TCP/IP** section. You can change the IP address from here, by editing the value of the **IPv4 Address** field:



Configure different IP addresses for all cameras that you may be using and advance to the next step.

Step 3: Configure Port Forwarding

Port Forwarding is a way of redirecting an incoming connection to another IP address, port, or the combination of both:



This means you can access multiple LAN devices via a single IP address, but using different ports. Since we have access to the router via its VPN IP (10.0.0.1), we can configure redirects from this IP to the NVR and the IP cameras.

To configure Port Forwarding on a RUT device, go to **Network → Firewall → Port Forwards** and scroll to the bottom of the page. Locate the **Add new instance** section and create a rule to reach the NVR's web interface:



By default, this rule will redirect connections from hosts in WAN connecting to port 81 to the NVR's IP and port 80 (default HTTP port). As discussed [earlier](#), we want to connect via VPN, not WAN; therefore, you will have to edit the rule accordingly. Locate the newly created rule in the list and click the "Edit" button next to it:



Change the Source zone from "wan" to the type of VPN that you are using and save the changes:



You can also create analogous rules for every other camera. Just remember to use different ports and specify actual camera IPs:



Step 4: remote access

To test whether the setup works, open your web browser and try to reach a camera. For example, to reach Camera 1:



If you are redirected to the camera's web interface, congratulations - the setup works!

Important note: viewing camera livestream from web browsers requires a special plugin. Unfortunately, most of the popular web browsers no longer support this plugin.

Devices used

List of devices used in this particular setup:

- **Cameras**
 - Hikvision network camera [DS-2CD2145FWD-I](#)
 - Hikvision network camera [DS-2CD2045FWD-I](#)
 - Hikvision network camera [DS-2CD2345FWD-I](#)
 - Hikvision network camera [DS-2CD2T45FWD-I8](#)
- **NVR**
 - Hikvision network video recorder [DS-7604NI-K1\(B\)](#)
- **Switch**
 - Step 4 Ports PoE+ switch [UTP3-SW04-TP60](#)

- **Router**

- Any type of RUT that has Ethernet ports or TRB140: [RUT230](#), [RUT240](#), [RUT900](#), [RUT950](#), [RUT955](#), [RUTX08](#), [RUTX09](#), [TRB140](#)

NOTE: the instructions should apply to other Hikvision equipment as well.