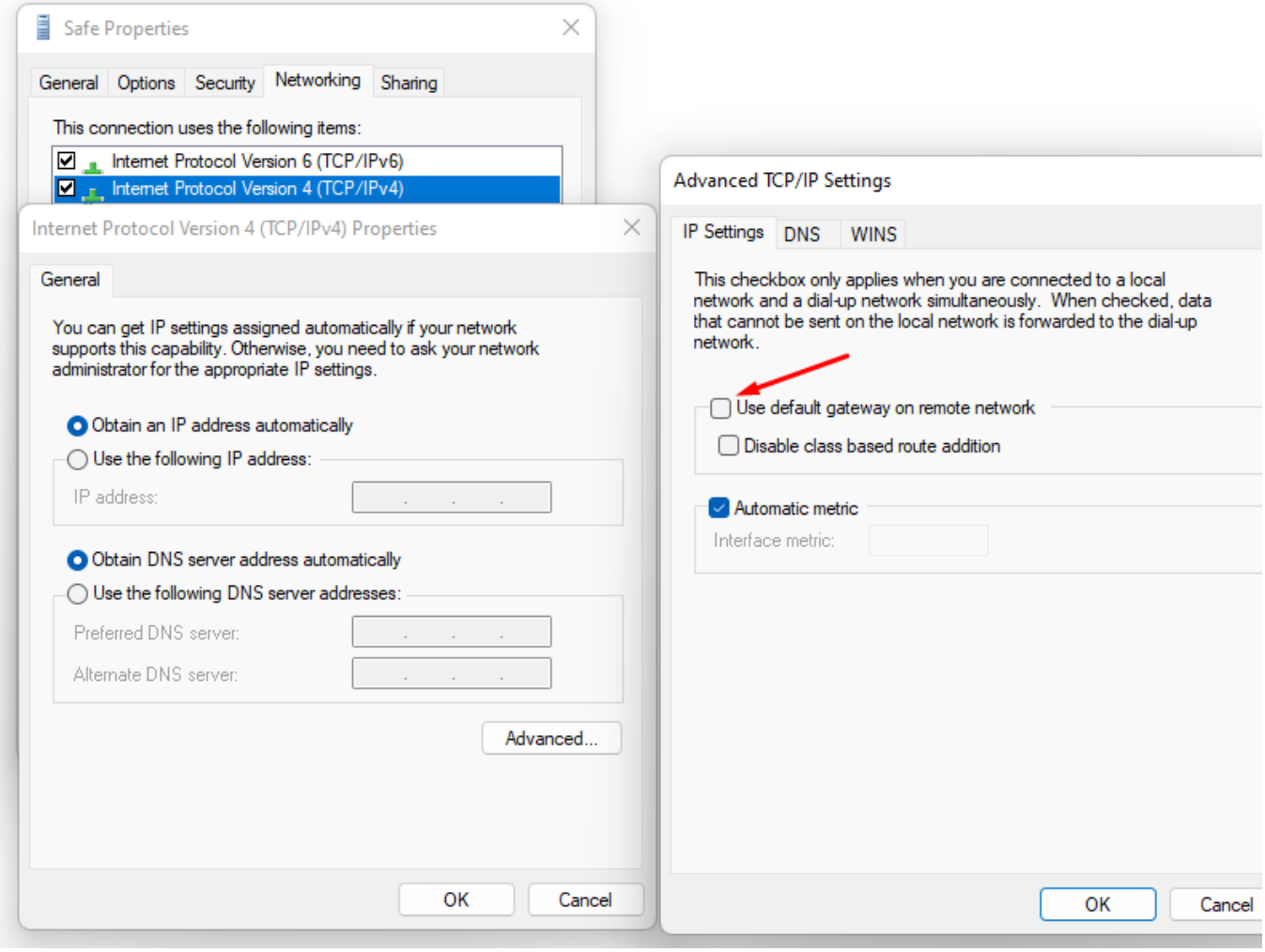
Features of Routing and Access Organization

If VPN is required only to access local network resources

If you need to access the Internet directly through your provider, and you need to use a VPN only to access corporate network resources on computers connected via VPN, you need to configure the following settings.

- In the VPN connection properties, uncheck the box **Use primary gateway on remote network**. Tab **Network -> Internet Protocol version 4 -> Advanced -> IP Settings**.



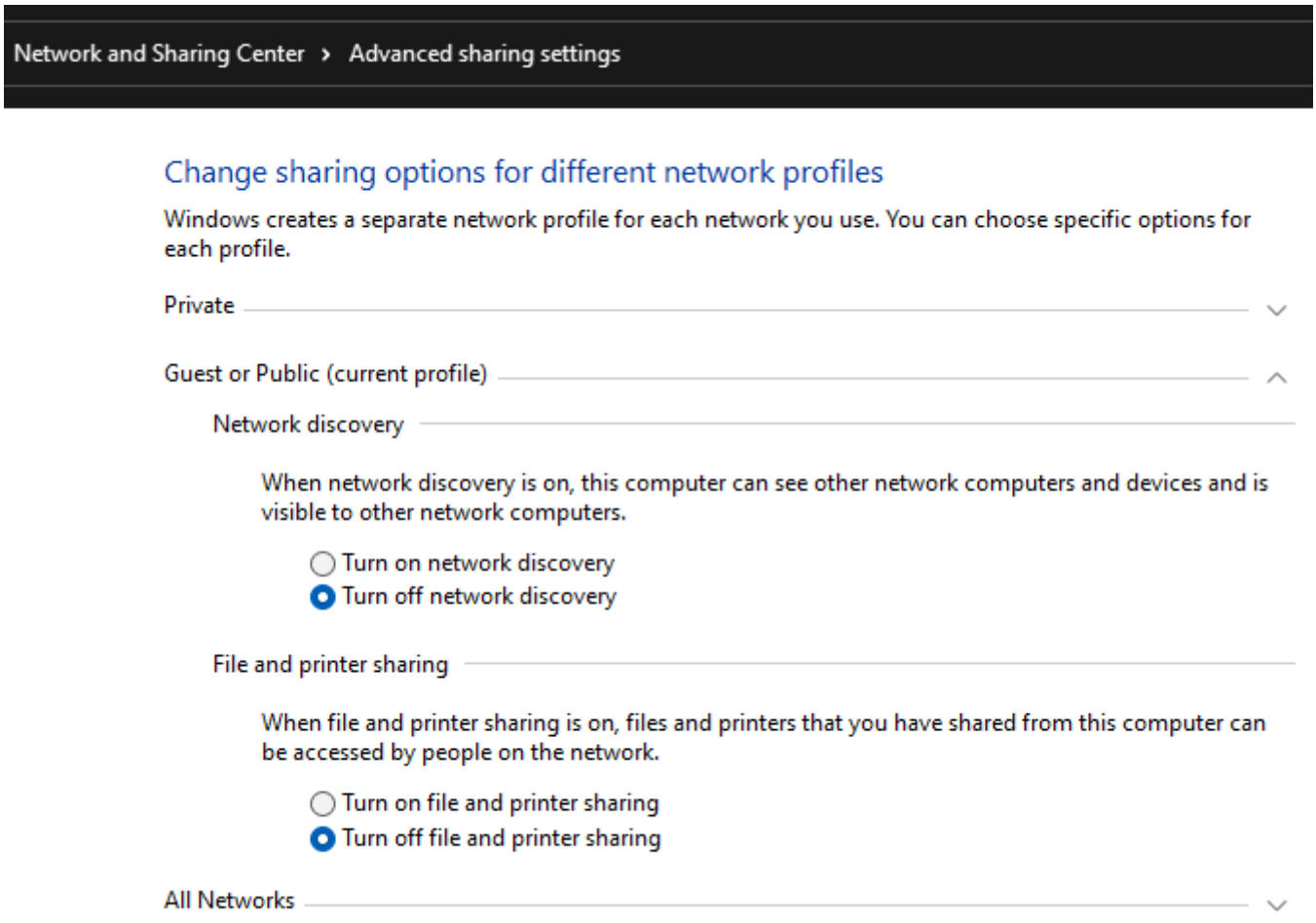
- Create a route to the corporate network (**in Windows 7, 8, 8.1, and 10, a route based on the class will be automatically created, depending on the address that the connection will receive via VPN. For example, a route will be added for the**

10.0.0.0/8 network if the VPN server receives an address from the 10.128.0.0/16 network). For IPsec-IKEv2, you can configure automatic route acquisition.
Route example: if the corporate network is `172.16.0.0/16`, and the network for VPN connections is configured to SafeUTM `10.128.0.0/16` (and the IP address is issued to the VPN connection from the same network), then the route will be: `route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1`

- In some cases, the route may not work, then there is a ping to the protected interface (`10.128.0.1`), but there is no ping to the hosts in the LAN. In this case, when creating a route, you need to specify the number of the VPN connection interface. The final route will be as follows: `route -p add 172.16.0.0 mask 255.255.0.0 10.128.0.1 if nn`
  where **nn** is the number of the VPN connection interface which can be viewed when the VPN connection is active in the output of the route print command in the console section **List of Interfaces**.

If it is not possible to access computers in the local SafeUTM network

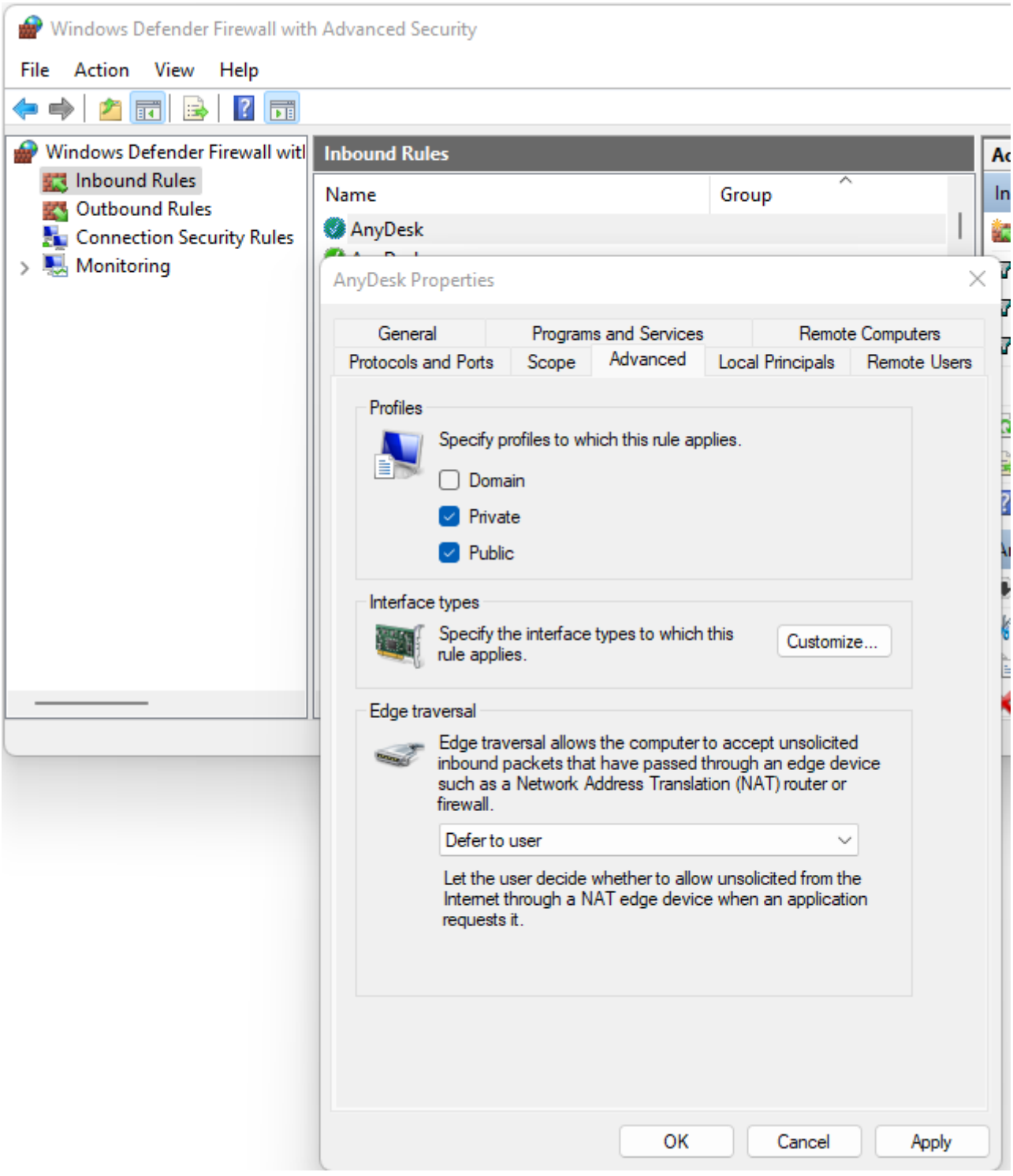
- Make sure that the local network (or the address on the network card) on the remote machine does not intersect with your organization's LAN, if it intersects, then there will be no access to your organization's network (traffic on the routing table will go to the physical interface, and not to VPN). **Addressing must be changed.**
- SafeUTM must be registered as the main gateway on LAN computers. If this is not the case, then you need to register the appropriate route manually on the devices, so that network packets go to SafeUTM for the VPN network.
  Example: `route -p add 10.128.0.0 mask 255.255.0.0 10.1.1.1`
  where `10.128.0.0/16` is the address of the SafeUTM VPN network (configured in **Users -> VPN connections**), and `10.1.1.1` is the IP address of the local SafeUTM interface.
- Check the firewall settings (**FORWARD table**) in SafeUTM for prohibiting rules.
- Computers and servers on Windows OS can restrict access to network folders using network profile settings rules (both on the side of the computer connecting via VPN, and on the side of computers and servers in LAN):



Enable access to files and printers for All Networks and Private Networks profile.

You can do this using PowerShell (launched with rights elevated to the administrator) by running the command:
`Enable-NetFirewallRule -Group "@FirewallAPI.dll,-28502"`

- Windows Defender Firewall may block access to certain programs or services (including RDP) to external networks.
  Check it in the settings of incoming and outgoing connections (you need to allow access from frequent and local networks):



- Antivirus software on the computer may block access to it from non-local networks. Or block access to specific programs.
  For example, for some antiviruses, it is necessary to add a network for VPN connections (10.128.0.0/16 by default) to exceptions.

Created 2022-08-24 21:25:43 UTC by Val Redman
Updated 2022-10-13 14:43:52 UTC by Val Redman