Blocking Specific Ports for UDP/TCP Traffic: FAQ

1. What are UDP and TCP protocols?

UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) are methods computers use to communicate with each other over networks. UDP is faster but less reliable, while TCP ensures reliable data delivery.

2. Why would my internet service provider block specific ports for UDP/TCP traffic?

Internet service providers block certain ports to enhance network security and prevent unauthorized or malicious activities. Blocking these ports helps protect networks and users from potential threats.

3. Which ports are being blocked for UDP/TCP traffic by Tele2 IoT?

Tele2 IoT may block ports commonly associated with fraudulent activities, including:
TCP: Port 25 (SMTP), Ports 135-139 (NetBIOS), Port 445 (SMB), Port 593, Port 12345
UDP: Port 25 (SMTP), Port 135, Port 445 (SMB), Port 593, Port 31337
The list of ports may be updated prior to change.

4. What should the customer do when their internet service provider blocks these ports?

Customers need to configure their devices to use alternative, safe ports for communication.
Set up IPsec (VPN) tunnels for secure data transmission, bypassing blocked ports.

5. How can customers verify if my current solution uses any of the blocked ports?

Check your software documentation. Seek assistance from your IT support team or software vendor if needed.

6. What actions can customers take to ensure my network remains secure despite the blocked ports?

Implement additional security measures such as IPsec (VPN) tunnels or adjust device configurations to use safe ports. Regularly update network security policies to adapt to evolving threats.

7. Will the traffic be blocked for both incoming and outgoing traffic?

No, the traffic will be blocked only for outgoing traffic (traffic from Tele2 IoT devices).

8. What steps should a customer take if they suspect unauthorized activity on their network despite the blocked ports?

Report any suspicious activity to Tele2 IoT technical support for investigation and guidance on mitigating potential threats or breaches.

9. Where can customers find more information about network security best practices and resources?

Explore online cybersecurity forums, industry publications, and reputable IT security organizations for valuable insights on network security best practices and emerging threats.

10. Can customers request not to have ports blocked?

Unfortunately, no. However, customers can utilize an IPsec VPN solution or alternative ports for their connectivity needs.