Router Update – Port Forwarding and Setting Changes to Support TechAlert

TechAlert · https://vettedsecuritysolutions.com/docs/required-ports-for-techalert-remote-monitoring-software/

Overview

To ensure the proper functionality of the TechAlert Remote Monitoring Software for Public Safety, specific network ports must be configured to allow seamless communication between the monitoring agents and the server. This article outlines the necessary ports, their functions, and configuration guidelines to optimize performance and maintain connection stability.

Required Ports

Port 10051 (TCP/UDP)

Purpose: Facilitates data reception by the TechAlert server from remote monitoring agents. It manages the transfer of collected metrics and monitoring data from the endpoints to the central server.

Direction: Inbound to the server

Protocol: TCP/UDP

Port 10050 (TCP/UDP)

Purpose: Used by the TechAlert agents to transmit data to the TechAlert server. It handles the reporting of monitoring statistics and performance data from endpoints such as devices, workstations, and infrastructure to the central server.

Direction: Outbound from the agent to the server

Protocol: TCP/UDP

Port 161 (UDP)

Purpose: Enables SNMP (Simple Network Management Protocol) communication, which is crucial for monitoring network devices like switches, routers, and firewalls. SNMP allows the software to collect network statistics and receive alerts from hardware devices.

Direction: Bidirectional for SNMP traffic (inbound and outbound)

Protocol: UDPFpepwave

Firewall and Network Configuration

To ensure uninterrupted operation of the TechAlert Remote Monitoring Software, firewalls or network security devices should be configured to permit traffic through the following ports:

Inbound Traffic:

Port 10051 (TCP/UDP) on the TechAlert server.

Port 161 (UDP) for SNMP-enabled devices.

Outbound Traffic:

Port 10050 (TCP/UDP) from monitored agents to the server.

Additional Configuration for Specific Devices

For Pepwave: Redirecting LAN HTTP traffic to HTTPS needs to be disabled on LAN only.

- Go to the **Network Tab**.
- Locate **HTTPS redirection settings** under **Advanced** or **Firewall** settings (model dependent).
- Uncheck **HTTPS on LAN** or **Redirect HTTP** to **HTTPS**.
- Apply and Save.

For Sierra: SNMP needs to be enabled on the local network.

- Navigate to the **Security** or **Services Section** under **Administration** or **Advanced.**
- Toggle SNMP to enable.
- Save.

F**or Cradlepoint:** GPS needs to be enabled on the router.

- Navigate to **GPS settings.**
- Enable **GPS** on each CP router encountered.

Conclusion

To ensure a successful deployment of the TechAlert Remote Monitoring Software, confirm that the necessary ports (10051, 10050, and 161) are open and free from restrictions on your network firewall. Proper configuration ensures smooth data flow between your devices and the central monitoring server.

If assistance is required for network or firewall setup, please contact the TechAlert support team.

CONTACT SUPPORT