SOLUTION BRIEF

Eliminate External Attack Surface and Implement Zero Trust with Remote.It

ARM IP

- Cortex-M
- Cortex-A
- Cortex-R
- Security IP
- Software Development Toolkit

OVERVIEW & GOAL

Remote.It provides connectivity while eliminating external attack surface and implementing Zero Trust. Since it doesn't require a public global IP address or port forwarding, private resources stay off the public internet and are not scannable by bots or malicious actors looking for known vulnerabilities or compromised passwords, thereby eliminating external attack surface.

Unlike traditional VPNs that grant access to an entire subnet, Remote.It grants access to services. A database admin can be granted access to a database hosted on a Linux server without being granted secure shell (SSH) access to the server.

APPLICATION AREA

- Industrial
- IoT
- Frameworks & Tools
- Security
- 5G
- Infrastructure
- Cloud Computing

Developers can achieve Zero Trust by implementing least privileged access to services hosted on their Arm-based devices such as Raspberry Pi, Nvidia Jetson, or Arm Virtual Hardware (AVH) devices.

CHALLENGE

Development using public cloud resources can be a security challenge. The only way to access services hosted in a public cloud is to use a public global IP address and port, but even VPNs require a public IP address and port. Additionally, security groups, IP allow lists, route tables, and other network configurations must be constantly maintained to be safe and secure. A simple misconfiguration could lead to a data breach.

VPN solutions also overexpose access rights since users are granted access to subnets. Even if you isolated all your devices into unique subnets and took on managing the configuration challenge, users would still have access to all services on a device. If a Linux sever hosted a web application and a database, an authorized user to the subnet/device could access the web app, database, and SSH to the server. By definition, this is not Zero Trust and least-privileged access.

SOLUTION & BENEFITS

Remote.It eliminates external attack surface by removing resources from public IP address, implements Zero Trust least privileged access, and reduces the possibility for network and security misconfigurations. Developers can now access their AVH devices from any development environment, such as local machine or public cloud, without having to manage IP allow lists, subnet range overlaps, VLAN segregations, public cloud routing tables, and more.

Developers have many options to install Remote.It on devices, such as installing device specific packages, using the one-line install and registration command, or deploying the Remote.It Docker container to their network.

For AVH users, the installation process is even easier. AVH users can install Remote.It during device provisioning. Developers can share individual services such as virtual network computing (VNC), SSH, web applications, databases, and more without complex SSH keys or VPNs and log all access for compliance audits.