IoT International

IoT INTL

On-Demand VPN-RioT Engine Ironclad

Remote VPN to Your Assets

On-Demand and Secure: Turn Off When not Needed

Industrial Applications

Remote Connect to your Industrial Assets, Program and Troubleshoot

No Investment in VPN Appliance

Uses VPN Cloud Meeting Point

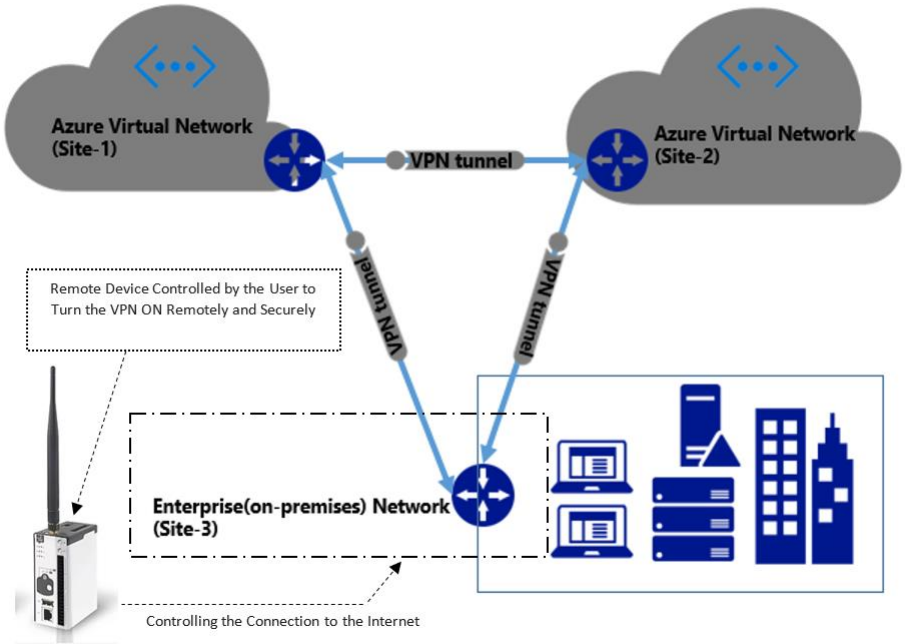
No IT Expertise Needed

Virtual Private Networks are the way businesses can allow access to critical business systems and infrastructure and still maintain the cybersecurity they need in their current businesses and lives. IoT International has implemented a way for small to mid-sized businesses to implement VPN technology without large scale investments in Network Routers and expensive Firewall technology (including saving on the programming and implementation of these devices). IoT international presents Ironclad.

There are two pieces to our solutions:

1. A small computer equipped with mini port technology and connected to your company's network behind any firewalls
2. A VPN subscription provided by IoT International and hosted in Microsoft Azure.

Once Ironclad is powered up, it establishes a VPN to your network and will allow remote workers to provide their network credentials and connect to Company systems and assets from home using their home Wi-Fi connection.



IoT International

IoT INTL

Advanced Security Technologies to Control the VPN Connection

Analytics and Notifications

Receive Notifications and Generate Analytics Based on Connections and Connection Attempts

Two-Factor-Authentication

SMS Codes to Users' Mobile Devices to Authenticate the Users Initiating the VPN Connections

Secure API's

Secure API's to Access Platform Data and Analytics

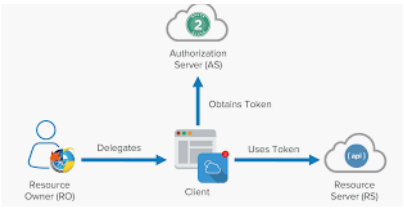
Role and Responsibility: Role Based security in accessing platform resources is implemented. Users can trace the history of access attempts, errors, receive notifications based on connection attempts, etc. In addition, by allocating the users to different roles, system messages and notifications can be routed to the right people. Three level of access:

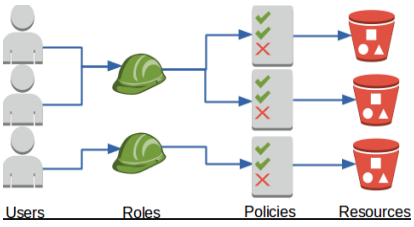
- Manager: Manger has access to the account level resources such as adding or removing an account. In addition, the Manager can add or remove the Admin users
- Admin: Admin users can add, modify or remove system artifacts and resources such as device connections, charts, reports, etc. They can add, remove or modify regular users.
- Regular User: Regular users can only view the artifacts developed and added by Amin users. We can also allocate the users to different groups to filter the notifications they receive.

Data Integrity: It is paramount to be able to trust the data before relying on it. The Timeseries platform provides a long security key that is used by the Engine when it pushes data to the platform. If the key does not match with the information saved at the service, the data is not accepted by the platform.

User Authentication: It is important to make sure only authorized uses have access to the data. The system provides two-factor-authentication to authenticate the users. If the user opts in, they receive a SMS with a code any time they try to log in. Only after successfully entering the code they can log in the system. OAuth Authorization Framework is used to authenticate the user to the platform. Using OAuth, users are granted limited access to the system without exposing their credentials. OAuth is a token-based system i.e. the user asks for an Access Token from an Authorization Server.

sent to the cloud platforms unidirectionally. Any control command is to be initiated and executed on the premise. rIoT platform is a perfect fit for this situation, as the edge gateways need to have only an outbound port connection. In traditional systems that the data is concentrated on the premise, it is a huge challenge to secure the incoming connections to query the data and keep track of all the security patches and updates.





IoT INTL

IoT International
(443) 718-0240
10015 Old Columbia Rd
Suite B-215
Columbia, MD 21046
www.iotintl.net