Strengthening IIOT Cybersecurity through SSH and VPN integration

Detailed Work Plan from 12th March-2024 to 30th May-2024

Phase 1: Preparation (March 12th - March 25th)

Project Kick-off and AWS Account Setup:

- Hold a kick-off meeting to introduce team members, define objectives, and set expectations.
- Set up an AWS account and configure IAM roles for team members with appropriate permissions.

Requirement Gathering and Analysis:

- Gather requirements for SSH and VPN integration, including the need for a physical router to establish VPN connections between AWS and on-premises networks.
- Risk Assessment and Compliance:
- Perform a risk assessment considering physical router deployment, ensuring compliance with security standards and regulations.

Resource Allocation and Budget Planning:

- Allocate resources and budget for the physical router procurement, installation, and configuration.

Phase 2: Planning (March 26th - April 8th)

Solution Design and Router Selection:

- Design the architecture for integrating the physical router with AWS VPCs for VPN connectivity.

- Select a physical router model that supports VPN protocols compatible with AWS VPN services.

Procurement:

- Procure the selected physical router model from a trusted vendor or supplier.

Timeline and Milestone Definition:

- Define a timeline with milestones for each phase of the project, considering router procurement, installation, and configuration.

Phase 3: Implementation (April 9th - May 10th)

Physical Router Installation:

- Install the physical router in the on-premises network infrastructure, ensuring compatibility and proper placement for VPN connectivity with AWS.

Router Configuration:

- Configure the physical router to establish VPN connections with AWS VPN services, including setting up VPN parameters, encryption settings, and authentication methods.
- Configure routing policies on the router to direct traffic between on-premises networks and AWS VPCs through the VPN tunnel.

Integration with AWS:

- Configure AWS VPN services (e.g., AWS VPN Gateway) to establish VPN connections with the physical router.
- Verify VPN connectivity and traffic routing between the physical router and AWS VPCs.

Phase 4: Optimization and Documentation (May 11th - May 24th)

Performance Optimization:

- Optimize router configurations for performance and reliability, adjusting VPN parameters and encryption settings as needed.
- Monitor router performance metrics to ensure efficient use of resources and minimal latency.

Security Hardening:

- Implement security measures on the physical router, such as access control lists (ACLs), firewall rules, and intrusion prevention systems (IPS), to protect against potential threats.

Documentation:

- Document the physical router configuration details, including VPN settings, routing policies, and security configurations.
- Create operational documentation for router management, maintenance, and troubleshooting procedures.

Phase 5: Deployment and Training (May 25th - May 30th)

Deployment:

- Deploy the configured physical router into production on-premises environments.
- Test VPN connectivity and traffic routing between on-premises networks and AWS VPCs, ensuring proper functionality.

Training:

- Provide training sessions for network administrators on managing and maintaining the physical router, including VPN configuration, monitoring, and troubleshooting.