In the following proposed system model, the connectivity with the prototype network have been demonstrated for the business. Within the network, there will be security and policy infrastructure, in which the deployment of active directory and CA can be done to authenticate individuals before accessing the systems. However, some off-premises gateways should be established like ASA etc. that filters all incoming packets and granting access to TechSolutions Inc. architecture. Wireless and wireless connections can be established, but for this a WLAN controller has been established, which checks every entry and grant permissions to access systems.

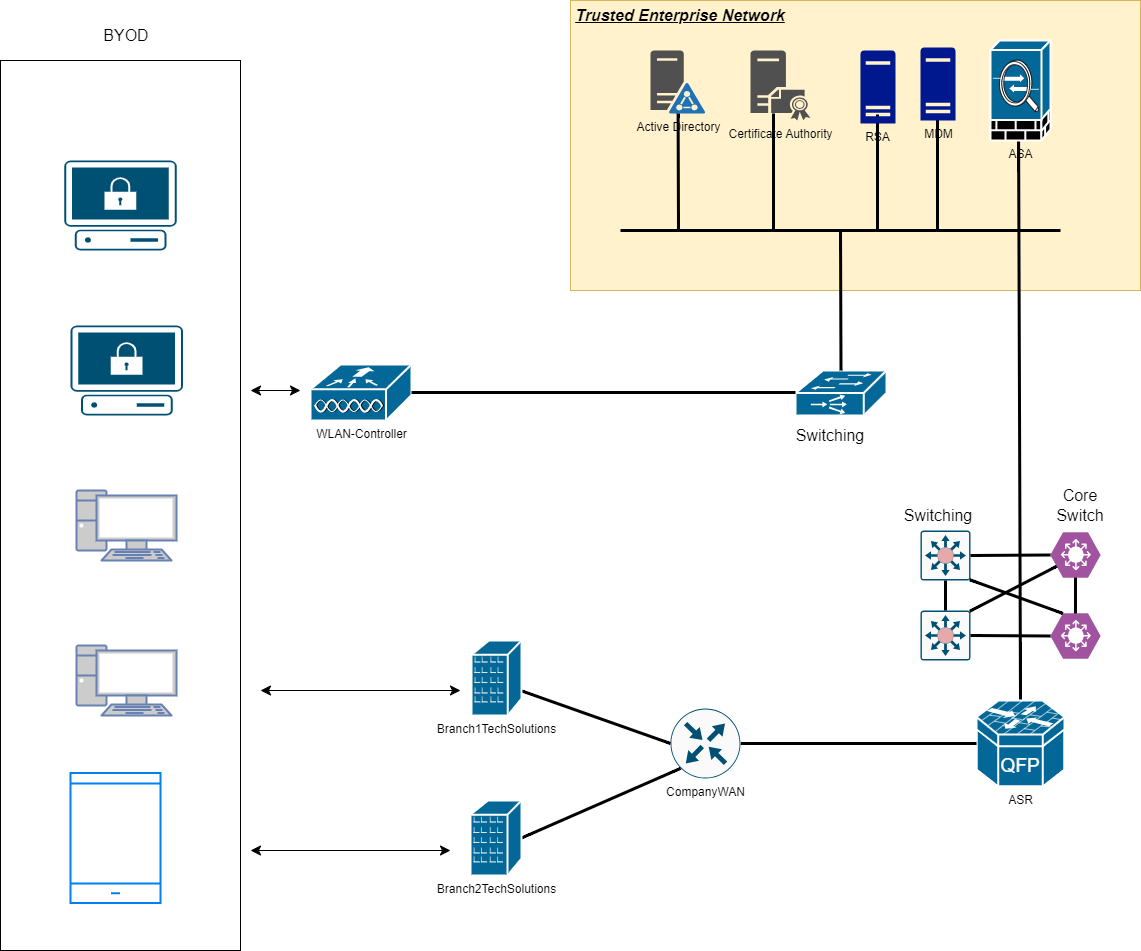


Figure : Proposed network architecture (self-drawn)

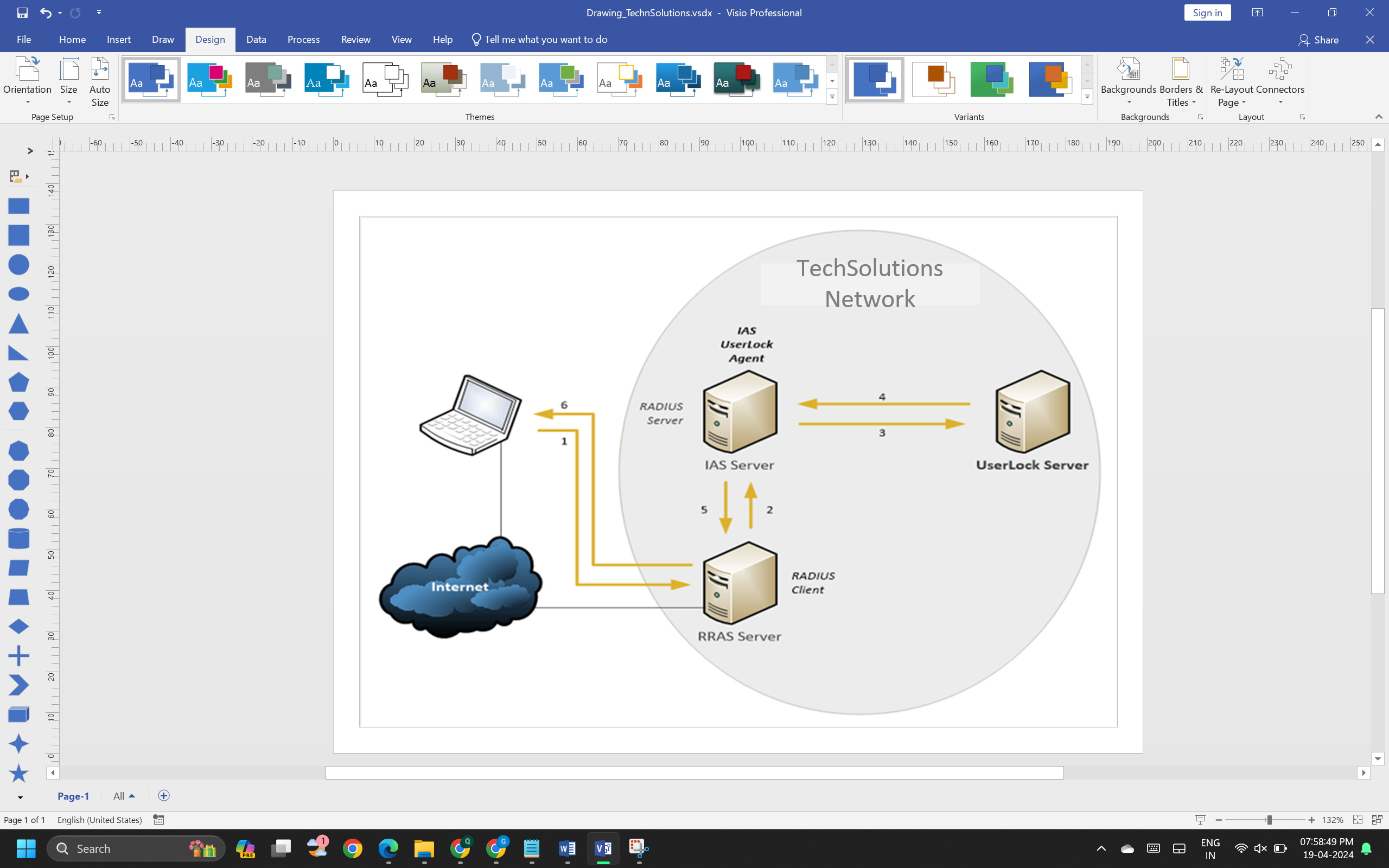
In the above proposed diagram, the numerous controls have been established, which can be crucial for infrastructure to secure their environment. The following are components, which have been used for the proposed systems:

1. ASA

In terms of BYOD, the deployment of this appliance helps to allow authorized devices and users to access corporate resources while handling and mitigating potential security threats.

1. MDM: - Mobile device management

MDM solutions are also essential in order to enforce BYOD policies, and helps to manage numerous devices connecting to corporate network. Along with this, the mobile device management enables IT administrator to remote manage devices, and enforcing security policies. The integration helps into BYOD policies as organizations are able to ensure consistent security and compliance across BYOD devices.



Similarly, RSA secureID has been providing strong authentication and access mechanism, which helps to secure environments. Active directory will be providing a central directory service, which helps to manage user identities, access controls, and group policies within the network of organizations.

In order to leverage BYOD policies into the environment of TechSolutions Inc. the following steps could be followed in the design approach. In the first step, the policy configuration will be performed, in which set of guidelines mentioned, and establishing group restrictions for the different individuals. Along with this, the deployment of appropriate data security methods could be done onto the systems, and employing BYOD to allow end employees to perform actions. In the same solution, the devices should be regularly check to identify, which devices have issue, and must be replaced. There should be IT Department approval for personal devices before granting accessibility to the resources.