|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Arwa AlQadheeb |
| Date: | Sunday, October 16, 2022 |

|  |
| --- |
| Overview |
| The OpenVPN Access Server software solution provides a virtual private network (VPN) that implements techniques to create secure a point-to-point connection (i.e., encrypted VPN tunnel) across the public internet which will allow COMPANY\_A’s employees to access the company’s resources remotely using OpenVPN Protocol and ensure that sensitive data is safely transmitted between COMPANY\_A’s on-premises datacenter and employees’ computing devices at homes.  The software solution comes with integrated certificate management, internal and external authentication systems, and bundled client software (i.e., OpenVPN Connect).  Deployment Checklist:   1. Installing Access Server on on-premises hardware. 2. Setting up the server. 3. Setting up employees’ computing devices. |
| Hardware & Software Requirements, Possible Integrations |
| Software requirements:   * Operating System: Linux 64-bit, CentOS7   (Recommended to install via repository)  Hardware requirements:   * Processor: 4 Core, 3GHz  (Support AES-NI). * Memory: minimum of 1GB. * Bandwidth: 10Mbps (Per user). * Hard Disk: 16GB.   Possible Integration:   * Configure OpenVPN Access Server to authenticate users using their LDAP username and password credentials. |
| Additional Administrative Considerations |
| 1. Enable port forwarding feature on COMPANY\_A router to allow forwarding inbound traffic coming on specific ports (i.e., TCP 443, TCP 943, and UDP 1194) to private IP address of OpenVPN Access server. 2. On internal firewall, allow inbound traffic coming from OpenVPN Private IP address. 3. OpenVPN Access Server checks username against LDAP directory to verify password in order to grant access with appropriate permission to COMPANY\_A private network. |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Arwa AlQadheeb |
| Date: | Sunday, October 16, 2022 |

|  |
| --- |
| Overview |
| Duo two-factor authentication is the perfect solution that adds additional layer of security to COMPANY\_A’s information system. In simple words, the concept of two-factor authentication is verifying employees’ identities by requesting two pieces of evidence (i.e., something they know such as username and password, something they have such as cellphone, or something they are fingerprint). In our situation, we can implement Duo solution in cooperation with our existing OpenVPN Access Server service and authenticate users using their username and password credentials + Timed One-Time Password (OTP) received on mobile devices.  Deployment Checklist:   1. Integrating Duo two-factor authentication into OpenVPN Access Server. 2. Configuring the server. 3. Setting up employees’ computing devices. |
| Hardware & Software Requirements, Possible Integrations |
| Software requirements:   * Mobile Device: Apple iOS 13 and higher, and Android 8.0 and higher. * OpenVPN Access Server: duo\_openvpn\_as package. * OpenVPN Client Connect 2.2 and higher.   Hardware requirements:   * Any mobile device (Support Apple iOS or Android)   Possible Integration:   * Configure OpenVPN Access Server to authenticate users using their LDAP username and password credentials and Duo two-factor authentication. |
| Additional Administrative Considerations |
| 1. Add Duo two-factor authentication as protected application to OpenVPN Access server using integration key, secret key, and API key. 2. Install external firewall to allow OpenVPN Access Server established connection to Duo Security over TCP 443 and block all incoming traffic. |