|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Mohammed Alnajrani |
| Date: | 8/24/2023 |

|  |
| --- |
| Overview |
| A virtual private network (VPN), tunnel program that will provide an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. We will use OpenVPN to handling client-server communications, it utilize OpenSSL and UDP or TCP protocol to communicate the data, but the most common protocol used by OpenVPN is UDP  Deployment checklist   1. We will click on get started button then choose the compatible deployment platform 2. Setting up OpenVPN Access Server 3. We will configure VPN 4. Lastly add users to VPN |
| Hardware & Software Requirements, Possible Integrations |
| *Software requirements*   1. A Linux operating system that supports OpenVPN. 2. A Non static-compiled kernel.   Hardware requirements   1. CPU support AES-NI 2. At least, 1GB of memory 3. At least, 16GB of disk space should be free   Possible Integrations   1. LDAP 2. RADIUS |
| Additional Administrative Considerations |
| 1. Configuring VPN Routing settings according to the company’s needs. 2. Configure the server with the IP address interface and company's domain name desire 3. firewall must be configured to forward client traffic between the public IP address and the server's private IP address. |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Mohammed Alnajrani |
| Date: | 8/24/2023 |

|  |
| --- |
| Overview |
| *(describe how the service works and provide a basic deployment checklist)*  Duo provide two-factor Authentication (2FA) which adds an extra layer of security to your identity. Duo 2FA will verify your identity by using something you know such as your username and password with something you have such as mobile phone, text message, landline phone to verify your identity and prevents anyone but you from logging in even if they know your password.  *Deployment checklist*   1. *sign up account for Duo* 2. *download and install the Duo* Two-Factor Authentication 3. *Click Protect an Application* 4. *and get your integration key, secret key, and API hostname* 5. *Run the Duo Authentication then enter your API Hostname and click next* 6. *Configure proxy for Duo traffic option and specify the proxy server's hostname or IP address* 7. *Enter your integration key and secret key then click next* 8. Select your integration options: 9. *Test Your Setup by attempt to log in to your newly-configured system as a user enrolled in Duo* |
| Hardware & Software Requirements, Possible Integrations |
| *(describe the components of the solution)*  ***Hardware requirements***   1. *2 cores CPU* 2. *200 MB disk space* 3. *4 GB RAM (although 1 GB RAM is usually sufficient)*   ***Software requirements***   1. *Windows Server 2012 or later (Server 2016+ recommended)* 2. *CentOS 7* 3. *Fedora 37 or later* 4. *Red Hat Enterprise Linux 7 or later* 5. *Ubuntu 20.04 LTS or later* 6. *Debian 11 or later*   **Possible Integrations**   1. *LDAP* 2. *RADIUS server* 3. *OpenVPN* 4. *WordPress* |
| Additional Administrative Considerations |
| 1. Regularly review your list of administrators to ensure that the people listed are still employed in that capacity, and remove or add administrators as appropriate. 2. Duo recommends to have at least two owners for any given account to maintain Duo Admin Panel access and functionality, prevent time-consuming account lockouts, and maintain security audit compliance 3. After administrators have set up their accounts, ensure they’re able to log into the Duo Admin Panel successfully using all authentication methods that you allow. |