|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Haneen Alamoudi |
| Date: | 10-11-2022 |

|  |
| --- |
| Overview |
| *(describe how the service works and provide a basic deployment checklist)*  *Virtual private network (VPN) tunnel program that would be secure, free, fast, and work on standard TCP and UDP protocols across the internet. A virtual network is created through OpenVPN to connects computers over existing networks securely by encrypting all of the data in transit. A tunnel is used in the public network to transmit data thus no one can intercept the data in the tunnel.*  *OpenVPN can be used to establish multiple functions:*   * *Secure Remote Access* * *Site-to-site connections to bring networks together* * *Multiple networks, subnets, gateways, and servers* * *Secure Internet traffic or contact limited-access systems*   *Deployment Checklist*   1. Choosing the Platform (a server on-premise, with a virtual machine, or through a cloud service provider) 2. Setting up OpenVPN Access Server (A supported Linux operating system, and Root privileges) 3. Obtain Admin Web UI login details 4. Configure the VPN through Admin Web UI  * Add hostname * VPN Settings including VPN IP Network, Routing and NAT, Split Tunneling, DNS Settings.  1. Adding users to OpenVPN Access server through the use of LDAP |
| Hardware & Software Requirements, Possible Integrations |
| *Hardware Requirements:*  *A VPN will be used to redirects all internet traffic which utilizes processing capacity for encrypting and decrypting on both the client and the server side. The following requirements are needed:*   1. *CPUs support AES-NI to speed up AES processing.* 2. *Memory: 2GB* 3. *Hard Disk: 16GB* |
| Additional Administrative Considerations |
| *(describe any other security management activities, e.g. do we need to change firewall rules?)*   1. *Disable SELinux and reboot the system.* 2. *Configure the server with the interface IP address(es) and domain name desire.* 3. *If the openVPN access server is installed on a private network behind a corporate firewall, the firewall must be configured to forward client traffic between the public IP address and the server's private IP address.*   *Needed Ports:*   |  |  |  | | --- | --- | --- | | **Service** | **Protocol** | **Default Ports** | | OpenVPN daemons | UDP | 1194 | | OpenVPN daemons | TCP | 443 (shared) | | Web services | TCP | 443 (shared) | | Web services | TCP | 943 | | Clustering API | TCP | 945 | |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Haneen Alamoudi |
| Date: | 10-17-2022 |

|  |
| --- |
| Overview |
| *(describe how the service works and provide a basic deployment checklist)*  *Duo provide a two-facture authentication service that could be implemented into a vast range of applications and services including VPN, email, web portal, cloud services. Through the use of Duo Mobile application, user can provide a secondary authentication by answering a call, a one-time passcode generated by the Duo Mobile app, a compatible hardware token, or received via SMS.*  *Duo can be integrated using LDAP, RADIUS, Wordpress, CISCO, OpenVPN, iPassword, AWS, and slack.*  *To integrate Duo in our company network, we will use LDAP.*   1. *Sign up for a Duo account.* 2. *Log in to the Duo Admin Panel and navigate to Applications.* 3. *Click Protect an Application and locate LDAP Proxy in the applications list. Click Protect to get your integration key, secret key, and API hostname.* 4. *Install the Duo Authentication Proxy* 5. *Configure the Proxy* 6. *Configure the Proxy for Your Primary Authenticator* 7. *Configure the Proxy as an LDAP Server* 8. *Start the Proxy* 9. *Configure LDAP Clients* 10. *Test the Setup* |
| Hardware & Software Requirements, Possible Integrations |
| *(describe the components of the solution)*  The Duo Authentication Proxy installation supports these operating systems:   * Windows Server 2012 or later (Server 2016 or 2019 recommended) * CentOS 7 or later * Red Hat Enterprise Linux 7 or later * Ubuntu 16.04 or later * Debian 7 or later.   Vendor recommenda a system with at least 1 CPU, 200 MB disk space, and 4 GB RAM (although 1 GB RAM is usually sufficient) |
| Additional Administrative Considerations |
| *(describe any other security management activities, e.g. do we need to change firewall rules?)*  *This application communicates with Duo's service on TCP port 443. Firewall configurations that restrict outbound access to Duo's service with rules using destination IP addresses or IP address ranges aren't recommended, since these may change over time to maintain our service's high availability.* |