|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Marvellous Onuma-Kalu |
| Date: | 01/08/2024 |

|  |
| --- |
| **Overview** |
| A VPN (Virtual Private Network) is an important concept of end-to-end protected network communication, whereby communication is sent over an untrusted network infrastructure such as the internet. It protects confidentiality and integrity of data in transit.  Advantages: VPN connects easily and cheaply to the internet, encrypts traffic over the internet, has a lot more bandwidth, creates two internet connection points, they are ideal for file transfers, email and so on.  Disadvantages: VPNs are not ideal for financial, medical and other real-time operations. They don’t get dedicated bandwidth across the internet.  **How it works**:   * The user first connects to the internet and then initiates a VPN connection: a locally installed client software (or web browser) to the VPN server located in the office. * The VPN server based on your access level permission grants you access to internal company resources via the secure tunnel; thus, keeping data secure and private over the internet.   There are two types of VPNs to consider: Client-to-site (transport - provide a remote access from a remote client such as traveling sale rep to the corporate network) and site-to-site (tunnel - provides connectivity to networks, such as headquarters and a remote office). These fall under the category Remote-access VPNs which we will install in this exercise.  **What we need**: We will need a VPN access server and VPN client software. The two most used technologies in remote access VPNs are IPsec and SSL VPN. In this example we will use OpenVPN (SSL). OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. |
| **Hardware & Software Requirements, Possible Integrations** |
| OpenVPN Access Server does not create or manage its own dedicated user database. Instead, it integrates with a user authentication database system. The currently supported system is Active Directory/LDAP Server which we have already installed on-premises. OpenVPN server supports multiple authentication protocols and thus can be configured to obtain connecting client information from an LDAP server, and to use that information as a basis for authenticating the client in addition to the use of the Client certificates and keys.  **Requirements**  Hardware: VPN Access Server (Linux machine)  Software:  On Client side: OpenVPN Connect for Windows and for Mac (design department)  On Server side:: OpenVPN Access Server source code  Pricing: Access Server subscription / 5, 10 - 2000 users / month $70 |
| Additional Administrative Considerations |
| Firewall:   * A firewall is a tool used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks — and are often used to prevent unauthorized web users or illicit software from gaining access to private networks connected to the internet. While disabling a firewall would put the entire network at risk, it is recommended to turn off a firewall altogether, you can open the appropriate (non-standard) ports in the firewall to allow authorized applications or services through. Some firewalls use a pre-defined port or range of ports, while others allow users to manually configure which ports the software utilizes. * Enterprise VPN Access Server, provides Layer 3 virtual private networking using OpenVPN protocol. OpenVPN protocol uses SSL/TLS with client and server certificates to perform key exchange and mutual authentication. |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Marvellous Onuma-Kalu |
| Date: | 01/08/2024 |

|  |
| --- |
| **Overview** |
| Duo Security is a popular multi-factor authentication (MFA) solution that provides an additional layer of security for various applications, including VPNs like OpenVPN. Integrating Duo 2-Factor Authentication (Duo 2FA) with OpenVPN adds an extra layer of protection by requiring users to verify their identity using a second authentication factor in addition to their username and password.  **Prerequisite:** Here's a general guide on integrating Duo 2FA with OpenVPN:  **How it works**: With Duo2F the user may log in as usual with his/her username and password and will then receive a push message on the user’s device where he/she can verify that it is him/her. The administrator can set up the system to work via SMS, voice call, one-time passcode, the Duo Mobile smartphone app etc. If you have a hardware token, you can press its button to generate a passcode. You can also use a Security Key (including U2F tokens). |
| **Hardware & Software Requirements, Possible Integrations** |
| Hardware: Hardware token or security key  Software: Duo2F account, Duo2F for mobile, Duo OpenVPN v2.4 plugin and Duo2F Wordpress plugin  **Duo 2 Factor Authentication setup:**   * Enrollment and setup accounts * Install Duo mobile apps. * Activate Duo Mobile * Install and setup Duo2F for OpenVPN (Ensure that Python 3 or 2.7 is installed on server) * Install and setup WordPress plugin * Please view Duo2F Network Diagram WorkBook.jpg to visualize this. |
| **Additional Administrative Considerations** |
| Configure OpenVPN to use the Duo Authentication Proxy for secondary authentication. This typically involves modifying the OpenVPN server configuration file to include the Duo integration settings.  Duo only integrates with OpenVPN servers that employ certificate authentication and use a unique common name (CN) in each user's cert. Support for OpenVPN deployments with password authentication may be supported in the future. |