|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Simone Canty |
| Date: | 06/14/2022 |

|  |
| --- |
| Overview |
| *(describe how the service works and provide a basic deployment checklist)*  **OpenVPN Access Server works by:**   * OpenVPN Access Server installs on a Linux operating system * VPN clients connect from [Microsoft Windows](https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-windows/), [macOS](https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-macos/), [iOS](https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-apple-ios/), [Android](https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-android/), and [Linux](https://openvpn.net/cloud-docs/openvpn-3-client-for-linux/) systems.. * User authentication includes a built-in system with web-based management or external authentication with PAM, LDAP, or RADIUS. * Advanced authentication is supported through custom programming with Python * Access Server includes built-in, fully automated VPN certificate management and provisioning. External PKI is also possible for full control over an existing integrated PKI. * VPN tunnels are secured with the OpenVPN protocol using TLS authentication, credentials, certificates, and MAC address lock (optional). * Multi-factor authentication is supported in various forms: Google Authenticator is built-in; Duo Security can be added with a post\_auth plugin; and LastPass can be added with a post\_auth plugin. * Access Control rules can specify user or group access to IP address and subnets and allow or disallow direct VPN client connections. * Full-tunnel and split-tunnel redirection: All VPN client internet traffic goes through the VPN tunnel, or only specified traffic, respectively. * Professional support provided by the OpenVPN Inc team, with our online support ticket system staffed by our global team of professionals.   **Basic Deployment Checklist:**   * Linux Operating System * Admin Web User Interface * Client Web User Interface * Users * User Credentials * Connection Profile * Multi-factor Authentication (MFA) * OpenVPN Connect * OpenVPN Server * Default Ports and Services |
| Hardware & Software Requirements, Possible Integrations |
| *(describe the components of the solution)*  **Hardware Requirements:**   * **Processor**: Central Processing Unit (CPU) with Advanced Encryption Standard New Instructions (AES-NI) chipset. CPU chipset with AES-NI will need approximately 12MHz for each megabit per second (Mbps) transferred in one direction. * **Memory:** Memory requirements are dependent on the number of connected devices and the level of NAT traffic your VPN server needs to process. At a minimum, you must start with 1GB of memory, and add approximately 1GB for each 150 connected devices**.** * **Bandwidth:** Bandwidth requirements are completely dependent on how much total data you want to route through your VPN tunnels. * **Hard Disk:** The only data that are necessary to store on disk are connection and program logs, and user certificates and settings. You need 16GB of disk space.   **Software Requirements:**   * There are no software requirements. * Works on any 64-bit Linux operating system such as Ubuntu, Debian, Red Hat Enterprise Linux, CentOs, and Amazon Linux 2.   **Possible Integrations:**   * Integrate OpenVPN Access Server with LDAP. |
| Additional Administrative Considerations |
| *(describe any other security management activities, e.g. do we need to change firewall rules?)*  A firewall will still be used. VPN along with a firewall can create a more well-rounded secure network. The OpenVPN will set to require LDAP. Therefore, the firewall rule will need to be changed to allow for access to Port 339. |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Simone Canty |
| Date: | 06/27/2022 |

|  |
| --- |
| Overview |
| *(describe how the service works and provide a basic deployment checklist)*  Duo 2FA works by:   * Providing two-factor authentication which adds a second layer to your online accounts. Verifying your identity using a second factor like a phone or mobile device, prevents anyone but you from logging in, even if they know your password.   How it works:   * Once you are enrolled in the software, you are ready to go. * You log into Duo, using your username and password, and use your device for verification. * The system administrator can set up the system via secure messaging system (SMS), voice call, one-time passcode, the Duo Mobile smartphone app, and etc. * If no mobile phone, you can use a landline or tablet, or ask the system administrator for a hardware token. * Duo lets you link multiple devices to your account, so you can use a mobile phone and a landline, landline and a hardware token, etc.   Basic Deployment Checklist:   * Choose Your Authentication Device Type * Enter Your Phone Number * Choose Platform: Android or iOS * Install Duo Mobile * Activate Duo Mobile * Configure Device Options * Duo Web SDK (software development kit) v2 or v4 |
| Hardware & Software Requirements, Possible Integrations |
| *(describe the components of the solution)*  **Hardware:**  Mobile Device: mobile phone  Landline or tablet  Hardware Token  **Software:**  Duo Mobile  Android: current version of Duo Mobile supports Android 7.0 or greater  iPhone: current version of Duo Mobile supports iOS 11.0 and greater.  Duo Web SDK  **Possible Intergrations:**  OpenVPN Access Server  WordPress Plugin |
| Additional Administrative Considerations |
| *(describe any other security management activities, e.g. do we need to change firewall rules?)*  Yes, it will go through a firewall and the rules will need to add/change. |