|  |  |
| --- | --- |
| Project Name: | OpenVPN Implementation |
| Prepared by: | Mohammad Alsowaini |
| Date: | 04/10/2022 |

|  |
| --- |
| Overview |
| Access Server presents the administrator with the most useful configurations of the many options supported by the sophisticated OpenVPN server and clients. An easy-to-use, Web-based configuration interface makes setting up and maintaining the Access Server deployment straight-forward and efficient. |
| Hardware & Software Requirements, Possible Integrations |
| **Hardware Requirements**  Almost all modern CPUs support AES-NI to speed up AES processing. Access Server automatically uses AES-NI for the default AES-256 encryption.  Memory requirements depend 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 requirements depend entirely on how much total data you want to route through your VPN tunnels. If you have a server with a 1Gbps network connection, and you have 100 connections, that means 10Mbps per user.  **Possible Integrations:**  LDAP allows you to configure authentication for LDAP. LDAP requires the most settings to configure and requires the most specialization in which you must have some basic knowledge of the LDAP syntax. The company already have a LDAP server. |
| Additional Administrative Considerations |
| *OpenVPN Access Server uses iptables to manage access control rules. It sends instructions to OpenVPN clients to send specific traffic through the VPN server and also functions as a firewall that prevents OpenVPN clients from trying to access more than what is allowed.* |

|  |  |
| --- | --- |
| Project: | Duo 2FA Implementation |
| Prepared by: | Mohammad Alsowaini |
| Date: |  |

|  |
| --- |
| Overview |
| *Progress steps:*   1. Success Planning  * Administration Overview * Determine Duo Enrollment Methods  1. Application Configuration & Testing  * Identify Applications * Configure Applications * Test Your Duo Applications  1. Policy & Control  * Customize User Access with Duo Policies * Deploy and Test Duo Device Health Application Overview * Configure and Test Trusted Endpoints Overview  1. End-user Communication  * Build End User Communication Materials  1. Help Desk Training  * Enable Your Help Desk Team * Overview of Duo Support  1. Duo Go-live   Duo Go-live Checklist:   * Internally market the deployment of Duo: * Post Duo announcements on intranet or employee community webpage. * Include Duo in company events or presentations. * Display Duo posters at all company locations - common & lunch areas work best. * Confirm Help Desk readiness and the Help Desk team’s Duo escalation plan. * Notify your organization (end-users, help desk, and IT admins) via email that Duo is going live with effective dates. |
| Hardware & Software Requirements, Possible Integrations |
| *Software and hardware requirements:*   * *A Duo Access or Duo Beyond plan in order to set Device Health policy options.* * *Access to the Duo Admin Panel as an administrator with the Owner, Administrator, or Application Manager administrative roles.* * *Windows 10 and later or macOS 10.13 and later endpoints with direct access or HTTP relay proxy connection to Duo Security's service on port 443. Proxy connections that perform HTTPS inspection or filtering from endpoints are not supported.* * *The Duo Device Health application does not support Windows Server (i.e. Windows Server 2022, Windows Server 2019, etc.) or earlier versions of Windows (like Windows 7 or Windows 8.1). Additionally, Duo Device Health does not support macOS beta versions or Windows or macOS virtual machines.*   *Possible integration:*   * *Duo's WordPress plugin enables two-factor authentication for WordPress logins, complete with inline self-service enrollment and Duo Prompt.* * *Duo can be configure with OpenVPN,* *Refer to the OpenVPN AS documentation if you're using OpenVPN Access Server.* * *Duo can be integrated with almost any device or system that supports using LDAP for authentication. In this type of configuration, users will receive an automatic push or phone callback during login.* |
| Additional Administrative Considerations |
| *There will be a new rule to allow Duo traffic to pass.* |