SDWAN and Secure Remote Access VPN Solutions – Authentication Recommendations

1. Overview

Vodacom's SDWAN service makes provision for remote VPN so that remote users can log onto the wide area network such as SDWAN. It is critical to implement Multi Factor Authentication as a minimum-security control when opting for remote VPN which can either be;

- Vodacom-Managed Multi-Factor Authentication enabled secure remote access VPN
- Customer-Managed Multi-Factor Authentication enabled secure remote access VPN

Protecting your secure remote access VPN is essential because it serves as a gateway into your broader network, meaning any weakness in its authentication or security controls can expose the entire environment to potential compromise.

Authentication considerations are critical for secure remote access VPNs because they ensure that only verified, trusted individuals can access sensitive corporate resources over potentially insecure networks. Strong authentication, especially Multi-Factor Authentication (MFA), significantly reduces the risk of unauthorized access, credential theft, and compromise, which are major attack vectors in remote-access environments.

Based on your requirements and the capabilities of your connectivity devices, the following MFA methods are available:

- Authenticator app (time-based one-time passwords (TOTP))
- Hardware token
- Smartcard or certificate-based authentication
- Biometric factor
- SMS / voice call codes (fallback only)

It is important to also note that Zero Trust guidance emphasizes continuous, least-privilege, per-request access rather than relying solely on strong authentication. While Vodacom recommends MFA as the primary control for securing secure remote access VPN access, true network protection also requires the addition of both ZTNA and Endpoint Protection (EPP). Each addresses different aspects of the security stack, and together they provide the in depth defence needed for secure remote access.

- **MFA** verifies *who* is connecting, but it doesn't continuously validate device health or constrain lateral movement once a session is established.

- **ZTNA** enforces granular, application-level access with ongoing checks (identity, device posture, context), reducing attack surface and lateral movement risk that traditional VPNs cannot address by themselves.
- **EPP (Endpoint Protection Platform)** controls *what* runs on the device (malware/ransomware prevention, exploit blocking, EDR), which remains necessary even if credentials are strong attackers still target endpoints and VPN gateways, so hardened endpoints are a core best practice.

2. Vodacom-Managed Multi-Factor Authentication enabled secure remote access VPN

With this approach, Vodacom takes full responsibility for managing user authentication on your secure remote-access VPN. We achieve this by integrating the VPN platform with a cloud-based MFA-as-a-Service solution. The specific service we recommend depends on the underlying technology. Below, we outline the available options for both Meraki and Fortinet.

A. Cisco Duo (with Meraki SD-WAN solution)

The VPN client we propose to use with your Meraki SD-WAN solution is the Cisco Secure Client (formerly AnyConnect) VPN, Advantage version as per your request. The cloud-based MFA service we are proposing to use with the Cisco Secure Client VPN is Cisco Duo.

Cisco Secure Client VPN supports a wide range of Multi-Factor Authentication (MFA) options, generally implemented through integrations with RADIUS, SAML, or LDAP protocols. Other major identity providers (IdPs) are supported namely;

- **Microsoft Azure MFA:** Integrates directly using SAML (for modern interactive prompts) or LDAP/RADIUS.
- **Okta:** Supported via RADIUS or SAML integrations.
- **RSA SecurID:** A common enterprise choice for MFA.
- **miniOrange:** Supports various MFA methods, including push notifications, Google/Microsoft Authenticator, and email/SMS OTP.

Cisco Meraki MX security appliances, acting as the hub for both Client VPN and SD-WAN, offer several robust options for user authentication, ranging from simple cloud-managed users to advanced enterprise directory integration. When using Cisco Secure Client (formerly AnyConnect) or native L2TP/IPsec, the Meraki VPN can authenticate users against the following databases:

- Meraki Cloud Authentication
- Active Directory (AD)
- RADIUS
- SAML Identity Providers (e.g., Azure AD, Okta, Ping)

Cisco Secure Client VPN on a Meraki SD-WAN (MX) network supports multiple MFA-capable options for user databases, primarily acting through third-party RADIUS servers or SAML identity providers. Because Meraki does not natively handle the second factor of authentication, it relies on proxying authentication to external databases that support MFA.

It is recommended to choose one of the following authentication methods, configured within the Cisco Meraki Dashboard:

- **Active Directory (AD):** The MX appliance can query your on-premise AD servers directly for user authentication.
- **RADIUS:** The MX appliance sends authentication requests to a specified RADIUS server, which then validates user credentials against its own database or another integrated source (like AD or an MFA provider).
- **SAML Identity Provider (IdP):** This approach uses modern authentication methods like Microsoft Entra ID (formerly Azure AD) or Okta for single sign-on (SSO) and often integrates with certificate-based authentication for enhanced security.

B. FortiToken (with Fortinet SD-WAN solution)

The VPN client we proposed to use with your Fortinet SD-WAN solution is the FortiClient VPN. In this proposal we have included the free version, which is ideal for basic remote access needs. Should you desire a more comprehensive ZTNA/EPP enabled solution, we can propose the licensed version of FortiClient, which has a more comprehensive full featured agent included.

The cloud-based MFA service we are proposing to use with the FortiClient VPN is FortiToken.

As you likely already know IPsec VPN predates SSL VPN, but was eventually replaced with SSL VPN due to the ease of deployment where some networks blocked IPsec traffic mixed with the inconvenience of distributing the IPsec preshared key with the VPN client. Fast forward to the present and SSL VPN is one of the most commonly attacked and exploited implementations.

Fortinet has deprecated and removed SSL VPN tunnel mode across all FortiGate appliances starting with FortiOS 7.6.3. Fortinet requires migration to IPsec VPN (which can use TCP port 443) for remote access. Thus the proposed FortiClient VPN solution is an IPsec VPN and not an SSL VPN.

FortiClient VPN supports multi-factor authentication (MFA) primarily through FortiToken (push/OTP), RADIUS-based solutions (e.g., Duo, Azure MFA), SAML, and third-party integrations. Key methods include FortiToken Mobile push notifications, hardware tokens, SMS/email codes, and integration with Azure MFA via a NPS (Network Policy Server) extension.

With FortiClient (specifically using SSL VPN on FortiGate), you can use Azure Entra ID (formerly Azure AD) as the SAML Identity Provider (IdP) for primary authentication and FortiToken as the Multi-Factor Authentication (MFA) method.

The authentication flow for this scenario is that a user initiates a VPN connection in FortiClient, which opens a browser window for Azure AD authentication. After validating credentials in Entra ID, the FortiGate (acting as the SAML Service Provider) triggers the FortiToken MFA prompt.

While you can use FortiToken, it is also possible to use Microsoft Azure MFA (e.g., Microsoft Authenticator app) instead of FortiToken, which may require Azure AD Premium P1 licenses.

3. Customer-Managed Multi-Factor Authentication enabled secure remote access VPN

Azure Multi-Factor Authentication (MFA), part of Microsoft Entra ID (formerly Azure AD), is a security service that requires users to provide at least two forms of identification to verify their identity when signing in. This extra layer of security helps protect against unauthorized access to cloud applications, on-premises resources, and VPNs, blocking over 99.2% of account compromise attacks. [6]

Azure Entra ID is able to provide MFA through the Microsoft Authenticator app. The following additional forms of verification can be used with Microsoft Entra multifactor authentication:

- Microsoft Authenticator (recommended)
- Authenticator Lite (in Outlook)
- Windows Hello for Business
- Passkey (FIDO2)
- Passkey in Microsoft Authenticator

- QR code
- Certificate-based authentication (when configured for multifactor authentication)
- External authentication methods (preview)
- Temporary Access Pass (TAP)
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call

If you are already using Azure MFA, there is a possibility that you may want to reuse this existing service for the MFA requirements of your VPN solution. This would allow you to make additions, deletions, or changes to your VPN users quickly yourself. Additionally you can configure SSO, provided the initial user sign-on uses 2FA.

However with this option there is a real risk that a misconfiguration of an AD user can allow a threat actor to gain access to your corporate network. From this vantage point, attackers can perform network reconnaissance, move laterally to sensitive systems, steal data, or deploy malware/ransomware. In this case Vodacom will not be responsible for any disruption or damages caused by the breach.

According to 2025 reports, attackers can move laterally for months undetected and achieve full network encryption in as little as 18 minutes after finding a high-value target where privilege escalation is possible. In 84% of cases, they use legitimate, built-in tools to avoid detection.[5]

It is not a Vodacom recommendation for you to manage your own MFA and user database for your secure remote access solution. But should this be your decision, we will still provide the VPN Client applications with both your Meraki and Fortinet SD-WAN solutions for you to use with your existing Azure Entra MFA and Entra ID services.

4. Vodacom Stance

For VPN solutions, Vodacom prefers to propose a fully managed MFA secured VPN solution with the user database managed locally on the firewall or other location.

We do not recommend a username and password only VPN solution and do not offer it for Vodacom secure remote access VPN solutions.

5. Reference Links:

1 https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/f03023fb-007b-11ec-8f3f-00505692583a/secure-sdwan-6.4-arch-for-mssp.pdf

2 https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html#:~:text=A%20year%2Dlong%20study%20by%20researchers%20from%20New,attacks%20*%20Block%2066%25%20of%20targeted%20attacks

3 https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

4 https://www.infosecinstitute.com/resources/general-security/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/

5 https://www.vectra.ai/topics/lateral-movement#:~:text=modern%20security%20programs.-,Lateral%20movement%20vs%20privilege%20escalation,attackers%20prioritize%20stealth%20over%20speed.

6 https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication?tabs=dotnet

7 https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

8 https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-a-dial-up-IPsec-VPN-with-Azure-SAML/ta-p/370414

9 https://docs.fortinet.com/document/fortigate/7.6.5/administration-guide/432396/configuring-microsoft-entra-id-as-saml-idp-and-fortigate-as-saml-sp