5 reasons to protect enterprise VPN access with MFA

ManageEngine
ADSelfService Plus

Table of Contents

Is VPN a gateway to vulnerability?

Virtual Private Networks (VPNs) have now become the de facto method for allowing users to securely access internal resources through the organization's intranet when they are located outside the office. While VPNs aim to promote better connectivity for organizations, IT teams face growing challenges to secure their VPN.

Criminals target credentials

According to the United States Department of Homeland Security, "the surge in teleworking has increased the use of potentially vulnerable services, such as VPNs, amplifying the threat to individuals and organizations".[1]

Enterprises consider VPNs to be one of the most important security technologies[2] (Fig. 1). However, as most VPN solutions only require user credentials for logging in, they are highly susceptible to data breaches. Employing multi-factor authentication (MFA) reduces the risks caused due to credential-based cyberattacks by 99.9 percent, as the primary authentication factor is combined with an additional authentication factor.[3]

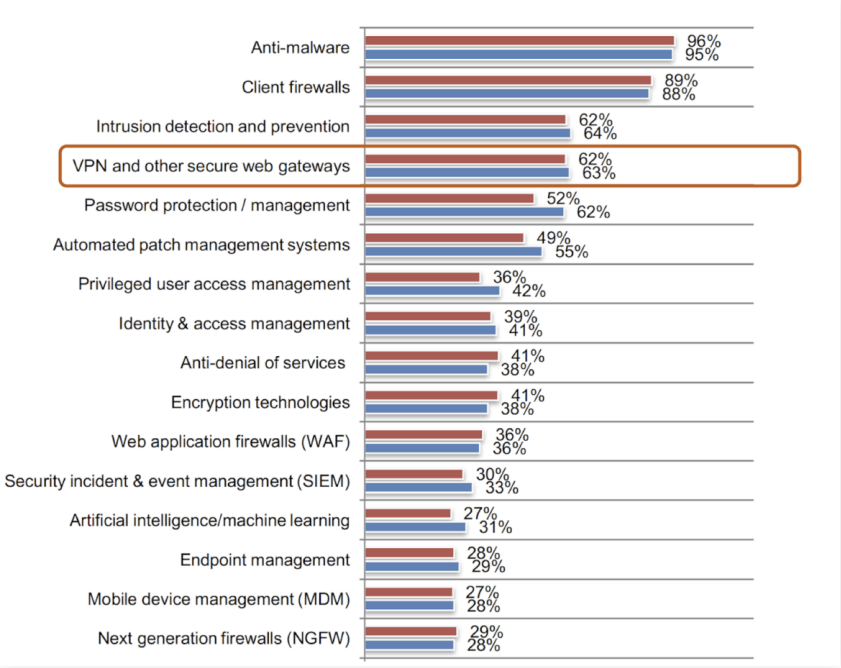


Figure 1: VPNs are one of the most essential security technologies.

Use MFA to secure VPN access

The goal of an MFA solution is to provide greater assurances about the identities of users who attempt to access internal resources through a VPN. With MFA enabled, cybercriminals are not able to breach user accounts, even with compromised credentials. For ensuring the utmost security, not any MFA solution would do as not all are created equal.

Most MFA solutions:

1. Are cumbersome to deploy.
2. Support only limited authenticators, and these can be circumvented by hackers.
3. Provide a poor user experience.

This inevitably will result in reduced return on investment (ROI) and poor user adoption rates.

5 reasons to protect enterprise VPN access with modern MFA

Reason

1

Dealing with stolen credentials

Stolen passwords are one of the top vectors responsible for data breaches.[4] When users adopt weak passwords to secure their VPN accounts, hackers can exploit password dumps or leverage credential-based attacks to breach their accounts. The hacker can then install malware, move laterally, and initiate actions to breach high-profile accounts.

Using MFA can stop such cyberattacks in its tracks because it verifies user identities before granting access, utilizing a secondary authenticator like biometrics or YubiKey.

Reason

2

Achieving regulatory compliance

For example, HIPAA requires organizations with electronic protected health information (ePHI) data data to secure all remote access, including through VPNs, with MFA. Data breaches due to non compliance result in hefty fines, and leave the organization's reputation in shreds.

Glossary:

1. NIST: National Institute of Standards and Technology
2. GDPR: General Data Protection and Regulation
3. HIPAA: Health Insurance Portability and Accountability
4. NYCRR: New York Codes, Rules and Regulations
5. FFIEC: Federal Financial Institutions Examination Council
6. PCI DSS: Payment Card Industry Data Security Standards

Reason

3

Gaining visibility in VPN access and authentication failures

As an IT administrator, you need to monitor VPN activities of remote employees for auditing purposes, and to ward off potential threats. In a nutshell, admins need data on who connects via VPN, when, and what activities are being performed.

MFA solutions generate reports that provide insights into unusual or suspicious activities, time of logon, VPN usage during peak and off-peak hours, VPN usage trends, authentication failures, and more.

Reason

4 Improving security with advanced authentication controls

A general consensus among admins is that biometrics and token-based authentication like YubiKey are more effective than techniques like security questions and answers, or SMS-based verification codes.[5] This is because hackers are initiating more sophisticated attacks, like SIM swapping, social engineering, or phishing, to circumvent basic MFA techniques.

Older MFA techniques are not strong enough to stop hackers. Only modern MFA solutions support advanced authenticators that keep most hackers at bay.

Reason

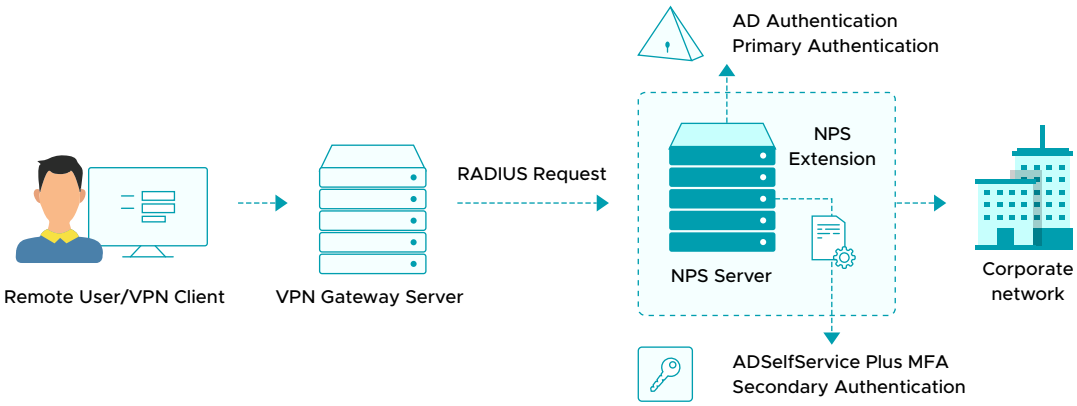
5 Supporting consistent access security for on-premises and cloud apps

With organizations adopting the cloud in droves, admins need to effectively secure remote access for both on-premises and cloud application access. Failing to do so, or creating a separate process for on-premises and the cloud, will create inconsistencies in resource access.

Using advanced MFA solutions will ensure consistent, secure access through a secondary authentication factor for both internal network access during VPN logins, and enterprise cloud application access during single sign-ons.

Modernize VPN security with ADSelfService Plus

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It secures VPN access to network resources with MFA.



With organizations adopting the cloud in droves, admins need to effectively secure remote access for both on-premises and cloud application access. Failing to do so, or creating a separate process for on-premises and the cloud, will create inconsistencies in resource access.

Using advanced MFA solutions will ensure consistent, secure access through a secondary authentication factor for both internal network access during VPN logins, and enterprise cloud application access during single sign-ons.

Behind the scenes: VPN MFA in action

1. A user tries to establish a VPN connection by providing their username and password to the VPN server.
2. The VPN server sends the authentication request to the Windows Network Policy Server (NPS) where the ADSelfService Plus' NPS extension is installed.
3. If the username and password combination is correct, the NPS extension contacts the ADSelfService Plus server, and raises a request for second-factor authentication.
4. The user performs authentication through the method configured by the admin. The result of the authentication is sent to the NPS extension in the NPS.
5. If the authentication is successful, the NPS conveys this to the VPN server.

Supported VPN authentication methods:

- Push notification
- Biometric authentication
- Time-based one-time password (TOTP) authentication
- Google Authenticator
- Microsoft Authenticator
- YubiKey Authenticator

Supported VPN providers

ADSelfService Plus aids all RADIUS-supported VPN providers. Some of the top VPN providers supported by ADSelfService Plus are:

- Fortinet
- Cisco IPSec
- Cisco AnyConnect
- Windows Native VPN
- SonicWall NetExtender
- Pulse
- Checkpoint EndPoint Connect
- SonicWall Global VPN
- OpenVPN Access Server
- Palo Alto
- Juniper and other RADIUS-supported VPN providers

In addition to supporting VPN MFA, ADSelfService Plus provides MFA during:

1. Self-service password reset and account unlocks
2. Machine logins
3. Cloud application access during single sign-on

Conclusion: Not all MFA solutions are created equal. With cyberattacks exploiting VPN exposures on the rise, it's time organizations select an MFA solution that provides advanced authentication controls, comprehensive reports, and is easy to utilize by both admins and users. ADSelfService Plus accomplishes all this and more to protect your organization against data breaches, and ensure regulatory compliance.

Footnotes

1. https://us-cert.cisa.gov/ncas/alerts/aa20-099a
2. https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf
3. https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
4. https://enterprise.verizon.com/resources/reports/dbir/
5. https://info.publicintelligence.net/FBI-CircumventingMultiFactorAuthentication.pdf