UDC 004.272.2

Mykola Serpuchenko, Oleksandr Rokovyi

MULTIFACTOR AUTHENTICATION IN CORPORATE VPN NETWORKS

The paper deals with the modern methods of multifactor authentication when connecting to VPN networks. On the example of Microsoft Direct Access and Forticlient SSL VPN technologies, the main approaches to solving this problem today are shown. The shortcomings of these existing approaches are shown and a new approach that corrects them is proposed.

Key words: MFA, VPN, Direct Access, SSL VPN.

Fig.: 3. Bibl.: 6.

Target setting. According to Forbes with reference to data scientists at Ladders 25% of all professional jobs in North America will be remote by the end of 2022, and remote opportunities will continue to increase through 2023 [1]. As Virtual Private Network provides the external access to the internal resources it is one of the most vulnerable parts of the corporate network.

Actual scientific researches and issues analysis. Nowadays various corporations offer their own ways to securely connect to a VPN. MFA or Multi-Factor Authentication helps secure company resources by additionally verifying the identity of the remote user and device. It serves to protect critical resources from some common identity attacks. There are several corporate solutions of implementing MFA in VPN. Most of them are vendor-specific (like Microsoft DirectAccess, FortiClient VPN, Cisco AnyConnect, DUO security check) and have some drawbacks in implementation.

Uninvestigated parts of general matters defining. Despite a considerable number of existing variants of using MFA in corporate VPN, proposed solutions have some drawbacks. For example, Microsoft DirectAccess is invisible and transparent from user perspective, as it automatically creates IPsec VPN tunnel using user and computer certificates, however, due to its architecture it is difficult routable and based on IPv6 which creates problems to some applications. SSLVPN, for example FortiClient VPN, has no problem with IPv4 and routing, but it requires user to manually connect their devices to the VPN. That mean that VPN connection cannot be established before user logon and the device cannot be manageable and controlled until the connection.

The research objective. The task is to analyze the existing technologies of securing VPN access with multifactor authentication, to find their weaknesses and to propose the solution of eliminating those drawbacks.

The purpose of this work is to develop MFA-based VPN structure that is transparent to a user, stable, cost-effective and scalable.

The statement of basic materials. Recently Microsoft introduced the replacement of Direct Access, Microsoft Always On VPN, which mitigates some problems of its ancestor. It supports IPv4 routing and is third-party vendors compatible. However, Microsoft Always On VPN, still has some weaknesses, and the main one that VPN tunnels, as it is shown on Fig. 1, are terminated on a Windows Server which is not designed to handle a large amount of various VPN connections.

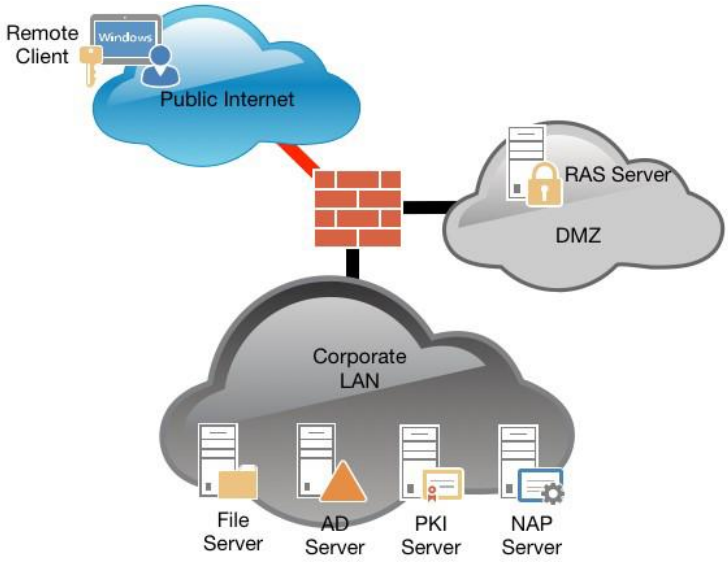

Fig. 1. Microsoft Always On VPN general structure

In order to mitigate the disadvantages of "pure" Microsoft Always On VPN solution it is possible to combine Always On VPN and firewall-based VPN.

General model structure. The chosen structure is similar to the one that is used in Microsoft Always On VPN, as it is a common way to organize the internal infrastructure, that usually has some Active Directory, Certification Authority and Radius servers. In the proposed solution the role of RAS (Remote Access Server) is taken by a corporate firewall. Fortigate firewall was chosen as an example in this research. The process of establishing VPN connection consists of 5 steps and is divided on 2 stages. The first stage (Fig. 2) is the establishing the device tunnel. After a PC was powered on it automatically initiate the creation of IPsec tunnel between itself and the corporate firewall.

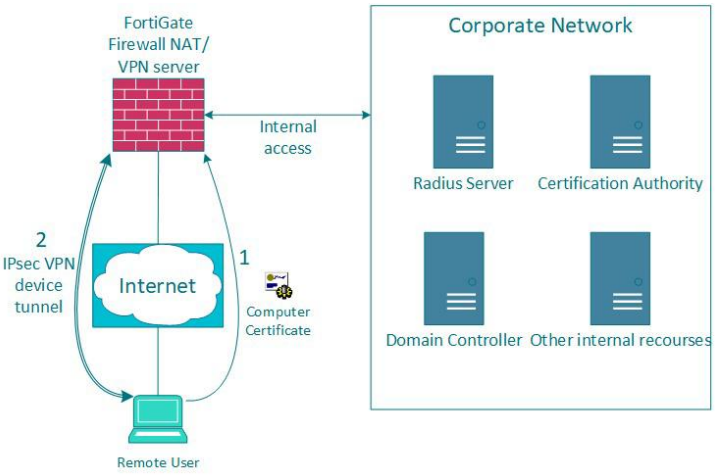

Fig. 2. The first stage in Firewall based Always On VPN

If the computer certificate is valid and trusted, the Firewall establish the VPN tunnel with the remote device. At this step the first stage is completed, VPN device tunnel is established. Device tunnel is an extremely limited connection which aim is to make the remote computer be manageable by the corporate infrastructure. The second stage (Fig. 3) aims to create the user tunnel – fully operational VPN tunnel with a granular access to the internal resources.

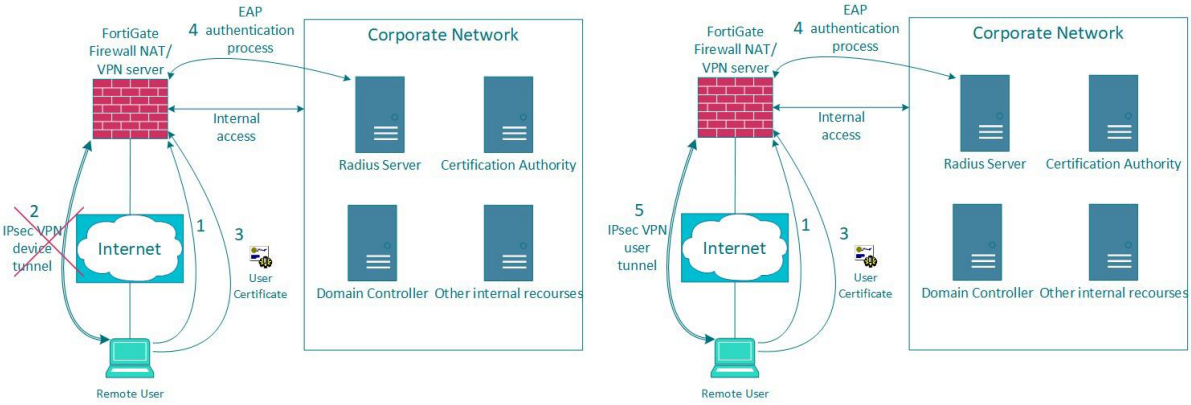

Fig. 3. The second stage in Firewall based Always On VPN

After the user logs in, the computer initiates the new IPsec tunnel based on the user certificate. At this step the firewall delegates the authentication process to a radius server. Authentication process uses secure EAP algorithms to prove the identity of the user and to complete the authorization. After the EAP authentication, Firewall establishes the user tunnel VPN connection and terminates the device tunnel.

Conclusions. The paper has demonstrated the new approach of creating MFA-based VPN structure that takes best parts of modern well-known techniques,

liquidating most of their limitations. The results of this research shows that the proposed solution exceeds other similar technologies in cost-effectiveness, compatibility, scalability, transparency and stability (unlike Windows server, firewalls like FortiGate or Cisco ASA are designed for handling a large amount of various VPN connections which makes the structure more stable).

References

1. This Is the Future Of Remote Work In 2021 // Forbes Dec 27, 2020. URL: https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/?sh=18fea8a1e1de (дата звернення: 10.06.2022).

2. How remote work is quietly remaking our lives // VOX Oct 9, 2019. URL: https://www.vox.com/recode/2019/10/9/20885699/remote-work-from-anywhere-change-coworking-office-real-estate (дата звернення: 10.06.2022)

3. ISO/IEC 27001:2013(en) Information technology – Security techniques – Information security management systems – Requirements (Інформаційні технології. Методи безпеки. Системи управління інформаційною безпекою. Вимоги).

4. DirectAccess // Microsoft Documentation article Jul 29, 2021. URL: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/directaccess/directaccess (дата звернення: 14.06.2022).

5. Configuring the SSL VPN tunnel // FortiOS - Cookbook версія 6.0.0. Дата оновлення 24.06.2020 URL: https://fortinetweb.s3.amazonaws.com/docs.fortinet. com/v2/attachments/a4a06ec3-12a7-11e9-b86b-00505692583a/FortiOS-6.0.0-Cookbook.pdf (дата звернення: 26.05.2022).

6. Always On VPN technology overview // Microsoft Documentation article May 19, 2022. URL: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/always-on-vpn-technology-overview (дата звернення: 18.06.2022).

AUTHORS

Serpuchenko Mykola – PHD student of National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: nikolay.serpuchenko@gmail.com

Rokovyi Oleksandr – associate professor, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: rokovoy@comsys.kpi.ua