



UDK: 005.334:334.72
711.45:004.7
COBISS.SR-ID 148860169
DOI: 10.5281/zenodo.12614792
Professional paper

PRIVACY RISKS IN THE SMART CITY CONTEXT: THE VPN CONUNDRUM FROM ENTERPRISE PERSPECTIVE

Nemanja Pantelić⁴⁹; Sreten Gligorić⁵⁰

Abstract

The escalating demand for privacy is promptly reshaping enterprise IT security in accordance with industry best practices. While smart cities advocate privacy as a core concern from both ethical and economical perspectives, authors of the paper, working as IT security consultants, have been witnessing outdated, insecure and impractical trends in using VPN as a primary security factor. The paper aims to outline the key weaknesses of the VPN approach as well as to propose an alternative perspective based on the current best practices and researches.

Keywords: *VPN, Identity, Security, Privacy, Smart, Cities*

Introduction

Enterprise IT Security represents the best balance between highly secure systems and personal accounts. *Traditional piecemeal, single-layer, single-dimensional security approaches are no longer adequate.* In organizations with the highest security requirements, user-friendly concept is highly disregarded in order to protect sensitive data. The system enables account access only from highly secure locations/ devices and protected networks. In the era of cloud computing, this scenario may appear as a regression as the users are limited by security regulations which affect productivity. Even in these kinds of systems, security breaches are possible and can happen from time to time. *Our experience has shown that the ideal solution does not exist* but based on the best practices, Enterprise IT Security is the closest to the ideal one.

⁴⁹ Nemanja Pantelić, 1985, IAM Consultant, nemanja.pantelic@ic-consult.com, iC Consult Gesellschaft für Systemintegration und Kommunikation mbH, Zettachring 8a, 70567 Stuttgart Germany, +49 160 5139446, n.pantelic@yahoo.com <https://orcid.org/0009-0004-6118-113X>

⁵⁰ Sreten Gligorić, 1989, BSc.Informatics, Danneckerstrasse 4 70182 Stuttgart, Germany, +49 1512 2957502, sretengligoric@yahoo.com <https://orcid.org/0009-0007-2901-6195>



On the opposite side, we have private users using different SaaS applications, globally available from the internet, protected merely by a weak password. Some services are enforcing complex password rules or an additional authentication factor, but it can negatively affect the demand of the application so it's still very common to see bare minimum security requirements. As most of the users are not educated on IT Security topics, on one hand, it's required to offer new security solutions, both fast and user friendly, while on the other hand, it has to enhance the security level. As the best-balanced system, modern Enterprise IT Security offers highly effective and end-user friendly security solutions which can combine user friendly processes with the optimal security requirements. The experience can help utilize the best practices from the industry and incorporate it to wide variety of end users (both private and corporate) in order to achieve optimal security towards user friendly environment ratio. New malicious attacks and breaches enforces Enterprise IT to keep up with the challenging market, bringing innovative solutions and changes which creates new best practices and new approaches.

Using VPN as a reliable security factor can cause damage and the tendencies in the industry should lead towards different approaches. Looking from this perspective, we should acknowledge that the best practices applied in Enterprise industry should be also become a new standard for personal account too.

Historical perspective

Before entering the Cloud era, access to enterprise apps was mainly network based (local). While being a part of a network, client got assigned specific access permissions which were based on local IP addresses/ local domains assigned privileges. In case where network can't be externally accessed, managing who can be a part of the internal structure was efficient enough in keeping unwanted players out of the picture. New requirements like higher availability influenced demand for VPN solutions where the end user could utilize the benefits of being a part of a local network from any physical location. Additional benefit was in fact that VPN is encrypting traffic which means that the chances of getting data intersected were lower.

New tendencies

With commercialization of cloud technologies, the Enterprise IT Security focus moves from securing environment to strengthening of identity. *IAM plays an important role in the case of accessing important data.* The new concept is insisting on secure Authentication and Authorization by utilizing a set of signals like device status, IP or physical location, to authenticate the validity of the incoming request. On top of that, it's possible to track user's behavior which can be helpful in understanding the situation, for example, if the same account logs-in from two distanced places in a short period of time, the system will recognize it as a potential risky sign-in (impossible travel). Based on set of signals, the system will make a decision whether to let the user sign-in, reject or append additional authentication methods.



A robust authentication method is needed to protect online user accounts and data from cyber-attacks. In authentication context, there are various factors for verifying an identity and it is based on three main groups:

- Something you know – mainly alphanumerical password. This is not the strongest security method and new tendencies are going towards passwordless authentication. Still, even if any sort of password is still in use, the complexity of itself should be configured.
- Something you have – it's usually a hardware token or a smart card with a function to carry security certificate (mainly PKI). New tendency is one of the authentication apps which simultaneously check something you have and you are.
- Something you are – In most of the cases, we're talking about fingerprint or face recognition.

The goal is to use these factors based on the situation complexity in order to reconfirm the identity securely with the fastest and easiest process for the end user. It's also important to mention that a significant number of industry leaders are still using VPN in this context. The most common method is to follow IP address as a signal. As an example, it's possible to set whitelist of IP addresses which can access an app. If the organizations whitelist only the VPN IP address, only sign-in attempts from VPN will be considered safe and be passed through. This state can be considered as a hybrid in the context of migration from “network based” environments, towards “cloud”. It's important to stress that the end solution where we are having pure cloud environment, should not rely on VPN. Zero Thrust model is highlighting this in one of the main principles – “Never trust, always verify”

As stated, new security tendencies are moving away from considering VPN to be used in order to upgrade safety and cloud services are less and less dependent on network/server infrastructure. Apart from the security aspect, cloud is offering additional advantages:

- From the redundancy perspective, it's very easy to set additional instances which can offer continues availability of the services. For example, Microsoft is offering Zone-redundant storage with availability at least 99.999999999% per year. This percentage can hardly be reproduced with private hosting of data centers, especially in network environment.
- Additional flexibility can be found in form of scalability. Unlike in case of hosting hardware infrastructure, cloud infrastructure can easily be changed and adapted to the latest needs. For example, demand of a web service can vary based on the time of day so additional instances can be added or removed and even set to scale automatically.



With the facts that cost efficiency is usually a way better and deployment is quite easier, we can conclude that in most cases, cloud environment represents better choice comparing to on-prem- network infrastructure.

Enterprise context example

Enterprises need to foresee and account for possible risks, threats, vulnerabilities, and mitigation strategies before using cloud computing. The main goal of IT security is to protect access to sensitive data. The complete infrastructure typically relies on applications to provide connectivity. To be able to communicate with the database, application will send different HTTP requests to get, change or delete existing or add new information. This connection is relatively static and therefore easy to protect. Moving backward towards the end user, application also receives HTTP requests from the client. In case of web applications, the client is usually browser based and can be access via internet.

When considering IT identity, the key part is in authenticating end user to the app. In order to make the process easy, enterprises will usually use different identity providers. The goal is to reconfirm user authenticity by authentication process and for the next step, issue the token which will be attached to the request and used to confirm authenticity of the user to the application. *Through the use of a message token and an authentication key, verification of the token ensures the authentication of the sender and the integrity of the message*

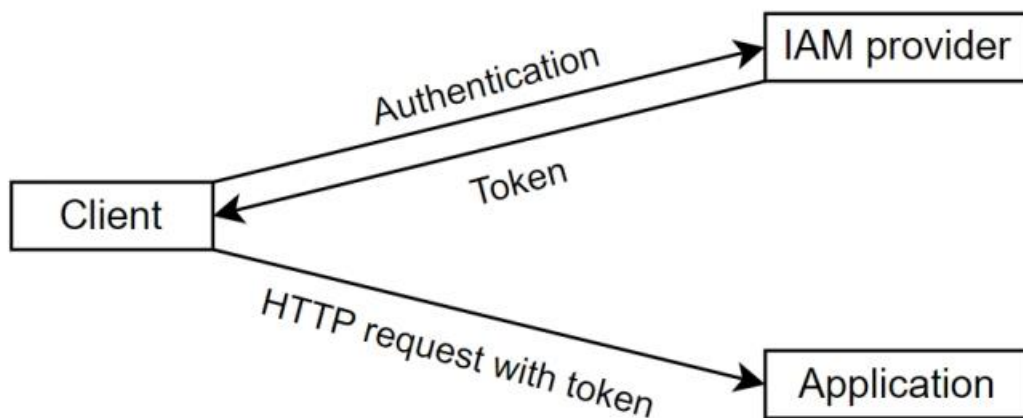


Figure 1 - Token flow

Apart from authentication process, the identity provider can also work on authorization. When the identity is confirmed, the provider is deciding on which changes the account can do. For example, upon authentication, an end user will be able only to read the data, but if authenticating as an admin, the rights will be given for both read and write. This is the



simplest example and on the enterprise level, we have a lot of different permission levels - based on the requirements, for example: access to different apps, option to update internal infrastructure settings, etc. This refers to a security question which is an important zero trust related topic – Least privilege access. The idea is that the accounts are having the lowest privileges to perform the daily tasks. Together with Least privilege access, Zero trust is proposing Just in time concept which is widely accepted in the modern enterprises. Applied to the example of administrators, the accounts will be able to ask for admin privileges for a certain period of time. Upon acquiring the approval, the user will be able to perform admin tasks.

Least privilege access and Just in time concept are the most important part of Attack surface reduction – the strategy to minimize exposed vulnerable points.

Safe sign – device based example

Upon sending the request, identity provider will check the device status. In case the device is trusted, authentication will be confirmed. Based on the action, the user will be allowed to access for the low risk actions or prompted for additional authentication factor to complete sign in process. In case of not trusted devices, additional authentication factor will be prompted for the end user actions while, due to the device status, the attempt will be rejected for high risk (admin) operations.

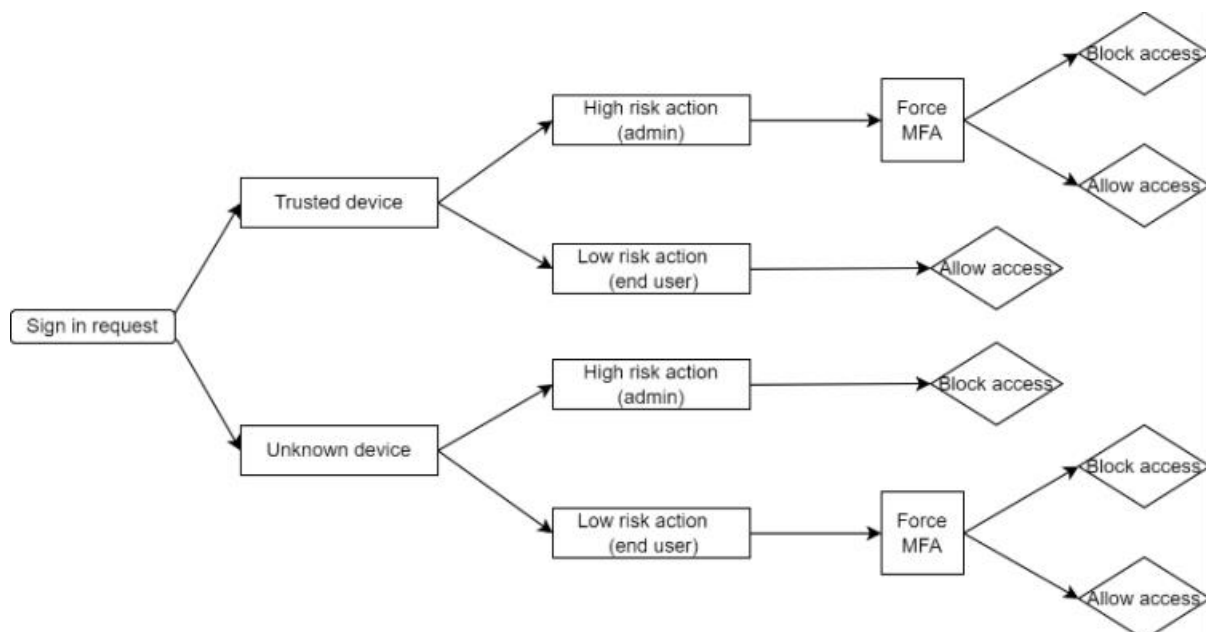


Figure 2 - Sign in flow



Applying best practices to personal accounts

Personal accounts in smart cities should be related to one identity object on one side and multiple services on the other. Due to the high number of different services, grouped in different security categories, we can easily apply the same practices from the enterprise environments. In the context of services, we're talking about lowest security ones which are related to fun and entertainment like gym access and public transport. For these apps, security requirements are low as not a big damage can be produced in case of unauthorized access. On the other side, apps like e-banking, access to the account information settings or health applications containing sensitive health related information requires additional protection level.

VPN role

Considering smart cities will utilize cloud environment along with cloud security practices, VPN role is losing on its importance. The key VPN roles will be listed below along with how "cloud" can address them:

- Tunneling: Two instances communicating over public network using tunneling protocols and encryption. Cloud is offering several encryption forms including Data at rest, Data in transit and End to end encryption which is the most suitable for this case.
- Remote access: Internal network functionality accessible globally. Instead of using network accessible apps, "cloud" approach is oriented to SaaS concept which is offering services like web apps in order to enable global access to the resources.
- Access policies: The policies can determine who can access which resources. With cloud Identity and Access Management, this can be achieved with same or better granularity level.

Based on the listed cases, cloud environment can successfully address majority of VPN roles by using cloud based solutions and technologies if we're referring to enterprise environment.

In a personal account context, access situation is even less suitable for VPN use. It can even be counterproductive. For example, if we want to follow the IP based location signals in case of high security applications like e-banking, using VPN would prevent us to track the real source IP address of the user.



Conclusion

Historically speaking, VPN has a major role in gaining secure remote access to the internal enterprise applications and services. Before the cloud era, network based environment was a common choice for work and, using VPN can be considered as an early form of remote workspace solutions.

In the Smart City context, cloud can be characterized as the core of the IT infrastructures. The most common VPN roles from both security and functionality perspectives can be easily addressed by other modern services and functions in the enterprise context. From the personal usage perspective, there's even less space for VPN. Together with the price and complexity of network requirement and related remote functionality servers, the conclusion is that Smart Cities should direct IT development towards cloud solutions and strong identity in order to achieve higher functionality and security level.

References:

- [1] Liu, S.; Sullivan, J.; Ormaner, J., A practical approach to enterprise IT security. IT Professional (2001), 3(5), 35–42. doi:10.1109/6294.952979
- [2] Fumy W., Sauerbrey J., Kornprobst S., Pillmaier R., Wildgruber R., Hribernik G., Weinzierl P., ... O'Reilly S. Enterprise Security IT Security Solutions: Concepts, Practical Experiences, Technologies, Siemens, Berlin and Munich, Germany (2013).
- [3] Singh, C., Thakkar, R. and Warraich, J. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 8, 4 (Aug. 2023), 30–38. DOI:<https://doi.org/10.24018/ejeng.2023.8.4.3074>.
- [4] Nader Abdel Karim, Hasan Kanaker, Waleed K. Abdulraheem, Majdi Ali Ghaith, Essam Alhroob, Abdulla Mousa Falah Alali, Choosing the right MFA method for online systems: A comparative analysis, International Journal of Data and Network Science (2024)
- [5] Shakir Ullah Shah, Fazl-e-Hadi, Abid Ali Minhas, New Factor of Authentication: Something You Process, International Conference on Future Computer and Communication (2009)
- [6] Steve Turner, David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merritt Maxim, A Practical Guide To A Zero Trust Implementation Roadmap: The Zero Trust Security Playbook, Forrester (2021)



- [7] Mina Nabia, Maria Toeroeb, Ferhat Khendekc, Availability in the Cloud: State of the Art, Journal of Network and Computer Applications (2015), <http://dx.doi.org/10.1016/j.jnca.2015.11.014>, 2.
- [8] <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage>, 20.02.2024.
- [9] Arjun Reddy Kunduru, Security Concerns and Solutions for Enterprise Cloud Computing Applications, Asian Journal of Research in Computer Science (2023), DOI: 10.9734/AJRCOS/2023/v15i4327
- [10] Chai K. Toh, Security for smart cities, IET Smart Cities (2020), 10.1049/iet-smc.2020.0001
- [11] X. Chen, W. Feng, N. Ge and Y. Zhang, Zero Trust Architecture for 6G Security in IEEE Network (2023), 10.1109/MNET.2023.3326356.
- [12] Steve Turner, David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merritt Maxim, A Practical Guide To A Zero Trust Implementation Roadmap: The Zero Trust Security Playbook, Forrester (2021)
- [13] Valentin Mulder, Alain Mermoud, Vincent Lenders, Bernhard Tellenbach, Trends in Data Protection and Encryption Technologies, Springer (2022), <https://doi.org/10.1007/978-3-031-33386-6>
- [14] N. Enomoto, H. Yoshimi, Chinryu Sai, Y. Hidaka, K. Takagi, A. Iwata, A secure and easy remote access technology, 6th Asia-Pacific Symposium on Information and Telecommunication Technologies (2005), 10.1109/APSITT.2005.203686
- [15] Hamed, H.; Al-Shaer, E.; Marrero, W., Modeling and Verification of IPSec and VPN Security Policies. , IEEE 13TH IEEE International Conference on Network Protocols (ICNP'05) - Boston, MA, USA (06-09 Nov. 2005) 13TH IEEE International Conference on Network Protocols (ICNP'05 ()), 259–278. doi:10.1109/ICNP.2005.25