

UDC 004.056

DOI 10.52167/1609-1817-2023-127-4-140-147

A. Nurusheva¹ , R. Safin², A. Amrenov¹, D. Satybaldina¹

¹L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

²V-Office LLP, Astana, Kazakhstan

E-mail: asselnurusheva7@gmail.com

NEW REALITY STRATEGY PROPOSAL: ZERO-TRUST METHODOLOGY

Abstract. Remote access was always one of the big compromises, in the one hand we provide access for employees to private infrastructure (in the COVID world we have only one way to deal with new reality), but on other hand, we drill a big hole for our private infrastructure and hackers and threat actors receive a possibility to attack our internal perimeter. The purpose of the article investigates strategies to mitigate those risks and provide solutions for securely working in a new reality. The article focuses on checking, continuous vulnerability assessment, and how to move from user authentication to a hybrid model - user and system authentication.

Keywords. Security controls, zero-trust, information security, strategy.

Introduction.

Nowadays, we are faced with situations where companies moved employees to home offices [1] and don't know how their devices receive updates and the latest configuration because they are placed out of the office perimeter. For example the best example from before COVID life, is Active Directory - companies enforce configuration and policies to user devices via a secured corporate network and know the result of these policies after enforcing. But after moving employees to the home office companies lost trusted channels to communicate with those devices and visibility of the IT department what happening in the company perimeter, because this perimeter was increased to employees' home network and to the whole Internet. Based on these statements we can make an assumption that the risks of compromising the IT infrastructure of companies are increased and possibility to mitigate those risks decreased [2–3].

The rapid development of the IT sector leads to accelerated application and introduction of digital innovations, and these innovations require highly qualified engineers who can implement those innovations and build modern infrastructures and services.

As we all know in the world high demand for highly skilled engineers, but Universities can't provide enough qualified specialists. Based on this statement we can predict a fast growth of consulting companies and contractors who supports this growth for market makers [4].

The Cybercrimes landscape moved from standalone hackers to highly motivated teams targeted to destruct companies' and governments' infrastructures, including critical infrastructure. Those actors communicate and use different tactics and tools. Many of those tools is a legitimate tool for daily automation and configuration duties. So that big part (in that case we can say that all of today's available antivirus or endpoint detection and response tools) can't prevent those attacks. We can propose user behavior analysis tools, but these tools generate tons of false-positive alerts for every company bigger than a small business (in that case mentioned companies operate more than tens employees). And from that point of view, we can conclude this software is useless from a security perspective [5-6].

Based on all topics before we can conclude that only continuous compliance checking can provide some part of visibility for company assets and give the possibility to infiltrate suspicious assets and devices from access to the company resources [7].

In case old-fashioned infrastructures are based on perimeter security techniques and VPN remote access security department receives one more threat - lateral movement inside infrastructure. For example threat actor takes control of one of a company's assets, doesn't matter

end-user laptop or some server, this actor has possibility to investigate the environment and attack the neighborhood infrastructure elements. This tactic is well known and described in the MITRE attack matrix [8].

Materials and methods.

This article described the reasons and purposes for building secured network infrastructure. And some pieces of historic information about the grown complexity of network architecture and modern applications.

As a start point, we take the document «Specification of Internet Transmission Control Program» by Vint Cerf, Yogen Dalal, and Carl Sunshine [9]. This document describes the specification of TCP and Internet, in this document we first time saw the name Internet. A big part of this document describes communication between networks and transfer of data between networks.

The most challenging task of describing this technology was the method of «castle-and-moat», this term means if one computer from some network is connected to the Internet, all of this network is connected to the Internet. Many old-fashioned networks operate with border firewalls and divide the network into two-part - internal and external. That method looks well in case when all company assets are placed in an internal network. But when we move some assets into an external network, we lose visibility of which device is trusted and complies with our standards. For example, a company asset was placed outside the internal network and was attacked by a hacker, inside the internal network company can receive some pieces of evidence of this attack, but when the company asset is placed outside the company network - the company has no possibility to investigate vectors of attack [10].

For mitigating this situation company needs to follow steps:

install security updates and patches as soon as possible

install endpoint firewall and host-based intrusion detection/prevention system

enable drive encryption on all internal drives (in this case mentioned drives contain system and user data)

apply hardening best practices (it depends on regulator requirements)

enforce to use strict authentication and password policy.

All of these steps look reasonable and simple achievable, but not enough one time to make this configuration. Work from home forced users to use BYOD, and request privileged access to they assets because they need to install some software and make some configurations without visiting the office IT team. High permissions bring the possibility to make misconfiguration to the operation system, including security controls (security misconfiguration is one of the worst security breaches). To avoid this breach company needs to implement continuous compliance checks and as part of this compliance check nice to have a security posture check.

In case when a company makes continuous compliance/posture checks company can avoid a big part of misconfiguration and security breaches. This part of the article described the user-side of continuous compliance/posture check. But monitoring on user side provides the company only visibility without instruments to avoid and respond to those risks. To respond and provide a possibility to respond to this risk company need to impose company policies for end-user. One of the best ways to impose policies is to restrict access to company internal/private resources from devices that don't comply with the company security policies. For that company can implement a secure edge. Secure edge terminates connections from end-user devices and verifies those devices and their configurations to comply with corporate security policies. In case when end-used device complies with corporate security policies - secure edge proxying this request to a corporate resource. In another case, when the device doesn't comply with corporate policies - secure edge shows a notification with clarification and steps on how to fix this issue.

These two steps help companies to mitigate risks related to end-user devices and protect company resources from communicating with untrusted devices.

Despite end-user compliance checking these steps don't mitigate lateral movement tactics and don't protect company server infrastructure from attacks between servers. To protect servers from attack companies need to create restriction rules on firewalls and restrict all incoming connections to servers.

This sounds like a plan, but what about access to services on this server?

We can initiate connections from the server, instead of waiting for an incoming connection, but we need to know what endpoint wants to receive this connection.

We create descriptions of secure access tunnels initiated from internal servers and secure edge services provided to end-users.

In this step, we need to create an equation between edge and access rules and create rules to bypass traffic.

From a security perspective, it looks like trusted-trusted access. From the threat actors' side, it looks like an outbound connection to an outbound connection, in simple words connection from neverland to neverland.

If no listen service and no inbound traffic nothing to attack. And definitely, all traffic is encrypted and protected from repudiation attacks, but this is a different story.

In this part, we discussed ways to mitigate end-user and server attacks.

Results and discussion.

As a result of the previous step we achieve «trust, but verify» paradigm. In this paragraph, we move forward with some technical pieces of realization of this paradigm.

Figure 1 shows a generic architecture diagram of a typical application. This application works without any additional compliance or security controls, and have not adequate protection from threat actors.

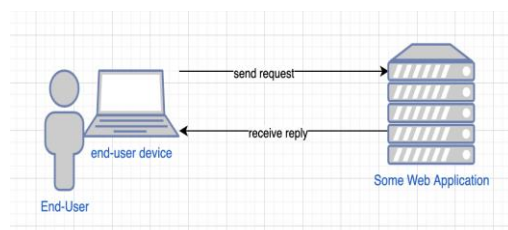


Figure 1 — Architecture diagram of a web application

As we can see, all requests are sent directly between the end-user device and the server. In that scheme, actors can scan web applications, and try to attack servers and web applications. The typical situation for most companies and servers. In that case, the best way is to harden server configuration and train users for digital hygiene.

The typical workflow for that case is for an end-user device to initiate a request to the server, and the server provides a response to this request.

In some cases, these request is encrypted in some cases not. But we keep in mind how easy might be to implement a man-in-the-middle attack [11-15] Figure 2.

Let's try to improve the situation and try to protect web applications and servers from some possible attacks. First of all, we need to move the web application under the secure edge, this is a well-known solution and many companies provide similar services. For many small businesses and not a critical infrastructure this is more than enough.

If we fall back on my experience, it usual dialog with CISO of big companies: «we used {some company name} as DDoS protection and they protect us from attacks».

Later in this article, we provide evidence, that is not enough protection in post-COVID reality. But let's move forward and take a look at the next solution flow.

Figure 3 shows the scheme with terminating traffic to Secure Cloud and after that proxying this traffic to the application. Compared with previous communication flow this solution looks like a silver bullet. With this flow, companies have a possibility to implement DDoS protection, by terminating suspicious traffic in the cloud, easy implement the Web Application Firewall, and protecting web applications from attacks at the web application level.

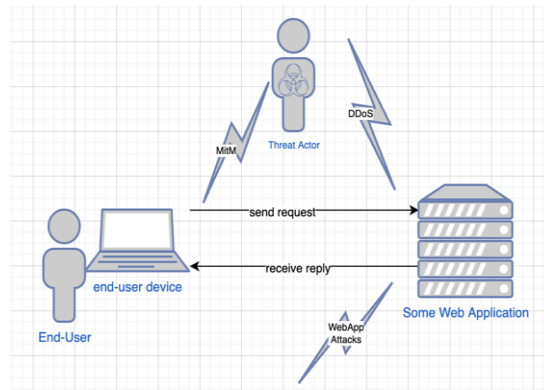


Figure 2 — Architecture diagram of a web application with attack flow

Looks awesome, but the most popular way to bypass this solution - search the IPs of the web application servers and communicate with server directly.

For sure administrators can whitelist IPs of Secure Cloud on the web server firewall, but in any case, this is not protection from misconfiguration, and this solution doesn't protect from an attack on other services on this server, for example, ssh.

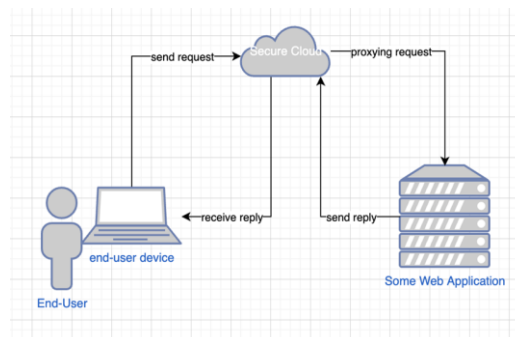


Figure 3 — Architecture diagram of a web application under Secure Edge

Figure 4 shows possible vectors of attack and weak points of modernized architecture. That is better than nothing, but all of the mitigation steps can be bypassed and the attack can continue after some preparation steps from the attacker's side.

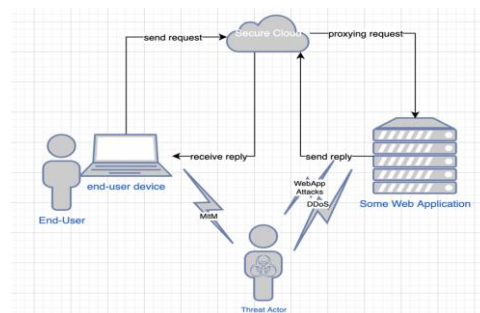


Figure 4 — Architecture diagram of a web application under Secure Edge with attack flow

Possible to implement additional hardening procedures and those procedures help to improve the situation, and for some cases, these steps are enough, in the case when we talk not about critical infrastructure. Also, in that case need to remember about the client-side device and harden it too. But usually, most companies are faced with two different situations. First case when end-user hasn't local admin privileges and we for that case increasing complexity of ways to remote support of this user and possibility to self-service. And the second end-user has enough privileges, but in that case, a user changes the configuration of the device and changes configuration to a less strong level.

Figure 5 demonstrates the scheme when a server has no direct connection to the internet, and all traffic is tunneled to the secure cloud. In that scheme, an attacker has no way to make an external attack on the server or application, because this server has no open ports and doesn't allow any incoming connection. This case looks like a VPN tunnel but has one principal difference - we decrease the blast radius for the potential attack to only one server. Furthermore, all risks related to end-user are still the same as in the first case.

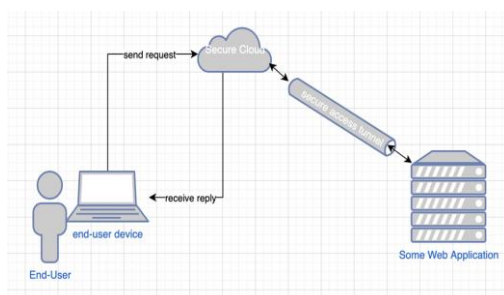


Figure 5 — Architecture diagram of a web application Secure Access Secure Edge

Figure 6 - attack surface for secure edge method. As we can see on the scheme attacker has no possibility to attack the server and stay with a secure edge - and should compromise as the first step secure edge, and after that move forward with a server under a secure edge.

Nevertheless, vectors with MitM and attack end-user traffic stayed without changes.

And via unprotected end-user device attackers can try to bypass the secure edge bastion and move forward to the server. To mitigate this risk we will try to improve this scheme and look into this problem and possible ways to solve it.

Figure 7 looks like a scheme in Figure 5, but with one small change added posture check agent, this agent continuously checks compliance of the end-user device and reports this state to the secure access cloud. When End-user tries to access the application his request goes to the secure cloud and in the cloud validates to compliance state and comply the security requirements. As security requirements might be mentioned for example endpoint detection and response agent, hard drive encryption, latest security update, and fixes for the operating system and all installed software enabled and configured local firewall, etc.

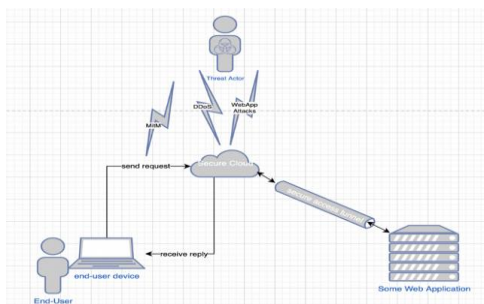


Figure 6 — Architecture diagram of a web application Secure Access Secure Edge with attack flow

All those requirements and controls can mitigate a big part of known attack tactics and make it harder for attacks and persist on the end-user devices. As a good point for improvement can recommend changing file associations on the end-point device and minimum quantity of installed software, to minimize the attack surface of the end-point device. With less attack surface we provide a minimal possibility to successfully attack we provide to threat actors [10].

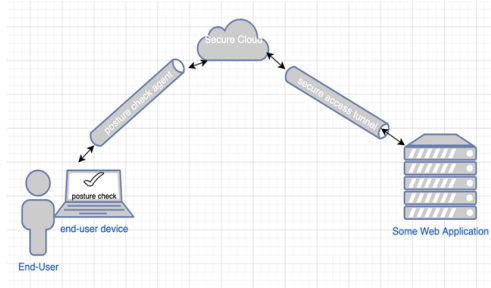


Figure 7 — Architecture diagram of a web application with Secure Access Secure Edge and Posture check

As a result Figure 8, can see all possible attacks will be terminated to secure the cloud, and server and end-user devices are under the protection and outside of the attackers' scope.

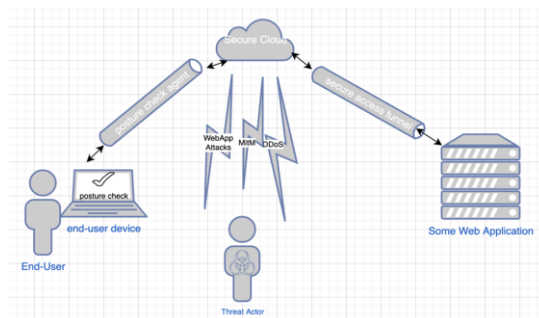


Figure 8 — Architecture diagram of a web application with Secure Access Secure Edge and Posture check with attack flow

There was described a few methods to mitigate possible attacks to server-side and client-side infrastructure, applicability of those methods depends from criticality and type of the service.

In current article we reviewed only web-based applications and basic types of attack to this type of application. But with simple approximation steps we can provide solutions for all of possible types application and attack.

This model already used in many companies and shows his efficiency [16].

Based on these theoretical statements and practical applicability and possibility we can propose this solution as a good step to minimize and avoid many of possible attacks and improve security of infrastructure.

As described above principle «trust, but verify» works fine and for modern threat too. We can use this principle in modern world as our predecers use this principle in they reality, and our descendants will live with this principle in his reality or our future.

Based in all provided above, we can mark the line this principle stayed actual and must have to implement on all critical infrastructure around the world.

Conclusion.

This article describes a new strategy model developed to provide secured access and minimize blast radius. As described above security incident shouldn't affect infrastructure and

defenders need make harder any lateral movement or attackers. New reality provide us opportunity to work from home, to make our work life reality more flexible and more faster than was before, but new challenges and threats make some change of our daily routine and habits. Thats not insane that's just our new reality and we need to evolute in this new reality, like first peoples in the stone age we need improve our habits, include new methods and continuously move forward to the new challenges to the new achievements.

Acknowledgments.

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19175746).

REFERENCES

- [1] G. De Vynck and N. Lanxon, «Google Tells Staff to Work From Home In North America and Europe», Bloomberg.com, 2020. <https://www.bloomberg.com/news/articles/2020-03-10/google-tells-all-north-america-staff-to-work-from-home>.
- [2] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, “A Fuzzy WASPAS-Based Approach to Determine Critical Information Infrastructures of EU Sustainable Development”, Sustainability, vol. 11, no. 2, p. 424, 2019.
- [3] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, “Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach”, Informatica, vol. 30, no. 1, pp. 187–211, 2019.
- [4] Fried, «Tech giants promise to pay hourly workers while employees telecommute», www.axios.com, 2020. [Online]. Available: <https://www.axios.com/tech-giants-promise-to-pay-hourly-workers-while-employees-telecommute-7c1dce8b-8522-4ada-90f2-fb7c30c74288.html>.
- [5] «Cybercrime | Europol», Europol, 2022. [Online]. Available: <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime>.
- [6] P. Kelly, «Trends in Cybercrime in 2022 and Beyond», Blog.govnet.co.uk, 2022. [Online]. Available: <https://blog.govnet.co.uk/technology/trends-in-cybercrime-in-and-beyond>.
- [7] M. Kellogg, M. Schäf, S. Tasiran and M. D. Ernst, «Continuous Compliance», in 35th IEEE/ACM International Conference on Automated Software Engineering (ASE '20), Virtual Event, Australia, 2020, p. 13.
- [8] «Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®», Attack.mitre.org, 2018. <https://attack.mitre.org/tactics/TA0008/>.
- [9] V. Cerf, Y. Dalal and C. Sunshine, «RFC 675 - Specification of Internet Transmission Control Program», Datatracker.ietf.org, 1974. <https://datatracker.ietf.org/doc/html/rfc675>.
- [10] «MITRE ATT&CK®», Attack.mitre.org, 2015. <https://attack.mitre.org/>.
- [11] «MITM on all HTTPS traffic in Kazakhstan», Bugzilla.mozilla.org, 2019. https://bugzilla.mozilla.org/show_bug.cgi?id=1567114.
- [12] M. Erwin and K. Wilson, «Continuing to Protect our Users in Kazakhstan», blog.mozilla.org, 2020. <https://blog.mozilla.org/netpolicy/2020/12/18/kazakhstan-root-2020/>.
- [13] «Kazakhstan man-in-the-middle attack - Wikipedia», En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Kazakhstan_man-in-the-middle_attack.
- [14] D. Warburton, «Kazakhstan Attempts to MITM Its Citizens», F5 Labs, 2019. <https://www.f5.com/labs/articles/threat-intelligence/kazakhstan-attempts-to-mitm-itscitizens>.
- [15] «Great Firewall - Wikipedia», En.wikipedia.org, 2021. https://en.wikipedia.org/wiki/Great_Firewall.
- [16] Zero Trust Maturity Model, 1st ed. CISA, 2021, pp. 1-19 https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

Асель Нурушева, PhD, доцент м.а., Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, asselnurusheva7@gmail.com

Руслан Сафин, «V-Office» ЖШС директоры, Астана, Қазақстан, Ruslan@v-office.org

Асхат Амренов, докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, askhat.amrenov@gmail.com

Дина Сатыбалдина, профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, satybalдина_dzh@enu.kz

ЖАҢА ШЫНДЫҚ СТРАТЕГИЯСЫНЫҢ ҰСЫНЫСЫ: НӨЛ СЕНІМ ӘДІСІ

Аңдатпа. Қашықтан қол жеткізу әрқашан үлкен ымыралардың бірі болды, бір жағынан біз қызметкерлерге инфрақұрылымға қол жеткізуді қамтамасыз етеміз (COVID кезінде жаңа шындықты жеңудің бір ғана жолы болды), бірақ екінші жағынан біз үлкен біздің инфрақұрылымымызға саңылауларды бұрғылаймыз, хакерлер мен шабуылдаушылар ішкі периметрге шабуыл жасау мүмкіндігін алады. Бұл мақаланың мақсаты осы тәуекелдерді азайту стратегияларын зерттеу және жаңа шындықта қауіпсіз жұмыс істеу шешімдерін ұсыну болып табылады. Мақалада күйді тексеруге, тұрақты осалдықты бағалауға және пайдаланушы аутентификациясынан пайдаланушы мен жүйе аутентификациясының гибриді үлгісіне қалай өтуге болады.

Түйінді сөздер. Қауіпсіздікті басқару, нөлдік сенім, ақпараттық қауіпсіздік, стратегия.

Асель Нурушева, PhD, и.о. доцента, Евразийский национальный университет им.Л.Н.Гумилева, Астана, Казахстан, asselnurusheva7@gmail.com

Руслан Сафин, директор ТОО «V-Office», Астана, Казахстан, Ruslan@v-office.org

Асхат Амренов, докторант, Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан, askhat.amrenov@gmail.com

Дина Сатыбалдина, профессор, Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан, satybalдина_dzh@enu.kz

ПРЕДЛОЖЕНИЕ СТРАТЕГИИ НОВОЙ РЕАЛЬНОСТИ: МЕТОДОЛОГИЯ НУЛЕВОГО ДОВЕРИЯ

Аннотация. Удаленный доступ всегда был одним из больших компромиссов, с одной стороны мы обеспечиваем доступ сотрудников к инфраструктуре (в условиях COVID был только один способ справиться с новой реальностью), но с другой стороны мы открываем доступ к нашей инфраструктуре, а хакеры и злоумышленники получают возможность атаковать внутренний периметр. Цель статьи исследовать стратегии по снижению этих рисков и предоставить решения для безопасной работы в новой реальности. Статья направлена на проверку состояния, непрерывную оценку уязвимостей и то, как перейти от аутентификации пользователя к гибридной модели — аутентификации пользователя и системы.

Ключевые слова. Контроли безопасности, нулевое доверие, информационная безопасность, стратегия.
