# Research on Telecommuting Security Solution Based on Zero Trust Architecture

Wanli Kou(✉), Huaizhe Zhou, and Jia Du

Test Center, National University of Defense Technology, Xi'an, China
kouwanli@nudt.edu.cn

**Abstract.** With the continuous deepening of information technology construction and the surge in demand for telecommuting, traditional security protection measures are difficult to cope with complex network environments. Solving security issues such as telecommuting based on Zero Trust architecture become a focus of attention. The core of a Zero Trust architecture is "continuous verification, never trust", which means that by default, both internal and external personnel, terminals, and businesses are considered untrustworthy, and their access to the network and business resources will be continuously verified and evaluated. The paper first expounds the historical evolution, basic characteristics, and key technologies of Zero Trust, and then proposes a telecommuting security solution based on Zero Trust architecture. The solution can effectively solve problems such as identity trustworthiness discrimination, device trustworthiness discrimination and behavior trustworthiness discrimination, to achieve secure and reliable business access for telecommuting workers and intelligent terminals. The solution has reference significance for further optimization and implementation of Zero Trust framework in relevant application scenarios.

**Keywords:** Zero trust · Telecommuting · Dynamic access control · Software defined perimeter

## 1 Introduction

With the rapid development of technologies such as 5G, cloud computing, the Internet of Things, and mobile internet, various universities and enterprises have vigorously promoted the construction of information technology conditions. Meanwhile, due to the impact of the epidemic in recent years, telecommuting has become increasingly popular in recent years and has become an indispensable work mode. Telecommuting generally involves establishing a temporary virtual secure private tunnel in the public network through VPN and other related technologies, forming a relatively secure and stable connection through the public network. Telecommuting provides us with many conveniences in our work and life, but there are also many security risks, such as telecommuting terminals being stolen, telecommuting workers' account passwords being leaked, and telecommuting workers' own security risks and so on.

The traditional network security architecture takes boundary protection as the principle, constructing layer by layer defense lines to protect sensitive resources in the

Y. Zhang et al. (Eds.): CENet 2023, LNEE 1127, pp. 82–89, 2024.
https://doi.org/10.1007/978-981-99-9247-8_9

network. Telecommuting has made traditional network boundaries increasingly blurred, and traditional boundary security measures are difficult to cope with complex network environments. Borderless network security protection begins to receive attention. In recent years, the concept of "de boundary" has gradually developed and grown, and has now evolved into a systematic and comprehensive concept - Zero Trust. Solving security issues such as remote work based on Zero Trust has become a continuous focus of attention for universities, enterprises, and other units.

## 2 Overview of Zero Trust Architecture.

As a new security concept at present, The Zero Trust architecture's core key lies in breaking the default "trust" [1]. It has evolved from a basic concept to a solution framework with certain core technologies, which can ensure identity trust, device trust, application trust, and link trust.

### 2.1 Historical Evolution of Zero Trust

The coarse security model based on boundary protection has been unable to cope with the increasingly severe network security situation, so the concept of "de-bordering" has been developed and gradually evolved into a systematic and comprehensive conceptual framework—Zero Trust.

At the 2004 Jericho Forum, the concept of "de-bordering" was first proposed. In 2010, the famous research institution Forrester officially proposed the term "Zero Trust". In 2011, Google began implementing the Beyond Corp Zero Trust implementation project, exploring the use of Zero Trust concepts to build a new network security architecture, enabling employees to securely access internal systems and resources of the company from anywhere. In 2014, the Cloud Security Alliance proposed a Zero Trust solution as SDP (Software Defined Perimeter), which utilizes mechanisms such as identity access control and comprehensive authorization management to build virtual network boundaries and provide stealth protection for micro applications and services. In August 2020, the National Institute of Standards and Technology of the United States released the "Zero Trust Architecture", which elaborated on the definition, principles, key technologies, and application scenarios of Zero Trust. In April 2020, Qi An Xin Technology Group Inc and Gartner jointly released the "Zero Trust Architecture and Solutions Joint White Paper", proposing a Zero Trust reference architecture and solutions based on typical application scenarios.

After more than a decade of evolution and development, the Zero Trust security concept has been fully recognized in the security industry. In terms of technological evolution, Zero Trust has gradually evolved from the initial network segment to a new generation of security architecture based on identity and covering multiple scenarios; In terms of development planning, various countries have published white papers, evaluation reports, and scheme architectures, and have also implemented them in typical application scenarios.

## 2.2 Basic Characteristics of Zero Trust Architecture

The Zero Trust security architecture differs from traditional security architectures in terms of protection concept, protection objects, and protection foundation (see Fig. 1). The core of a Zero Trust architecture is "continuous verification, never trust", which means that all personnel, terminals, and businesses are considered untrustworthy by default, and their access to the network and business resources will be continuously verified and evaluated.

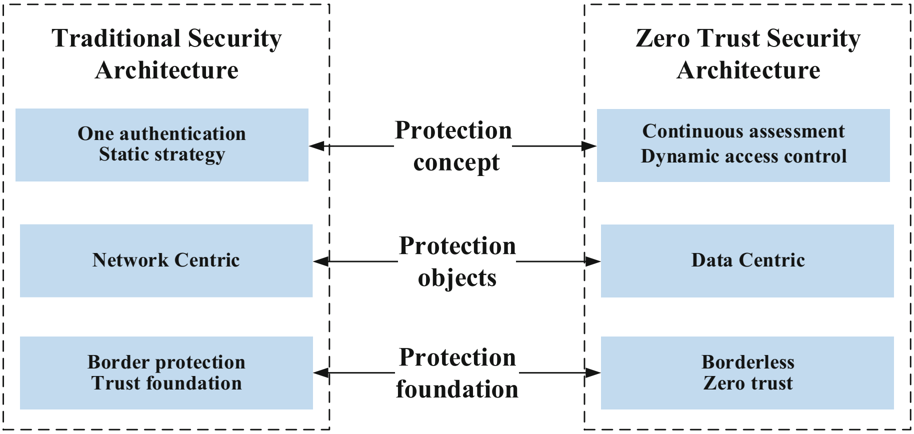

**Fig. 1.** The difference between zero trust and traditional security institutions.

**Based on Identity**. In a Zero Trust architecture, comprehensive identification of personnel, devices, and businesses in application scenarios is a prerequisite and cornerstone for achieving Zero Trust. The Zero Trust architecture collects multiple identity authentication factors such as passwords, certificates, biosignature, and assigns a unique digital identifier to all legitimate users, devices, applications, services, achieving comprehensive identification of various entities. This is the foundation for forming end-to-end trust relationships.

**Continuous Trust Assessment**. Traditional security protection has one-time certification and has been effective for longer time. In order to ensure the continuous legality and security of identity, Zero Trust is based on continuous trust evaluation for authorization decisions. In trust assessment, multiple factors with higher intensity will be used for authentication, and trust judgment will also be made based on comprehensive evaluation of relevant factors such as risk status and environment.

**Dynamic Access Control**. Zero Trust is different from traditional boundary protection devices based on static access control policies. It is identity centric for dynamic access control. Zero Trust requires mandatory identity recognition, authorization judgment, and fine-grained access control for every access request in all business scenarios. Under the Zero Trust architecture, it is a dynamic and micro decision logic that dynamically authorizes access control through risk assessment through continuous trust assessment.

**Minimum permission control**. Zero Trust emphasizes the on-demand allocation of resource usage, with the minimum degree of resource openness based on comprehensive judgments such as business reality, subject needs, and trust evaluation. At the same time, Zero Trust uses technology such as port hiding and traffic encryption to hide resources outside of the subject's permissions, in order to protect business resources.

### 2.3 Zero Trust Key Technologies

**Software Defined Perimeter (SDP)**. The Software Defined Perimeter technology [2], as the security framework of the cloud security alliance, is based on the use of identity access control and comprehensive permission authentication mechanisms to construct virtual boundaries. The SDP puts on "invisibility cloak" for applications and services within the boundaries, so that attackers cannot see the target of the attempted attack at the root, effectively protecting data security. SDP can verify users, devices, data, and other related resources and allow them to access the required services within a specific virtual boundary. It has the characteristics of network stealth, pre authentication and pre authorization.

**Intelligent Identity Management**. Zero Trust intelligent Identity management technology focuses on the intelligent management of key factors such as identity, permissions, environment, activities, to ensure that the right subjects access the right resources based on the right reasons in the right environment. In a Zero Trust architecture, achieving the effects of continuous trust evaluation and dynamic access control will inevitably significantly increase management overhead. To improve the automation level in the Zero Trust architecture, only by introducing intelligent identity analysis can better achieve the implementation of the Zero Trust architecture.

**Micro Isolation Technology**. Micro isolation was first proposed by the VMware technical team as a more fine-grained network isolation technology. For data centers, traditional firewalls typically only provide security protection against north-south traffic while lacking control over internal network east-west traffic. Micro isolation technology can logically divide data centers into different security segments and define security policies for each segment to provide corresponding control services, with a focus on preventing attackers from horizontally moving and spreading within the data center network.

## 3 Telecommuting Security Solution Based on Zero Trust

In the context of large-scale telecommuting applications, due to complex user roles, environments and large network exposure, risk factors will follow such as terminal management and control risk, Man-in-the-middle attack risk, network asset access risk, identity authentication risk, static access control risk and so on. Therefore, there is an urgent need to build a trust system based on the existing security protection architecture. It perceives the comprehensive perception of the environment, continuously evaluates trust, and adapts access control to solve some problem such as security compliance requirements, terminal access requirements, and network security requirements.

### 3.1 Architecture Design

The essence of Zero Trust security is to dynamically control business access based on identity authentication, mainly consisting of identity security infrastructure, Zero Trust proxy, control analysis platform and so on. Through these components, a security access framework that links control and data plane is established. It ensures the credibility of the access subject's access to object applications, data and so on (see as Fig. 2).

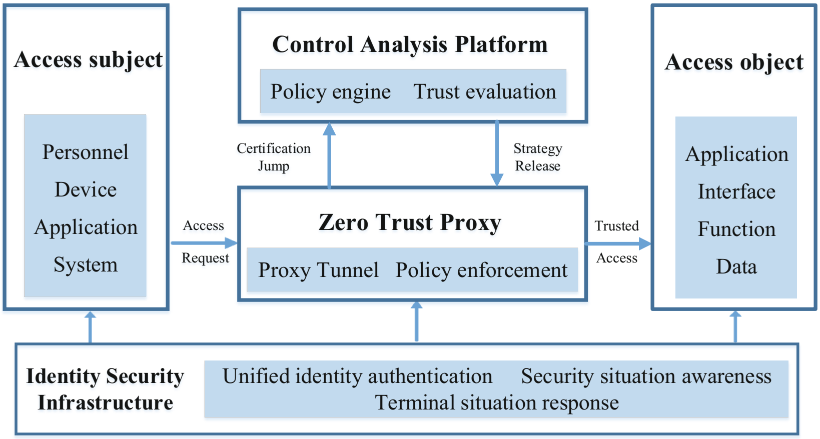

**Fig. 2.** Zero trust basic architecture.

Identity security infrastructure [3, 4] mainly includes unified identity authentication, security situation awareness, terminal situation response and other components, providing Identity management, authority management, situation presentation, terminal protection and other functions. It provides Zero Trust agents with identity, authority and other security baseline data. Zero Trust proxy mainly includes functions such as proxy tunneling and policy execution, and it is a policy execution point for dynamic access control. The control analysis platform mainly includes control engine, trust evaluation and other components, which conduct continuous analysis on access behavior and continuous evaluation. Based on the dynamic Principle of least privilege, all access requests are authenticated and authorized, and are delivered to the Zero Trust proxy module for execution.

### 3.2 Deployment Design

According to the demand analysis and architecture design of telecommuting, a trusted access system for various personnel and devices can be established based on a Zero Trust system [5]. It can achieve trusted detection and discrimination of personnel identity, device access to the business system, and personnel behavior, solving the problem of secure and trustworthy business access for employees and intelligent terminals working outside (see as Fig. 3).

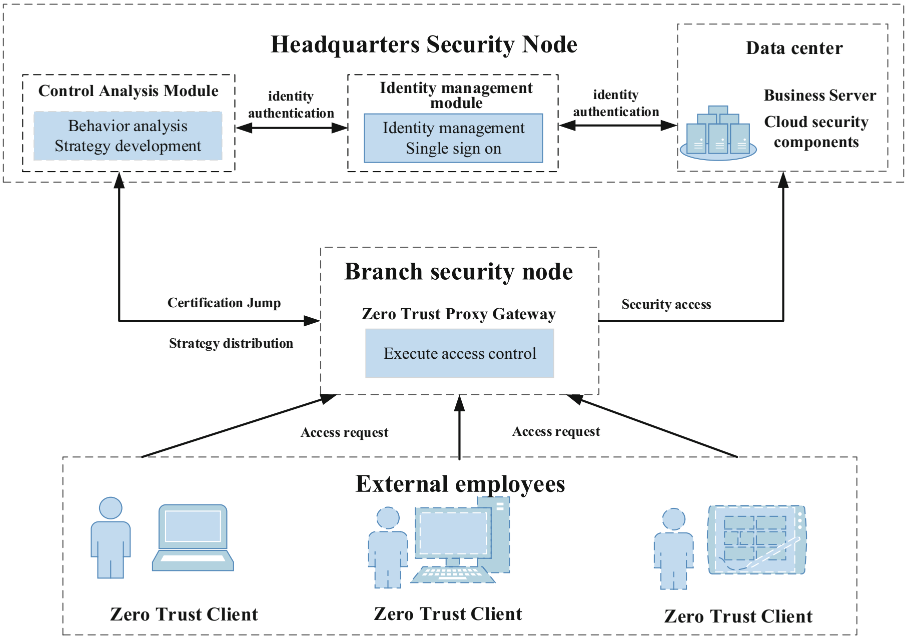

**Fig. 3.** Basic architecture of zero trust system deployment.

This solution is designed according to the application scenarios of three-level security nodes for headquarters, branches, and external personnel. Based on retaining the original security means, the company headquarters deployed a Zero Trust control analysis system and a unified Identity management system, the headquarters data center deployed business servers and related cloud security components, each branch only needed to deploy a Zero Trust proxy gateway, and the employees outside needed to deploy a Zero Trust client to build a terminal trusted access system.

The PC, Pad, mobile phone and other smart terminals used by external workers need to install Zero Trust client. When they initiate remote office and other access requests, the Zero Trust client will start immediately, mainly to ensure that the security compliant terminal is allowed to access business. It prevents attacks on business and data through vulnerable or lost terminals as a springboard, and strengthen the security detection and evaluation of device side applications. It discovers and block untrusted applications from accessing business systems, effectively preventing untrusted applications from accessing the system. After checking compliance with the terminal baseline, it accesses the Zero Trust proxy gateway in an encrypted manner.

The Zero Trust proxy gateway [6] deployed by the branch security node supports the protection function of user accounts throughout their entire lifecycle, application control policy lifecycle management, and control policy exception analysis function. After linking with the Zero Trust platform of the unit headquarters, it can jump to the Zero Trust analysis control module for identity authentication. Authorized users can access the corresponding resources, otherwise access will be denied.

The Zero Trust control analysis module and the unified Identity management module deployed by the headquarters are mainly responsible for the authentication, policy management and distribution of various access business system behaviors, and for the overall scheduling and management. They are responsible for the trust evaluation of the accessed identity, terminal, environment and behavior. Based on the results of the behavioral risks judged by various algorithm models, they decide to allow or reject sessions and let the trusted gateway open or block them.

Before and after the entire external personnel access process, the Zero Trust platform will continuously evaluate the identity, terminal, and behavior of personnel, and can interact with traditional security protection methods. Once risks are discovered, corresponding dynamic access control actions will be executed.

### 3.3 Capability Design

**Establish a trusted Identity management system**. The solution integrates and controls personnel, identities, accounts, permissions, data, and communication methods comprehensively for various business systems in the company headquarters data center and various external access employees. The solution achieves identity unification and provides multiple identity authentication methods. It enhances identity authentication methods in abnormal environments, and verifies the effectiveness and authenticity of access behavior, and prepares for subsequent association analysis and refined dynamic access control.

**Possess the ability to identify abnormal behavior risks**. Through the behavior analysis component provided by the Zero Trust Control Center, the solution learns and models the access behavior of personnel. After a period of learning, the solution summarizes various characteristics of personnel accessing the business system, such as time baseline, access object baseline, access behavior baseline, etc. And the system compares and learns the baseline situation of these elements during each visit process, timely identifying potential risk situations.

**Building a continuous analysis and evaluation system**. This solution has the ability of abnormal behaviors analyzing and distinguishing in situations where the security of personnel outside the unit is uncontrollable, such as the theft of personnel identities or terminals. Zero Trust system continuously evaluates the trust of access subject, terminal and behavior based on multiple data sources, and comprehensively evaluates whether each access can be based on trusted Environment and Behavior.

**Establish a trusted business usage environment**. For different business usage forms and environments of remote office, it is necessary to ensure that the terminal itself can access the corresponding business system in a safe and trustworthy manner. During the process of accessing the business system, other unrelated processes cannot be executed. The Zero Trust system has the ability of network stealth and application stealth. It adapts "authentication before connection" approach, greatly reducing network exposure and effectively alleviating various network attacks.

## 4 Conclusion

The Zero Trust architecture aims to protect data security, aiming to solve the inherent problem of establishing trust based on traditional boundary static access control, and reflects the latest concept achievements of security architecture. The Zero Trust architecture has become an important option for cloud computing, big data, and mobile to realize de boundary network security. However, Zero Trust is still in its early stages, and institutions such as universities and companies should take the optimization and iteration of the network security system as an opportunity to integrate the concept of Zero Trust, and use typical scenarios as a starting point to promote the transformation of Zero Trust capabilities. In addition to telecommuting, application exploration can be carried out in multiple fields such as edge computing environment [7, 8] and 5G security, promoting further optimization and implementation of Zero Trust frameworks and related technologies.

## References

1. Shaw, K.: What is zero trust network architecture (ZTNA)?. Network World (Online) (2022)
2. Singh, J., Refaey, A., Koilpillai, J.: Adoption of the software-defined perimeter (SDP) architecture for infrastructure as a service. Can. J. Electr. Comput. Eng. **43**(4), 357–363 (2020)
3. Hao, P.: He Yuanwen. Research and application of network security architecture based on zero trust Guangdong communication technology **02**, 63–67 (2022)
4. Minlu, T., Meng, R.: Research on zero trust security system. Inf. Secur. Commun. Confident. **10**, 124–132 (2022)
5. Xiaohai, C., Xiaohua, Y., Yanling, L.: Design of remote office security solutions in the context of the epidemic. Guangdong Commun. Technol. **43**(01), 20–23+31 (2023)
6. Tao, Z., Jian, G., Zhen, L., Xuan, Z.: Design of a security gateway based on zero trust architecture. Netw. Secur. Technol. Appl. (06), 2–4 (2023)
7. Dawei, L., Enzhun, Z., Ming, L., Chunxiao, S.: Zero Trust in edge computing environment: a blockchain based practical scheme. Math. Biosci. Engin.: MBE **19**(4), 4196–4216 (2022)
8. Haiqing, L., Ming, A., Rong, H., Rixuan, Q., Yuancheng, L.: Identity authentication for edge devices based on zero-trust architecture. Concurrency Comput.: Practic. Experi. **34**(23) (2022)