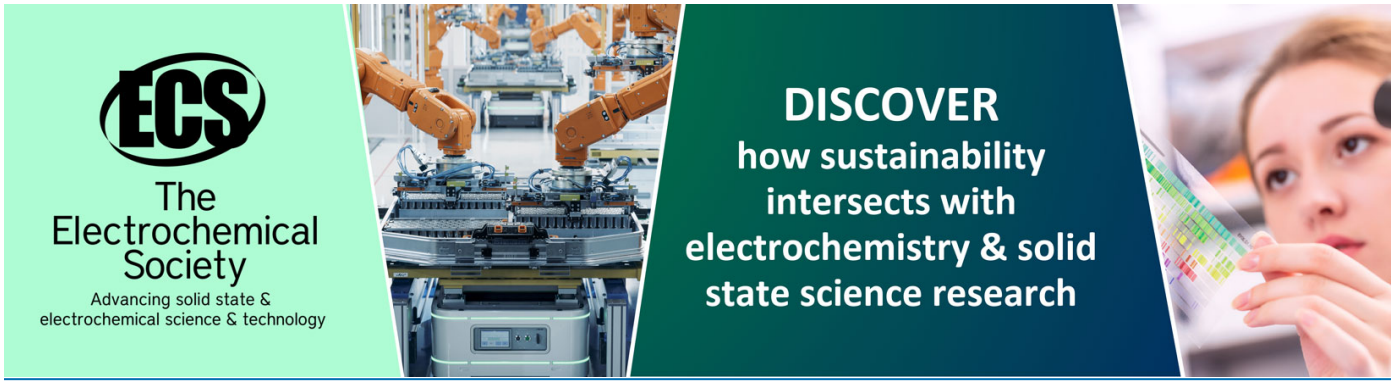
An Implementation Method of Zero-trust Architecture



An Implementation Method of Zero-trust Architecture

Tao Chuan[1 a *], Yao Lv[1], Zhenfei Qi[1], Linjiang Xie[1] and Wei Guo[1]

[1]Information Center of Yunnan Power Grid Co. Ltd.

[a]chuantao@yn.csg.cn [*]Corresponding author's e-mail: ynchuantao@163.com

Abstract. With the development of the Internet, the company network architecture is also undergoing profound changes, and the boundaries between the original internal network and external network are becoming increasingly blurred with the emergence of cloud services. More and more company businesses are deployed on the cloud server, which increases the risk of data exchange between the cloud server and the intranet. An implementation method of zero-trust architecture is proposed in this paper to apply to this scenario. The method can ensure safe and reliable data exchange when the external application server accesses the internal network, effectively protect network communication and business access while not affecting the original internal network protection measures, and make the company network safer and controllable.

1. Introduction

With the advancement of the "Internet plus initiative", high-security networks that were originally physically isolated from the Internet are gradually opening up to provide services for the Internet. The original network structure is usually divided into internal network and external network. Network security protection equipment, such as firewalls and IDS, is deployed at the boundary of the internal and external networks. Data traffic between the internal and external networks flows through these devices. In this way, the traditional network security architecture is more and more difficult to guarantee the security of the network[1], and there are two major security risks. First, this structure defaults to the security of the internal network, which lacks effective defense against attacks from the internal network, making the "fortress" often breached from the inside; second, the security of the internal network is overly dependent on the security protection equipment at the border. Once the security boundary is breached, the intranet lacks an effective means of protection.

The original application servers, such as web servers, are mostly located inside the firewall. The firewall is responsible for security issues, and the server only needs to process business logic. However, with the rapid development of cloud computing, many companies have begun to transfer their business to the Internet cloud platform, which has changed the original company network architecture. It brought about two security issues. The first one is that cloud servers transmit data through public networks. The server is exposed to the Internet and the risk of attacks increases. The second is the blurring of network boundaries [2]. It is difficult to demarcate a clear physical boundary between the cloud server, the company's intranet, and the Internet, making it impossible to deploy traditional network security protection equipment. The original boundary-based security protection concept is also difficult to meet the security requirements of increasingly complex network structures.

In order to solve the problems existing in the network security scenarios, the zero-trust security concept came into being. The zero-trust model was first proposed by Forrester analyst John Kindervag [3], and Google started to build the BeyondCorp project in 2011 [4]. Both have their own focus, but

their core concept is based on “zero-trust”, that is, all networks, traffic, users and devices are untrustworthy.

Because only relying on lagging and passive defense mechanisms such as firewalls, IDS, antivirus, etc., cannot ensure the security of high-level network boundaries, more flexible technical means must be used to establish new logical boundaries for dynamically changing people, terminals, and systems [5]. Through the identification and tracking of people, terminals and systems, and the implementation of effective access control mechanisms, comprehensive identification is achieved. The network architecture established on this basis is zero-trust architecture [6]. In this structure, identity has become the new boundary of network security, and identity-centric zero-trust security will be the general trend of network security development.

In zero-trust architecture, all users and devices are untrusted by default. Before devices and users can access data, they must obtain authentication and authorization [7]. As an advanced network security concept, zero-trust has different implementation methods in specific application scenarios.

“Airport Network Security Protection Scheme Based on Zero Trust Security Architecture” [8] through the registration of users, equipment, applications and other natural entities to form a digital identity, use the digital identity to authenticate users and devices. On this basis, it realizes identity lifecycle management, account sorting and monitoring, authority management and assignment. Its solution is fully functional, but it does not specify how to deploy and apply it to existing network security equipment and software in current applications.

“Application and research of zero-trust architecture in the construction of network security in colleges and universities” [9] redirects all requests for access to campus network services to the access agent. At the same time, the computer needs to provide a device certificate and a user identity token. The access control engine performs authorization checks on the access request, and determines whether to allow its access by judging whether it is credible and has access permissions. However, this program mainly carries out authority discrimination and control, and lacks dynamic evaluation of identity, authority and risk.

“Zero Trust Based Identity Security Solution” [10] gives people, devices, and applications digital identities, and builds an identity-centric fine-grained access control mechanism. The overall solution includes a dynamic trusted access control platform, an intelligent trusted identity platform and smart phone tokens. It can effectively solve the problem of data security access in new business scenarios such as cloud computing and big data, and pilot promotion and application have been carried out. However, this solution requires a lot of equipment and complex network structure. It is mainly aimed at the application requirements of data center and big data platforms, and is not suitable for the network security requirements of small and medium-sized company.

The implementation method of zero-trust architecture proposed in this paper is mainly aimed at the application scenario that users access the intranet data through the application server deployed on the cloud server, and is suitable for small and medium-sized companies whose partial applications are deployed on cloud server but need to interact with the company intranet.

2. Proposed Scheme

2.1. Scheme structure

Part of the business logic requires the external cloud server to access the company intranet data. In order to solve the security problem in the process, security authentication is required before the business logic is invoked, and only secure access requests have the right to invoke intranet data. This method is based on a zero-trust architecture and adopts zero-trust for all devices that are about to access intranet data, which can effectively protect network communication and business access without relying on the physical security mechanism of the network. The zero-trust architecture framework diagram of this method is shown in Figure 1.

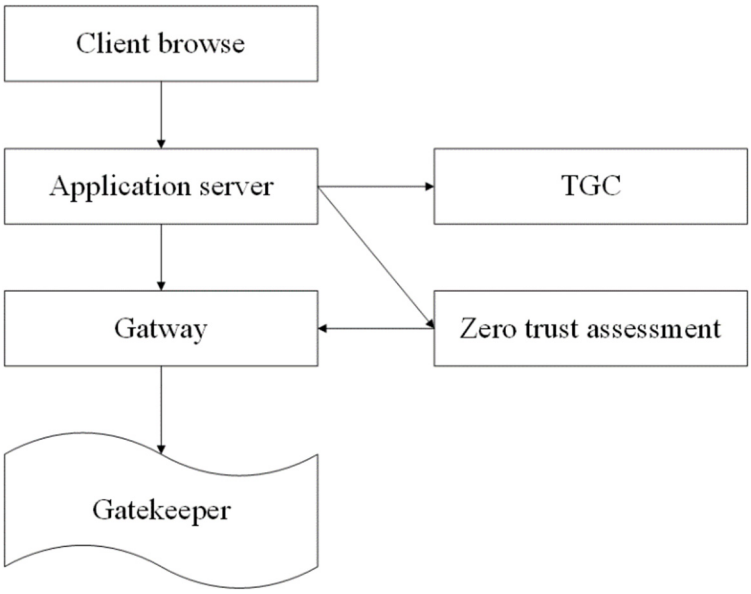


Figure 1. Block diagram of zero-trust architecture

The overall system is mainly composed of TGC (Token Generate Center), application server, evaluation server, and gateway.

- The application server is the actual business server on which business application software, initialization certificates, zero-trust client software, etc. are installed. Client reports security information of the server, such as security vulnerabilities, system design, progress, weak passwords, etc. to the evaluation server.
- The evaluation server is mainly used to evaluate the installation status of the application server. It receives security information from the application server, evaluates and scores the information, and sends the scoring results to the gateway. The application server connects and communicates with the evaluation server through SSL.
- TGC is a token management server used to generate token information for applications. It accepts the SSL connection of the application server, generates tokens for token requests and manages the tokens.
- The gateway is located between the application server and the gatekeeper and is used to determine whether to allow the application server to access the gatekeeper. The gateway accepts the evaluation result of the application server by the evaluation server. Servers with a score greater than 60 are allowed to pass, and servers with a score of less than 60 are forbidden to request.

2.2. Evaluation process

When the client accesses intranet data through the application server, the evaluation server performs a security evaluation on the application server and sends the calculated evaluation score to the gateway to determine whether to allow the application server to access the intranet. The evaluation elements include: (1) Required programs (including weak password detection programs, website detection programs, configuration detection programs, host vulnerability detection programs, brute force protection programs, hardening programs, mandatory access control programs, and micro-isolation control Program and so on; (2) operating system security vulnerabilities; (3) network security vulnerabilities; (4) weak passwords; (5) high-risk ports; (6) sensitive information protection; (7) account and password. The evaluation process is shown in Figure 2.

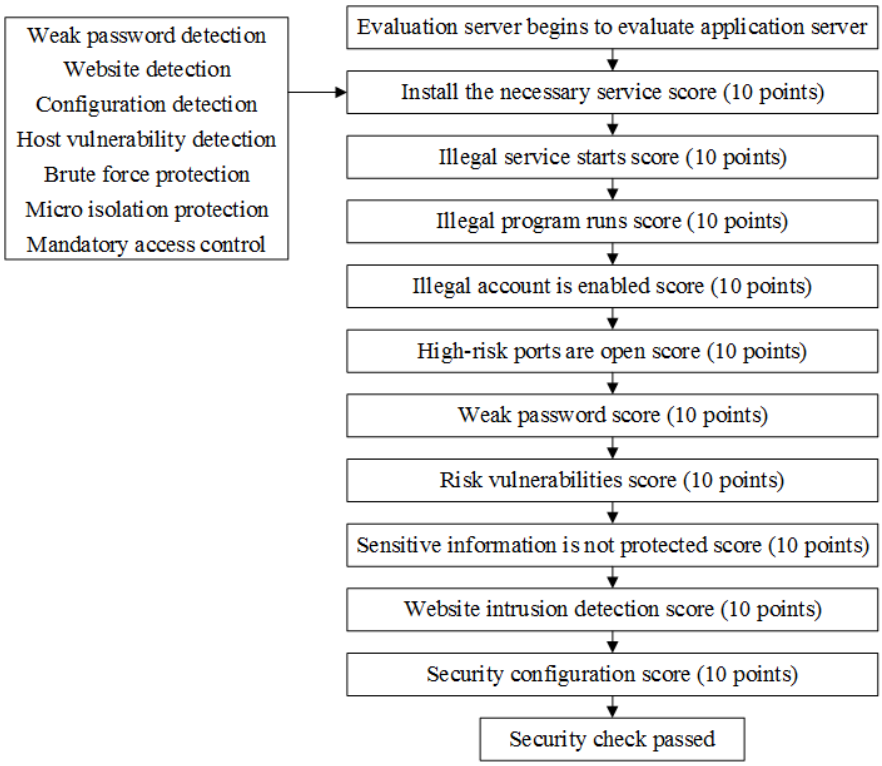


Figure 2. Zero-trust evaluation process

2.3. workflow

The overall working process of data exchange between internal and external networks based on the zero-trust architecture is shown in Figure 3. The operation of the entire process also requires the support of the certificate system. The evaluation server, TGC, gateway, and application server use the same root certificate, including SSL communication and token digital signature. The application server certificate must be installed and configured first, and the gateway needs to verify the digital signature when verifying the token. The workflow of each part is as follows

- The application server installs business software, security software (including but not limited to all software mentioned in the evaluation), and zero-trust proxy client software. The proxy client software runs normally.
- The proxy client software regularly sends application server security information to the zero-trust evaluation server, including various security information and status information needed during the evaluation process, as well as the result information of the security software scan.
- The security evaluation server receives the security information of the application server and the UUID (Universally Unique Identifier), IP, MAC and other information of the machine, evaluates and scores the information, and sends the evaluation score to the gateway. The gateway evaluates the score and decides whether to allow the application server to pass.
- The gateway receives the application server evaluation results of the security evaluation, establishes a status node for each application server, stores its corresponding {IP, Mac, score, evaluation time, validity period}, and overwrites the previous evaluation results after the subsequent evaluation results arrive. The gateway processes each evaluation result into {IP, pass} or {IP, reject} and stores it in the network control kernel so that it can be released or intercepted when the kernel processes the application server request.
- The application server uses the pre-installed certificate to establish SSL communication with the TGC and the evaluation server to complete related communication tasks. The application server needs to obtain a token from TGC, and then use this token to request data from the intranet.

- The TGC server is used to generate, allocate, and manage tokens, and manage and use tokens together with the gateway.
- After the application server obtains the token, it signs it in the URL to request internal data from the gateway or gatekeeper.
- After the gateway receives the request from the application server, it looks up the local pass table according to the IP. If the result is "{IP, pass}" and its token has permission to access the data, it is allowed to access the intranet. Otherwise the request will be refused.
- After the application server requests to penetrate the gatekeeper, it gets a response from the internal network, and the gateway returns the response to the application server, and the access is complete.

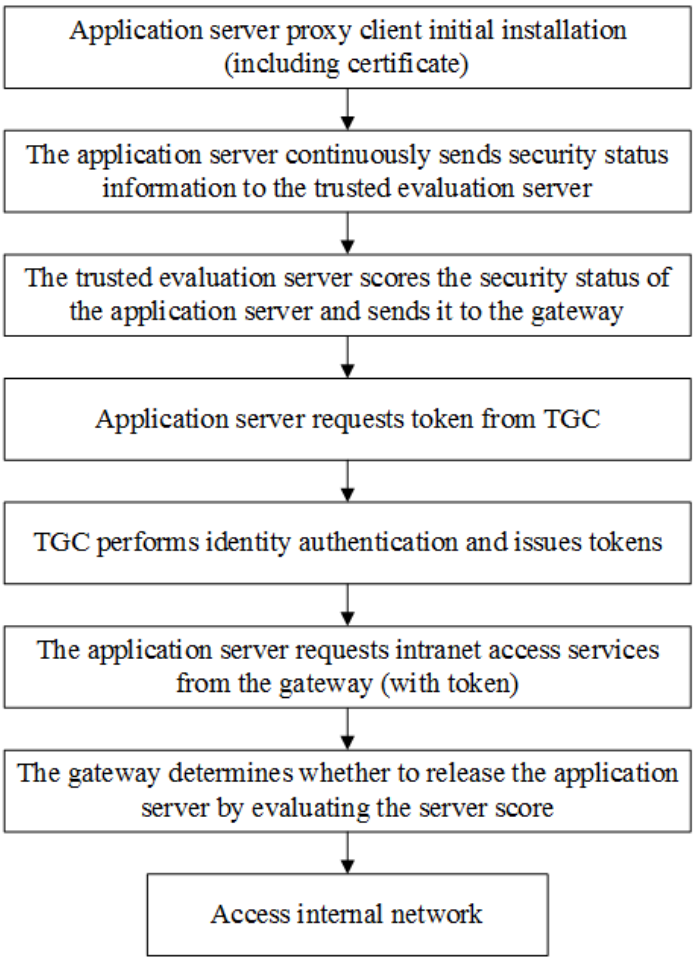


Figure 3. Zero-trust architecture working process

3. Conclusion

Due to the rise of cloud computing, the physical boundaries of the company internal and external networks have become blurred [11], and the application servers transferred to the cloud have lost the protection of the firewall, increasing security risks. For example, web services deployed in the cloud face huge security threats when they exchange data with the internal network. The method proposed in this paper guarantees the security of data exchange between the external network application server and the internal network by building a set of access control mechanisms based on the zero-trust architecture on the existing network of the company, and realizes the flexibility of the access process by dynamically evaluating the server status. It can easily "keep out" unsafe access.

References

[1] Liu, Q. (2018) Data center security protection in the industry based on zero-trust architecture. Security & Informatization, 12:107-109.
[2] Yang, Z., Jin, M., Zhang, X. (2020) Research on Security Technology of Zero Trust in Cloud Business. Information Security and Communications Privacy, 3: 91-98.
[3] Kindervag, J. (2010) Build security into your network's DNA: the zero-trust network architecture. Forrester Research Inc, 1-26.
[4] Ward, R., Beyer, B. (2014) Beyondcorp: A new approach to enterprise security. Login the Magazine of USENIX &Sage,39(6):6-1.
[5] Liu, Z. (2018) Discussion on the construction of network information security system for digital transformation enterprises under the new normal. Cyberspace Security, 9(11): 80-87.
[6] Zuo, Y. (2018) Zero-trust architecture: a new paradigm for network security. Financial Computerizing, 11: 50-51.
[7] Zeng, H. (2020) Discussion on Network Security Model and Zero-trust Practice. Computer Products and Circulation, 7: 48.
[8] Zhong, X., Guo, W., Ma, Y., Wang, M. (2019) Airport Network Security Protection Scheme Based on Zero Trust Security Architecture. Journal of Civil Aviation, 3(03): 114-116+107.
[9] Lin, C., Li, X. (2019) Application and research of zero-trust architecture in the construction of network security in colleges and universities. Computer Products and Circulation, 9:209-210.
[10] Cai, R., Zhang, X. (2019) Zero Trust Based Identity Security Solution. Information Technology & Standardization, 9:46-49.
[11] Xue, Z., Xiang, M. (2017) Data Center Security Protection under Zero-Trust Security Model. Communications Technology, 50(06): 1290-1294.