Peer to Peer Grid Topology with Full Mesh Networking Technology and its Applications

Wenqiang Song
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:wenqiang_song@jit.com.cn

Chuan He
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:chuan_he@jit.com.cn

Zhaoyang Xie
School of Cyberspace Science and Technology Institute
Beijing Institute of Technology
Beijing, China
email:zhaoyangxie@bit.edu.cn

Yuanyuan Chai
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:yuanyuan_chai@jit.com.cn

***Abstract*—The continuous development of computer network technology has accelerated the pace of informatization, and at the same time, network security issues are becoming increasingly prominent. Networking technology with different network topologies is one of the important means to solve network security problems. Zero trust network solves the Virtual Private Network (VPN) problem through peer to peer authorization and continuous verification, but most of the solutions use a central proxy device, resulting in the central node becoming the bottleneck of the network. This paper put forward the Hard Network Address Translation (NAT) traversal formula based on the birthday paradox, which solves the long-standing problem of Hard NAT traversal. Based on this, a full mesh networking technology based on the variable parameter full dimensional spatial peer-to-peer grid topology was proposed, which realizes peer-to-peer resource interconnection for both the methodological level and the engineering level.**

Keywords-Zero trust; Birthday paradox; Hard NAT; port scanning; NAT traversal; full mesh networking technology.

I. INTRODUCTION

Network security is an important branch of the IT industry, with the goal of protecting network systems, data, and services from unauthorized access and attack [1][2]. With the spread of the internet and the acceleration of digitalization, the importance of network security is becoming increasingly prominent. In the early days, network security mainly focused on preventing the intrusion of malicious software, such as viruses and worms [3]. However, as the means of network attacks have become increasingly complex, the scope of network security has expanded to include preventing data breach, protecting user privacy, and preventing identity theft, among other aspects.

A Virtual Private Network (VPN) is a network security technology that creates encrypted network connections, allowing users to securely access remote or public networks. The advent of VPNs can be traced back to the 1990s [4] when businesses began seeking a solution to connect remote offices and employees securely and economically.

Zero Trust is a network security model whose core concept is "never trust, always verify". The emergence of this model is a reflection on the traditional "firewall" security model. In the traditional model [5], companies usually set up firewalls at the boundaries of their networks, and once users pass the firewall, they can access all resources within the network.

VPN and Zero Trust networking [6] are the two existing networking modes, each with its own characteristics. The security of VPN is based on geographical boundaries, but the granularity is relatively coarse, making it difficult to cope with dynamic changes in the security situation. Zero Trust networks solve the problem of VPN through end-to-end authorization and continuous verification, but most solutions adopt centralized proxy devices, making the central node a bottleneck and single point of failure in the network. Another possible implementation is peer-to-peer full mesh communication, but it is necessary to solve the NAT traversal problem.

This paper aimed to solve the core problem in Zero Trust networking. And as a prerequisite for the implementing full mesh networking, a Hard NAT traversal formula based on the birthday paradox was put forward, which solves the long-standing Hard NAT traversal problem [7]. In addition, the full mesh networking technology based on variable parameter full dimensional spatial peer-to-peer grid topology proposed in this article can also solve the problems and drawbacks of zero trust networking, achieve peer-to-peer resource interconnection, and meet the network communication requirements of full mesh networking, covering all types of networking solutions such as site to site networking.

In the second section, we present the virtual network model and explain our contributions in this article. In the third section, we introduced The Hard NAT Traverse Problem and Penetration Formula. In the fourth section, we introduced our solution, Full Mesh, which is a Networking Technology Based on Variable Parameter Full Dimensional Space.

 ISBN: 978-1-68558-099-5

II. NETWORKING REQUIREMENTS

Network Address Translation (NAT) is an address translation technology that can modify the IP address in the header of an IP datagram to another IP address, and achieve address reuse by using the translated port number. NAT is widely used as a transitional technology to alleviate the exhaustion of IPv4 public network addresses, due to its simple implementation. However, NAT also poses a potential security risk, as it can make it difficult to trace the origin of network traffic and can be used to hide malicious activities. Therefore, it is important to implement appropriate security measures, such as firewalls and intrusion detection systems, to ensure the security of networks that use NAT.

A. The difference between zero trust networking and VPN networking

Zero Trust and VPN are both technologies used to establish secure connections between two computers. However, they have some significant differences:

Zero Trust is a cloud-based architecture that allows data exchange between different organizations without a common trust basis, which uses encryption to protect the privacy and integrity of data, and uses authentication and authorization techniques [8]. In contrast, VPN is a technology used to establish a secure network connection between two organizations and also uses encryption to protect data, but it also uses Virtual Private Network (VPN) protocols to hide users' internet activity.

In addition, Zero Trust architecture is typically used to share data between different organizations, such as in healthcare, financial services, or government agencies. VPN is typically used to connect remote users to enterprise networks or to connect two enterprise networks together.

B. Issues with existing networking methods

The security of VPN is based on the division of geographical boundaries (intranet and internet), which has a relatively coarse granularity. Once inside the VPN boundary, access to the entire system is allowed. The security authentication of VPN is static and cannot respond well to the dynamic changes in security situations [9].

Zero Trust solves the problems of VPN by implementing end-to-end authorization and continuous verification. However, most Zero Trust solutions typically use a centralized proxy device to proxy traffic to access services. Although this solves the inherent problems of VPN's boundary division and continuous verification, the centralized topology of the proxy device causes it to become a bottleneck and a single point of failure in the network. Another possible implementation of Zero Trust [10] is for all communication nodes to implement point-to-point full mesh communication with each other, which can overcome the problems of VPN and avoid the typical issues of centralized topology in Zero Trust solutions. However, due to the existence of a large number of NAT devices in the current network, the problem of NAT traversal needs to be solved first to achieve truly feasible full mesh communication.

III. THE HARD NAT TRAVERSAL PROBLEM AND FORMULA

When two devices in different private networks want to communicate to each other, we will face the NAT traversal problem. Two kinds of NAT traversal problems are discussed in this section, and we attempt to propose a solution to the problem.

A. The Hard-NAT problem

The traversal problem occurs when two private networks want to communicate over the Internet and the NAT device is unable to properly route the packets to the correct destination because they are both using private IP addresses. The most common scenario [11] for this problem is when both devices are on different private networks and they cannot communicate directly because their private IP addresses cannot be properly forwarded to each other over the Internet.

There are two types of traversal problems: Soft NAT traversal and Hard NAT traversal. Soft NAT traversal is usually caused by a NAT device that is not properly configured or does not have UPnP turned on. Universal Plug and Play (UPnP) is a universal network protocol that allows devices to automatically configure port mapping rules so that ports can be opened and closed automatically when needed. If a NAT device does not have UPnP enabled or does not configure the port mapping rules correctly, this can lead to Soft NAT traversal problems.

The Hard NAT refers to a stricter form of NAT, also known as Symmetric NAT. In Hard NAT, the NAT device assigns each connection a unique port number that can only be used for that connection and cannot be used by any other connection. This assignment results in external devices not being able to directly access devices in the private network, which can lead to Hard NAT traversal problems. By using asymmetric port mapping, Hard NAT makes it impossible for external devices to directly access devices on the private network. When a device on a private network wants to communicate with an external device, it usually needs to use some special techniques and protocols, such as Session Traversal Utilities for NAT (STUN), Traversal Using Relay NAT (TURN), Interactive Connectivity Establishment (ICE), etc., to solve the Hard NAT traversal problem.

In Easy NAT, the NAT device assigns each internal device a public IP address and port number that is unique to that device, and external devices can access that device through that address and port number. Compared to Hard NAT, Easy NAT uses a relatively loose port mapping method, which makes it easier for external devices to access devices on the private network. When a device initiates a connection to the outside, the NAT device uses the public IP address and port number of this device to map this

 ISBN: 978-1-68558-099-5

connection. When an external device initiates a connection to this device, the NAT device decides which device to forward this connection to based on the destination IP address and port number of the connection. Easy NAT is a relatively loose NAT translation method that uses a relatively loose port mapping method, which makes it relatively easy for external devices to access devices on the private network. However, Easy NAT also has some security issues, and the appropriate security configuration should be considered.

We call Hard NAT and its variants "Endpoint-Dependent Mapping" (EDM). But Hard NAT is a big problem for us, as long as there is such a device in the path, the previous scheme will not work. In addition, certain networks block NAT traversal, which has a much greater impact than this Hard NAT. For example, we found that UCBerkeleyguestWiFi blocks all outgoing UDP traffic except DNS traffic. No matter what NAT hacks are used, there is no way to get around this block. Therefore, a reliable fallback mechanism is needed.

This section discusses the NAT traversal problem in the network, including Soft NAT traversal and Hard NAT traversal, and two types of NAT translation methods, Easy NAT and Hard NAT. For the Hard NAT traversal problem, the use of techniques and protocols such as STUN, TURN, and ICE are proposed to solve the problem. However, some networks that block NAT traversal would require a reliable fallback mechanism.

B. The Hard-NAT traversal formula based on the birthday paradox

The main problem is that the Easy NAT side does not know which address (IP port combination) to send data to on the Hard NAT side, but must also send data to the Hard NAT side to open the firewall on that side.

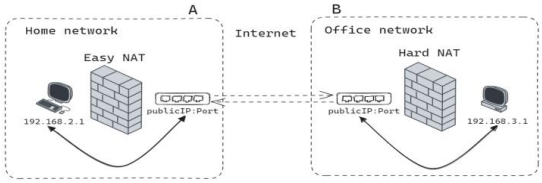

Figure 1. Easy NAT and Hard NAT traversal

As shown in Figure 1, we have known some ip-port combinations for the hard side, because we have run STUN. Assuming for a moment that the IP address is correct, then it is the port that needs to be addressed. There are 65535 possible port numbers. We can scan them one by one and find the correct port number in 10 minutes at worst, if we scan 100 per second. It can solve the problem, but not very cleverly. And it looks so much like port scanning to the IDS software (because that's what we're actually doing) that it's basically going to be blocked.

Using the birthday paradox theory, we can do much better than port scanning! Instead of scanning 65535 possible ports one by one, we can open 256 ports at once on the Hard NAT side by establishing 256 sockets which can send data to the Easy NAT side and let the Easy NAT side randomly probe the target ports.

The birthday paradox is the probability that at least two people out of no less than 23 people have the same birthday is greater than 50%. For example, in an elementary school class of 30 students, the probability of two people having the same birthday is 70%. In a large class of 60 students, the probability is greater than 99%. The birthday paradox is a "trick" in the sense that it creates a logical contradiction. However, this mathematical fact is so counterintuitive that it is called a paradox. The mathematical theory of the birthday paradox has been applied to the design of a cryptographic attack method - the birthday attack.

In the Hard NAT traversal problem, A side is Easy NAT and B side is Hard NAT, the ports of A are fixed (one and known), and B hypothetically opens 256 ports (but it is impossible to know what these 256 port numbers are), which we can scan a total of m (m=t*R) times.t is the scan time and R is the scan frequency.

If we consider the total number of ports that can be used in the end to be from 1025 to 65535, then the problem can be simplified as following: there are a total of (65535-1024) balls in a pool, of which there are B black balls, and the probability that we will catch the black ball if we catch it A times is the results we want. Here B is the number of ports opened on the B side, for example 256, A is the number of times the A side probed. Based on the birthday paradox, the Hard NAT traversal formula (1) is as following:

$$P = 1 - \prod_{i=0}^{A-1} \frac{K - B - i}{K - i} \qquad (1)$$

where, P is the final calculated probability that it can be successfully traversed, the constant K is the total number of available ports (from 1025 to 65535), A is the number of probes on the A side (i.e., scan-time*scan-frequency), and B is the number of open ports on the B side (e.g., 256).

Figure 2 shows the variation of connection success probability with the number of random probes for 128, 256, and 512 ports opened in Hard NAT. Figure 2 compares the number of probes required to achieve 99% success probability when different numbers of ports are opened in Hard NAT. Notice that the higher the number of opened ports, the less probes are needed to reach 99% success probability. Based on engineering experience and resource consumption in real-world usage, we generally use 256 as the number of opened ports on the hard side for NAT traversal.

 ISBN: 978-1-68558-099-5

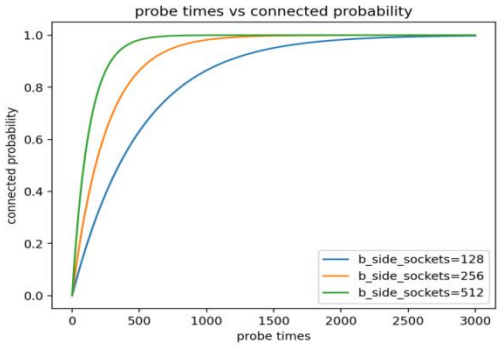

Figure 2. the probability of a successful connection as a function of the number of random probes (with 128, 256, and 512 ports opened in Hard NAT, respectively).

IV. FULL MESH NETWORKING SCHEME AND APPLICATIONS

This Section mainly discusses the full mesh networking scheme based on variable parameter full dimensional space that can be realized by using the birthday paradox based NAT traversal technology on the basis of NAT traversal capability, gateway requirements and encryption requirements. These networking schemes basically cover all existing VPN network application scenarios and have high flexibility and scalability.

A. Preliminaries

The NAT traversal formula (2) based on birthday paradox can be simplified as following:

$$P = det(t, R, n) \qquad (2)$$

where, P represents the total traversal rate, t represents the total scanning time, R represents the scanning rate (times/s), and n represents the total number of ports scanned. Usually, n is taken as 256. According to the previous conclusion, under the condition of limiting R to 100 times per second, the P value can reach 50% within 2 seconds of t, and P value can be above 99.9% before t reaches 20 seconds.

Based on the calculation of NAT traversal capability, which is P, the full mesh networking scheme based on variable parameter full dimensional space can be summarized as formula (3):

$$T = hom(G, P, \theta) \qquad (3)$$

Where, G is Gateway, in which 0 means a network without gateway and 1 means a network with a gateway. P is the NAT traversal rate, in which 0 means unsuccessful traversal and 1 means successful traversal. θ is end-2-end encryption, in which 0 means end-2-end encryption is not in place and 1 means end-2-end encryption is in place.

The full mesh networking technology based on variable parameter full dimensional space proposed in this article can comprehensively cover the following four networking schemes at both the theoretical level and engineering level, including 1) Point-2-Site scheme when G=1 and P=0, θ=1 2) Site-2-Site scheme when G=1 and P=0, θ= 0 3) Site-Mesh scheme when G=1 and P=1, θ= 1 and 4) Full-Mesh scheme when G=0 and P=1, θ= 1.

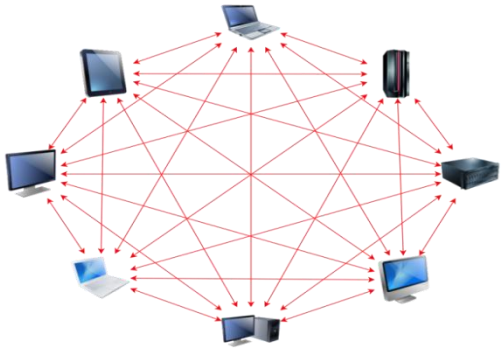

Figure 3. Figure of Full Mesh

Full mesh scheme is the most ideal network form that meets all zero trust requirements, as shown in the figure 3. Each computing node (including physical and virtual) joins a peer-to-peer fully connected network through an SDP agent, and the connection between any two points is encrypted and access permissions are individually separately.

B. Applications

The full mesh networking technology based on variable parameter full dimensional space proposed in this article can be used in many different applications.

First and most popular application is to form a private VPN network for enterprises. Compared to normal VPN applications, a full mesh solution could perfectly and permanently solve the following problems: 1). Single point of failure 2) Performance bottleneck and 3) High Data latency.

In a normal VPN network, all traffic will go through the central VPN server. This server becomes a single point of failure as well as a bottleneck of performance. Using a full mesh solution, traffic travels between each pair of nodes directly through the Internet without going through any central point, thus no single point of failure. System performance depends not upon the bandwidth of the central server, but the bandwidth between each node.

Consider the latency of the system, suppose our central VPN server is located in Boston, and we have two roaming nodes one in Los Angeles, which we call it A, and another in San Francisco which we call it B. When A needs to communicate to B, the data traffic will go from Log Angeles to Boston then from Boston to San Francisco. With a full mesh solution, data traffic could simply go from Logs

 ISBN: 978-1-68558-099-5

Angeles to San Francisco. The typical latency would drop from around 80-100ms to 10-20ms, which is huge for certain applications such as gaming.

The second application is Internet of Things （IoT） devices. Usually IoT devices need to be put in a private network and the quantity of the devices is very large. Constructing such a private network is a heavy burden to the IoT Systems, but our full mesh solution will benefit from its peer-2-peer feature. The large quantity of IoT devices can easily form an overlay private network without any difficulty.

V. CONCLUSION AND FUTURE WORK

In order to solve the problem of NAT traversal when devices need to access each other on the internet, we propose a peer to peer grid topology with full mesh networking technology. We first discussed networking requirements and two different types of network configurations: VPN and Zero Trust networking.

When discussing the NAT traversal issue, we introduced the concepts of Soft-NAT and Hard-NAT traversal and compared the two NAT traversal methods, Easy-NAT and Hard-NAT. For the Hard-NAT traversal problem, we suggested using technologies and protocols such as STUN, TURN, ICE, and also proposed a fallback mechanism to cope with situations where some networks may block NAT traversal entirely.

Next, we detailed the network penetration technology based on the birthday paradox, which can solve the problem of being unable to determine the target port when data communication occurs between Easy NAT and Hard NAT.

Finally, we discussed the variable parameter full-dimensional peer-to-peer networking schemes that can be achieved using the network penetration technology based on the birthday paradox. These networking schemes basically cover all existing network application scenarios of VPNs and have high flexibility and scalability. Through this section's introduction, readers can better understand networking requirements, the NAT traversal issue, and the network penetration technology utilizing the birthday paradox, thus better addressing actual network application scenarios.

In the future, we plan to apply this full mesh networking technology to the actual VPN networking and zero-trust solution, and test its actual performance under heavy traffic.

ACKNOWLEDGMENT

Thanks to the teachers and researchers of the Research on satellite communication security system Project Team of the Jilin Science and Technology Office. Thanks to everyone!

REFERENCES

[1] S. Lee, and MN Kim “This is my paper”, ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[2] A Gizem and O Ayese (2009) Communications and Networks, Network Books, ABC Publishers.

[3] S. Vinoth, et al. "Application of cloud computing in banking and e-commerce and related security threats." Materials Today: Proceedings 51: 2172-2175.

[4] Mughal, A Arif. "Well-Architected Wireless Network Security." Journal of Humanities and Applied Science Research 5.1 : 32-42.

[5] X Wu, et al. "Threat analysis for space information network based on network security attributes: a review." Complex and Intelligent Systems: 1-40.

[6] F Li. "Network Security Evaluation and Optimal Active Defense based on Attack and Defense Game Model." 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, 2023.

[7] B Bijender, et al. "Big Data Architecture for Network Security." Cyber Security and Network Security: 233-267.

[8] Ghelani, Diptiben, KH Tan, and KRK Surendra. "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking." Authorea Preprints.

[9] Hasan, K Mohammad, et al. "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things." IET Communications 16.5: 421-432.

[10] Pramanik, Sabyasachi, et al., eds. Cyber Security and Network Security. John Wiley and Sons, 2022.

[11] Ghelani, Diptiben. "Cyber Security in Smart Grids, Threats, and Possible Solutions." Authorea Preprints.

 ISBN: 978-1-68558-099-5