Journal of Computer and Communications, 2020, 8, 45-58
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

# Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology

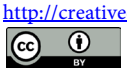
**Heping Pu[1], Yijun Wang[1], Xinke An[2]**

[1]Network and Information Center, Southwest Petroleum University, Chengdu, China
[2]Hangzhou Dip Technology Co., Ltd., Hangzhou, China
Email: puheping@swpu.edu.cn, anny6629882@swpu.edu.cn

**How to cite this paper:** Pu, H.P., Wang, Y.J. and An, X.K. (2020) Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology. *Journal of Computer and Communications*, **8**, 45-58.
https://doi.org/10.4236/jcc.2020.88005

**Received:** August 5, 2020
**Accepted:** August 25, 2020
**Published:** August 28, 2020







## Abstract

Based on the analysis of the security problems existing in the cloud platform of the data center, this paper proposes a set of cloud platform security protection scheme being with virtualization technology. This paper focuses on the overall architecture of cloud platform as well as the design of virtualization security architecture. Meantime, it introduces the key technologies of VXLAN in detail. The scheme realizes flexible scheduling of security resources through virtual pooling of independent security gateway and virtual machine isolation through VXLAN technology. Moreover, it guides all horizontal traffic to independent security gateway for processing, unified management of security gateway through cloud platform by using Huawei NSH business chain technology. This scheme effectively solves the horizontal transmission of security threat among virtual machines, and realizes the fine security control and protection for the campus data center.

## Keywords

Network Security, Cloud Platform, Virtualization Technology, VXLAN, Horizontal Traffic

## 1. Introduction

With the development of information technology, campus private cloud, which is famous for its characteristics of cost-effective, easy-to-expand and modular management, etc. in the construction of data center in campus. Compared with the traditional data center, the completion of the cloud platform data center has brought new challenges to the security management of the data center, meanwhile further enhancement on service capability of information technology in

teaching security, scientific research innovation, administrative office and so on.

According to the research, there are two main ways to realize the security protection of data center cloud platform. The first is to install software products (NFV) on virtual machines [1] [2]. This method is currently widely used, but there are serious server performance consumption, virtual machine compatibility, etc., which do not meet the needs of high reliability and high stability of the campus network data center. Another way is to deploy traditional hardware security equipment [3] [4], which can protect the vertical traffic of the data center, but in this way it's difficult to protect the horizontal traffic inside the campus network virtual machine. The existing cloud data center security protection design does not have a unified standard for cloud data center security protection in the industry, yet cannot fully meet the needs of campus private cloud construction. Therefore, it is imperative to design a security protection model for campus cloud data centers.

Data center is a vital infrastructure of intelligent campus construction in colleges and universities. In addition to performance, capacity and other carrying capacity requests, security is an important guarantee to all users. Effective services to faculty and students throughout the campus are unable to be provided with an unsecured data center. With the support and status of cloud platform, safety-critical issues on horizontal flows are particularly prominent. For magnificent efforts, school and professional security company carried out a practical research on horizontal flows security protection together. Based on the implementation of the cloud platform deployment, conduction of cloud platform virtual machine horizontal flows to an external private security business gateway for suitable manipulation. It has both achieved the realization of the cloud platform fine-grained security protection and the attempt at increasing the burden of virtual machine resources as much as possible.

## 2. Security Issues on the Cloud Platform of Data Center

In the current framework of cloud platform, there are multiple technical criteria. Specifically, the applied framework for computing virtualization includes VMware, KVM, Docker, etc. In technology of network virtualization, there are VEPA, Open Flow, VXLAN, etc. Criteria for virtual storage such as HDFS and Hbase, etc. are also available.

However, in view of various kinds of security problems which may exist in the cloud platform of colleges and universities, there are no systematic security requests. This article summarizes the security issues of cloud platform virtualization technology in the following four categories [5].

### 2.1. Security Issues in Network Infrastructure

Data center network structure is similar with campus network structure. Both of them include core, aggregation and access but there may also be some differences, which depends on the scale of the data center and the use of switching equip-

ment. Data center switches, SDN switches may bring new changes to the network level, but the security issues in which are fundamentally consistent. The security problems in data center network mainly come from three aspects: first is due to network equipment, cables and other problems caused by the equipment security risks; second is the power supply, air conditioning and other failures caused by environmental security risks; the third is network paralysis and security risks on data leakage caused by network attacks. In the status of "Everything-Linked by Internet", the level of attack to critical infrastructure is less difficult [6]. However, in the case of "not-timely" update of network infrastructure security policy, cloud platform security will be a severe problem.

### 2.2. Issues on Environmental Security of Data Center Computing

Data center computing environment domain mainly consists of internal and external server access, in terms of the different business importance and security protection requirements. Generally, it has been refined into ordinary servers, important servers and core server access areas. Meanwhile, there is also dedicated network core service area. The existing data center computing environment in our campus includes managed data room, core data room, backup data room and so on. The main problems in data center computing environment are confusion of access management, irregular operation process, hardware as well as software failure, data security as well as privacy issues, database environment instability [7]. Moreover, other problems of horizontal flows among virtual machines, such as virus spread, virtual machine migration and quite a few inevitable problems. Environmental security of data center computing is the fail-safe factor for normal operation of virtual machine service clusters on cloud platforms.

### 2.3. Issues on Management of Network Security

Network security management generally consists of operations management, network management as well security management access area, according to its own characteristics of network size for the merger or regional division. The main issues of network security management are network transmission leakage, access without authorization as well as abuse, poor management of authentication strategy. The issue of network security is the fundamental of the normal operation service in cloud platform of data center and an important factor of stability for database.

### 2.4. Issues on Boundary Access

The data center cloud platform primarily offers service to internal teachers and students, meanwhile sporadic off-campus services will also be in existence. All of this is because the staff who are not living in the campus and students who are trainees outside also have comprehensible needs to access the on-campus data center. The boundary access of data center is mainly composed of internal access

area, off-campus access area, on-campus access area, etc., which is the primary channel of data exchange and authorized access of cloud platform. If the boundary access security protection is not good enough and the entire virtualized cloud platform directly "exposes" on the Internet, the difficulty of subsequent security protection for cloud platform will be in sharp increment. Boundary access is primarily a threat from external intrusions by hackers, external penetration of viruses, and cyberattacks against data center.

Security issues are one of the basic guarantees for the stable operation of data center cloud platforms. The aforementioned security issues have correspondent solutions in the public cloud, among which the mainstream solution strategy is to adopt the NFV (Network Function Virtualization) approach. This method can live out the functions of network firewall, switch, router, load balancing and so on through software virtualization, thus achieving flexible virtualization of business modules and network modules.

However, adaptability problem of the application scenario exists in NFV. On the one hand, NFV needs to consume quite a few computing resources from the server when it comes to processing the business. That means when NFV handles security issues, the CPU performance of the server will be degraded. On the other hand, the way NFV virtualizes makes server performance and security management problematic. The campus cloud platform requires specifically of independence, privacy, and functional personalization of management so on and so forth from products. Therefore, NFV's operation and security is not the best solution for schools [8], and it is imperative to design a protective mechanism for security based on campus cloud platform.

## 3. Security Design of Cloud Platform Virtualization for Data Center

### 3.1. Architectural Design for Cloud Platforms

In this article, a data center cloud platform system based on technology of virtualization security is designed for the research of virtualized horizontal flows. By means of building a logically isolated, user-owned, user-configured and user-managed cloud platform virtualization environment, to improve the security of school data center resources and simplify data center network deployment is a good intention. The campus private cloud can choose the IP address range arbitrarily. Facilitation for network management and configuration might be achieved by means of the creation of multiple subnets, customizing security groups, and configuring routing tables as well gateways, etc. For the sake of the execution of simultaneous implementation of security policies at cloud platform in the process of rapid network change, fabulous management and configuration of should be achieved. Meanwhile, through the comprehensive application of "inner-and-inter" security groups' access regulation as well as various security measures such as firewalls, the access control of instances in the subnet will be strengthened. The cloud platform adopts a protective framework for end-to-end, full-virtualization, as shown in **Figure 1**.

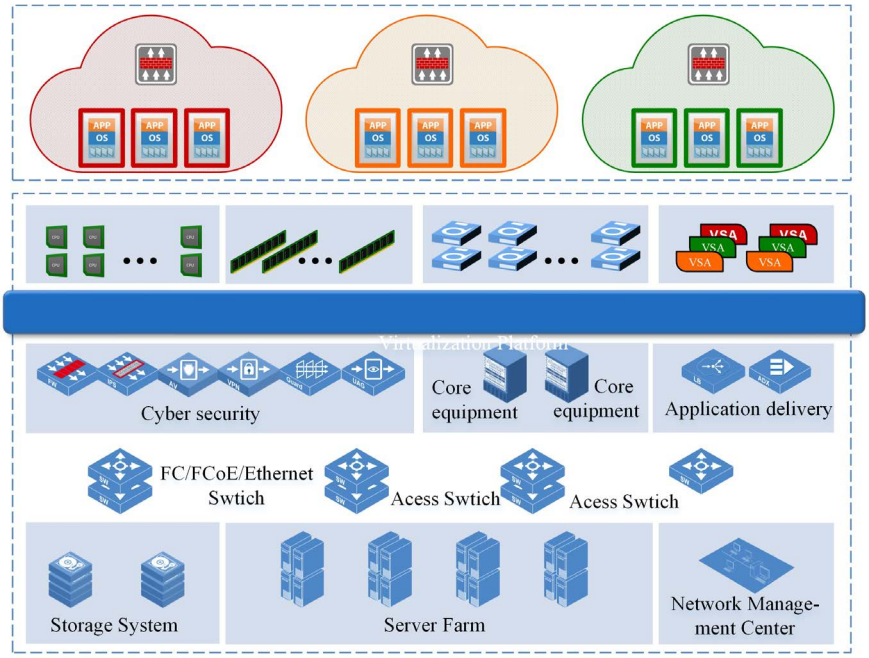



**Figure 1.** System overall architecture design block diagram.

The data center cloud platform based on virtualization protection combines three resource pools, such as Boundary access, storage, and network security. This style of framework is notably characterized by the combination of core switches in data center with network security equipment, which achieves fixing and traction through the core gateway. According to the requirements of the application, the core security network switching equipment is equipped with business board cards, which can realize the functions of applied firewall, protection to IPS intrusion, loading balance for application system, flows cleaning, etc. In addition, execution of professional security protection at 4 to 7 layers to meet the security needs of the cloud computing data center is also inevitable [9].

In terms of the different business in data center and requirements of security area boundary protection, the functions of each business board have been virtualized. To meet the requirements of security level protection for businesses in schools and focus on corresponding security policy deployment, establishment on intelligent security network resource pool, each virtualization function (such as virtual firewall, virtual IPS intrusion defense, virtual load balancing, etc.) through N:M virtualization are at hand. These functions are corresponding to one or a type of business which is in the same needs [10].

### 3.2. Architectural Designs on Virtualization Security

For the security protection of the data center cloud platform, mainly focus on the security problems of the cloud platform discussed previously. Based on a comprehensive analysis of various security risks, according to different location partitions, security domains as well as levels of protection requirements, the implementation of personalized security policy. According to the requirements of

cloud computing technology and traffic model for the construction of security platform, security platform is with high performance and low-latency processing power, high reliability and capabilities of rapid responses [11]. This article focuses on the management of divisions for detailed security domain and virtual security domain of business hosting and virtual machines to achieve the comprehensive security protection and auditing capabilities for different virtual businesses [12] [13]. On behalf of ensuring the isolation and security of each business platform, building a safe resource pool with devices of security gateway which could support virtualization technology, firewall as well as intrusion defense is undoubted strategy. Meanwhile, being with the function of assigning security modules such as virtual firewall and virtual IPS to each business platform well also should be attached importance on. The design of security architecture is shown in **Figure 2**.

Being with this framework and architecture, virtual machines are isolated by VXLAN technology, while all virtual machines' flows will be conducted to a security pool for secure processing, and the processed lateral flows will flow back to the corresponding virtual machine in terms of different business needs. This technology scheme can both guarantee the recognition to application as well as security of virtual machines, and realize the control of flows within virtual network by the security resource pool. In addition, application support for virtual machine migration can also come true.

Virtualized security pool (**Figure 3**) integrates firewall, IPS, security audit and other functions into a whole one. It can both achieve the rapid expansion of

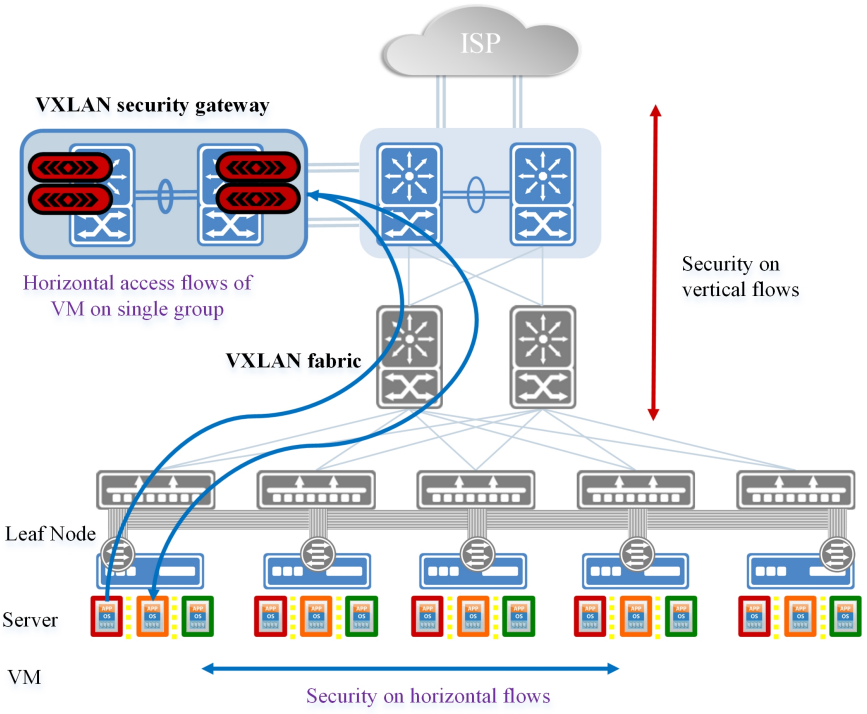



**Figure 2.** Virtualization security architecture.

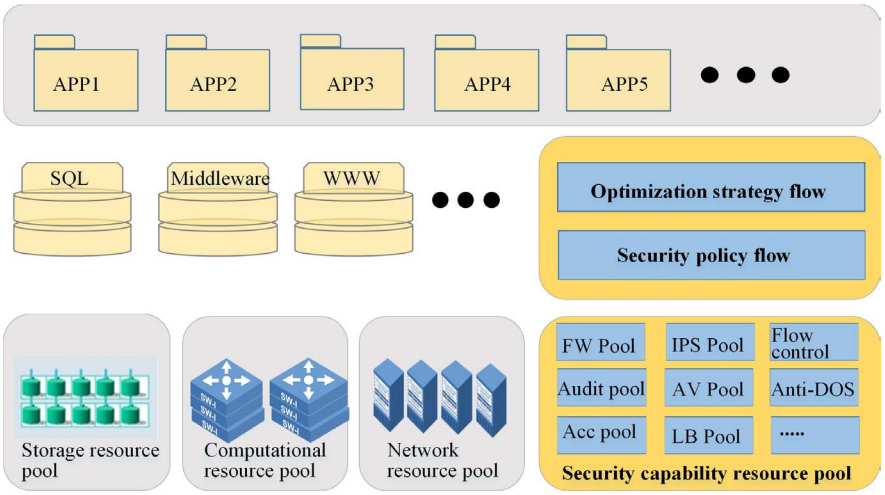



**Figure 3.** Security resource pool.

security pool through virtualization technologies virtualize multiple host into one logical fabric as well as the fine-grained management of security matters through virtualize one logical fabric into multiple host. The construction of a security pool is not limited to the aggregation of board cards which are with homogeneous functions on the same device, but also enables performance consolidation of multiple physical devices. According to different requirements on application, the security pool is committed to personalized resource allocation in terms of relevant security performance, and then provide virtualize one logical fabric into multiple host.

### 3.3. Application of VXLAN Technology in Virtual Machine Security

In the campus security protection for cloud platform, one of the fatal technical problems to be solved by cloud platform security protection is how to deal with the security protection of horizontal flows among virtual machines well and reduce mutual impact. Besides, realizing the continuous effectiveness of security protection strategy during the process of virtual machine's drift does likewise. After the relative research and exploration, a new method of providing security discovery and separation for virtual machines has been found--VXLAN (Virtual Expandable LAN) technology.

VXLAN is a technology model in virtualization which is superimposed on the network architecture. In addition to enabling massages of two-layer to transmit at three-layer network, the number of VLAN supporting increases in a size of geometric series. While meeting the needs of cross-network, it can provide adequate virtual segment support for large-scale, ultra-large-scale data center, so as to make network security protection for a single virtual machine available [14] (**Figure 4**).

The functions of the two-layer gateway and three-layer gateway are both available in VXLAN technology. The corresponding conversion between the VLAN and the VXLAN requires a two-layer gateway to support. The function of

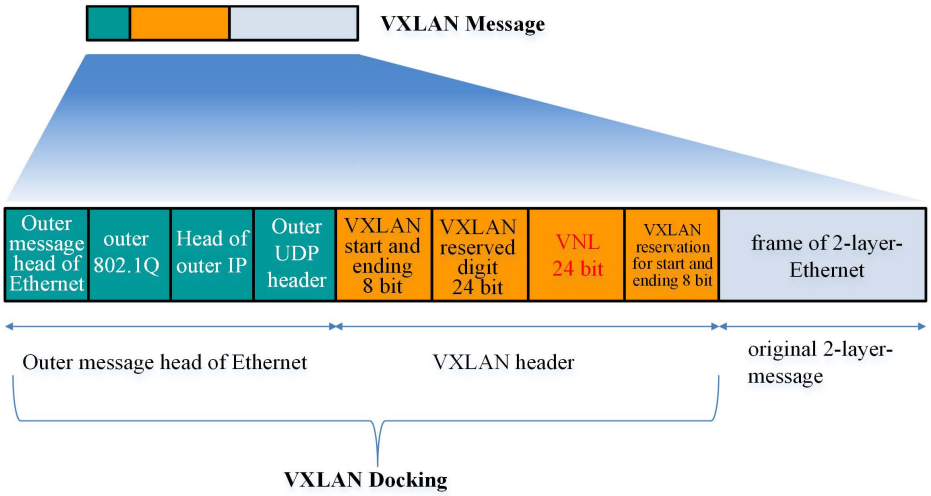



**Figure 4.** VXLAN message structure diagram.

three-layer gateway plays an important role in security for cloud platform and the second-layer gateway can't realize the transmission of the cross-VLAN. The transmission between VXLAN must be achieved through the three-layer gateway function, and the precondition for it is to encapsulate the VXLAN message header before transmission. Of course, the VXLAN gateway can't solve all the problems, until extensive support to VXLAN by means of relevant security devices has come true. All above can meet the rest needs of outer network layer (**Figure 5**).

The encapsulation and unblocked process of for VXLAN message transmission is achieved through VTEP (VXLAN Tunnel End Point), during which the virtual machine needs to encapsulate the secondary message for the sake of security. Therefore, the VTEP function of both ends in virtual switch needs to be in power-up at the same time, sending the secondary message to the other end of the switch by encapsulating the secondary message. After receiving the message, the other end unseals it, and transmit it according to the appropriate MAC address. If there's any need to transmit a three-layer message across VXLAN, it's available to use an all-in-one gateway device with VXLAN support, where the device must have both secure board and switched board. So as to further improve the security isolation issue among multi-renters, a complete VXLAN network needs to be built in a virtual machine and security gateway for control and management of the information transmission among virtual machines with different VXLAN [15] [16] [17].

### 3.4. Algorithm for Flows Traction Based on VXLAN Technology

Encapsulation and unblocking during the process of VXLAN message transmission can be realized through VTEP (VXLAN Tunnel End Point). VTEP can be an independent physical device or the server where the virtual machine is located at, and then the second-layer message of virtual machine will calculate before the process of transmission. Calculation will be conducted to subnet mask

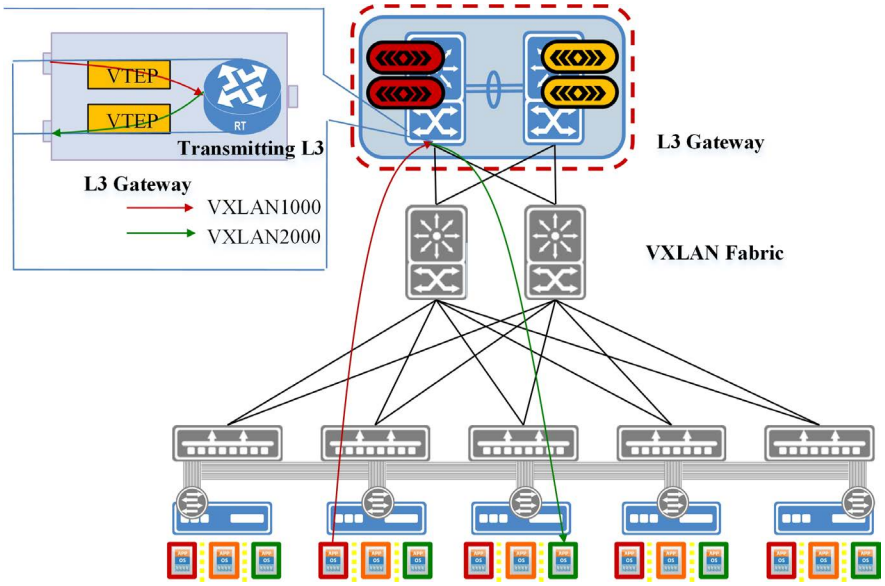



Figure 5. Schematic diagram of gateway on the third floor.

of the destination IP address' original one, if the calculation result is the same, the two IP addresses will be in the same subnet [15].

The calculation process for flows traction based on VXLAN technology as shown in Figure 6. Next, the article will be described in detail with examples of the computation process.

For instance: original IP address is 192.168.1.9 and subnet mask is 255.255.255.0; destination IP address is 192.168.1.10 and its subnet mask is 255.255.255.0. Calculation will be conducted with the addresses above, and then the decimal IP address will be switched into binary ones. The specific process, as shown in the table below:

Source IP address: 11000000.10101000.00000001.00001001
Subnet mask: 11111111.11111111.11111111.00000000
Destination address: 11000000.10101000.00000001.00001010
Subnet mask: 11111111.11111111.11111111.00000000

AND operation:
11000000.10101000.00000001.00001001
11111111.11111111.11111111.00000000AND
11000000.10101000.00000001.00000000
11000000.10101000.00000001.00001010
11111111.11111111.11111111.00000000AND
11000000.10101000.00000001.00000000

The result is identical, then two IP addresses in the same segment of internet can operate communication. If the result—gateways are not consistent with each other, then communication will be conducted in different segments of internet. This article focuses on the principle of communication and traction between different VXLAN (Figure 7).

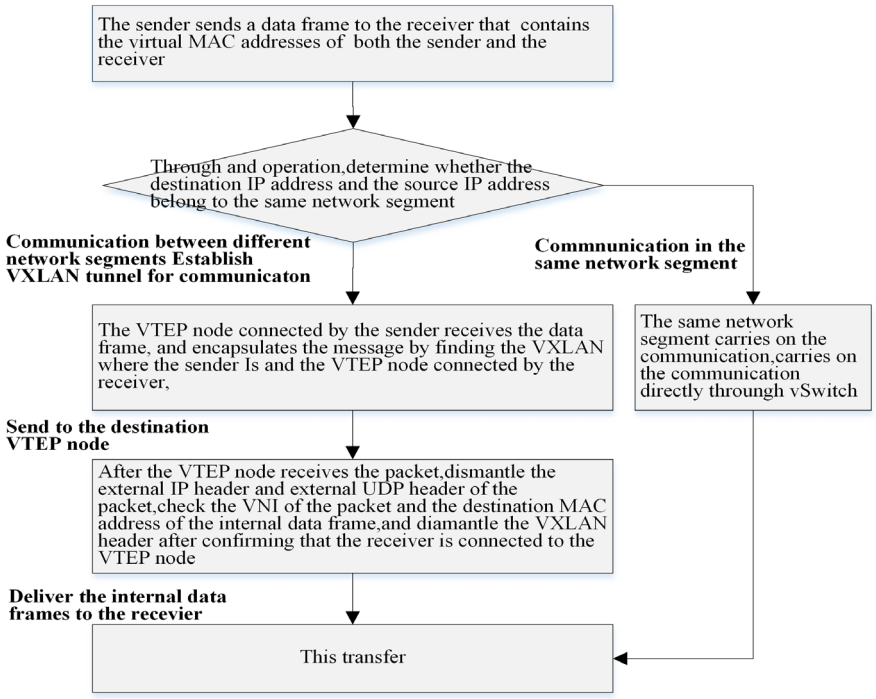



Figure 6. VXLAN operation flow chart.

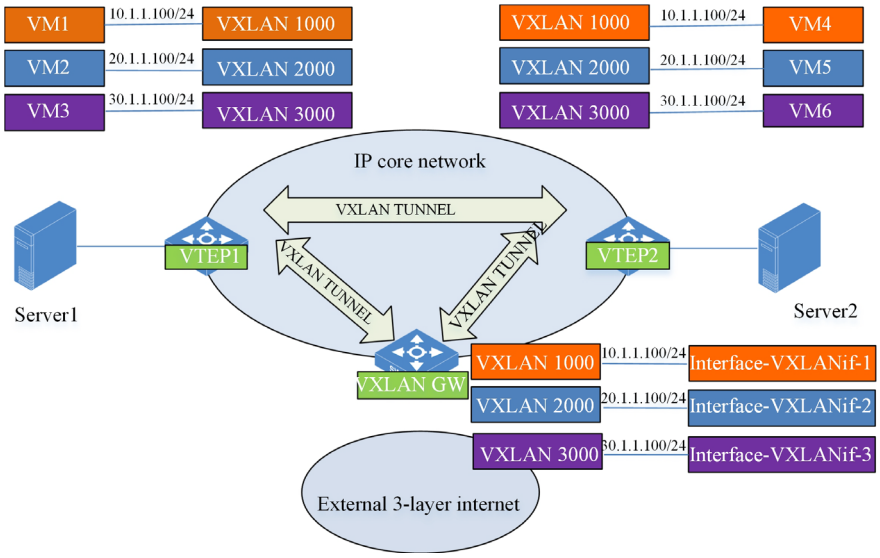



Figure 7. VXLAN communication traction schematic diagram.

1) When virtual machine VM 1 (IP 10.1.1.100) communicates in 3-layer across the network segment, the MAC address of the three-layer gateway (IP 10.1.1) will be requested by sending ARP for VXLAN 1000 in format of broadcasting at first.

2) After Receiving the ARP request, VTEP 1 adds the encapsulation of VXLAN and sends it to all remote VTEP.

3) When VXLAN's message has been received and unsealed by VXLAN GW and after learning the destination IP address (10.1.1.100) of the ARP request, respondence of ARP will be forwarded to virtual machine vm1.

4) When VTEP 1 receives answering message from ARP, the message will be transmitted to the virtual machine.

5) The virtual machine sends the encapsulated VXLAN message containing the gateway address of MAC to VXLAN GW via the VXLAN tunnel.

6) VXLAN GW unseals the VXLAN message and after removing the head of link layer, three layers of the inner IP message have been transmitted and sent to the node of the final external network.

Through the calculation, a complete VXLAN drainage system has been formed, which enables the scheduling of flows among multi-renters [18] [19] [20].

### 3.5. Realization of Virtualization Security

The experiment in this study is based on Huawei cloud platform in our university and the DiPu Deep Secure Business Gateway, which supports VXLAN and virtualization functions. Huawei's cloud platform consists of 3 control nodes, 6 computing nodes and 4 distributed storage units, with a virtual source of calculation for CPU of 480 cores, 1.5T in memory and 288T in storage resources. DiPu Deep business routing switching gateway, is specifically designed for the cloud platform data center, introducing engine and switching network separation technology (CLOS framework), with 64T switching capacity, 18 expansion slots. It also supports 100G cloud ports and package forwarding rate is at 23,040 Mpps. The whole machine security processing capacity is at 3.2 Tbps. All the advantages above can contribute to achieve high performance, and when the engine switches, zero packet of data can be achieved.

In the experiment, regarding the access among different virtual machines within the same business system, such as web, middleware, and database servers, access control permissions will be set according to the security management requirements. Because these virtual machines belong to the same application and the primary VLANs are identical, so they can communicate with each other on the second tier of traffic. In the security policy deployment, for the sake of achieving the two-tier isolation between each other, all the web, middleware and virtual machines of database should be taken into the isolation of The VLAN. Setting up ARP agent in the multi-service integrated security gateway, so as to enable all the web, middleware, database communication to go through the integrated security gateway for multi-service. Realization on flexible matching security resources according to business security needs will be available by means of focusing on planning security strategies in terms of source IP, purpose IP, physical interface.

In order to further improve the application experience of Huawei's cloud platform, we also conducted a test on a centralized scheduling and management of the DiPu virtualization security gateway by Huawei Cloud Tube Platform in our experiment. Huawei Cloud provides Cloud Fabric all-in-one cloud network virtualization scenario and VXLAN security gateway which can be perfectly dealt through Huawei NSH business chain technology. Meanwhile, network environment docking, security strategies, NSH business chain, high reliability and other

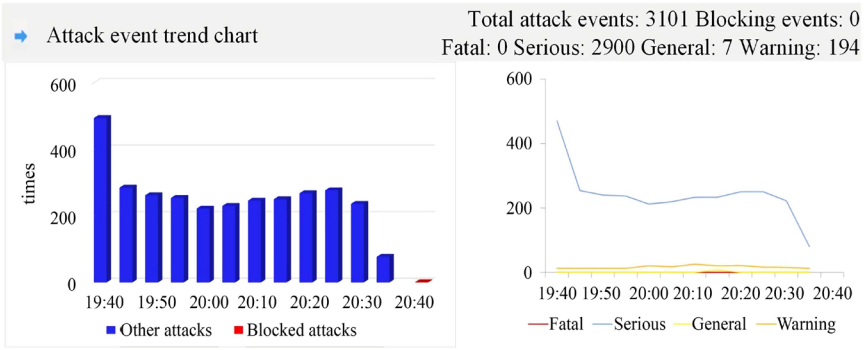



**Figure 8.** Attack incident statistics.

core functions docking capabilities also can be achieved. Moreover, this operation can live out intelligent network operation and maintenance, to provide users with easy-to-use, safe and reliable network environment.

### 3.6. The Implementation Effect of Virtualization Security Protection

Through the running test of the on-the-spot network environment, it is found that the security protection effect based on hardware VXLAN technology is good. The current statistics of device interception attack events are as follows Figure 8.

Since the start of the online test, there have been 3101 security gateway consensus attacks, including 2900 dangerous level serious incidents. The test results are significant, and the security protection ability meets the security protection needs of the data center.

## 4. Conclusion

Based on virtualization technology, the horizontal traffic security system of data center cloud platform can realize the flexible expansion of security gateway function and performance through virtual pooling of integrated security business gateway. Meanwhile, the system may overcome single point failure once it happened to the traditional security gateway equipment. All of this makes it possible to carry out personalized security protection resource allocation. Through VXLAN technology, to achieve minimum grain-size isolation of virtual machine is available. Meanwhile, drawing the virtual machine's horizontal flows in unification to an independent security gateway for processing, without affecting the performance of computing resources, which also achieves a fine management to the virtual machine security. With the help of a perfect connection by Huawei NSH business chain technology, the integrated management of virtual security gateway by cloud platform can be realized, and which will be more efficient and better experienced. The horizontal traffic protection model based on virtualization technology will be popularized and applied more and more in the security protection in school data center.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References


[1] Liu, J.Q. (2017) Research on Security Risks and Protective Measures of Server Virtualization. *Computer Knowledge and Technology*, **13**, 33-35.

[2] Tang, L., Li, W., Yan, R.J. and Song, L. (2014) Security Protection under Server Virtualization Environment. *Electronic World*, No. 7, 163-164.

[3] Chen, Y.P. (2014) Analysis of Security Protection in Virtualized Environment. *Computer CD Software and Applications*, **17**, 181-182.

[4] Huang, Y.X. (2017) Cloud Computing Platform Security System and Security Countermeasures. *Science and Technology Innovation Herald*, **14**, 127-128.

[5] Jiang, D.J. (2018) Research on Security Technology Based on Cloud Computing. *Computer Programming Skills & Maintenance*, No. 5, 164-165+170.

[6] Huang, Y.H. (2018) Design and Research of Cloud Platform Safety Protection in Smart Campus: A Case Study of Wuxi Institute of Technology. *Journal of Huainan Vocational & Technical College*, **18**, 67-68.

[7] Pang, Z.Y., Sun, N. and Pan, Y.Q. (2019) Cloud Computing and Security Technology. *Information Recording Materials*, **20**, 96-97.

[8] Fan, P. (2019) Research on Network Security Technology in Cloud Computing Environment. *Digital Communication World*, No. 9, 107.

[9] Chi, E.Y., Wang, D. and Yang, Y.Z. (2015) Network Security and Protection. Higher Education Press, Beijing.

[10] Liu, N.N. (2017) Cloud Computing Security: Research on Architecture, Mechanism and Model Evaluation. *Digital Communication World*, No. 12, 240.

[11] Che, J., Duan, Y., Zhang, T., *et al.* (2011) Study on the Security Models and Strategies of Cloud Computing. *Procedia Engineering*, **23**, 586-593. https://doi.org/10.1016/j.proeng.2011.11.2551

[12] Liao, F., Chen, J. and Xiao, Y.F. (2019) Cloud Computing Security Architecture and Protection Mechanism. *Communications Technology*, **52**, 2472-2482.

[13] Geng, Y.J., Wang, J. and Zhou, H.L. (2019) Research of Network Defense in Depth of Cloud Data Center. *Information Security and Communications Privacy*, No. 7, 22-29.

[14] Wen, X.M. (2018) Research and Application of VXLAN in Data Center Network. *Information Technology and Informatization*, No. 7, 120-122.

[15] Li, X. (2015) A Cloud Datacenter Solution Based on SDN and VXLAN. *Electronic Science & Technology*, **2**, 587-592.

[16] Xu, F. and Sun, W.Y. (2017) The SDN Based Could Data Center Design of the Colleges and Universities. *Computer Knowledge and Technology*, **13**, 46-48+54.

[17] Tan, Q.F. and Lu, X.X. (2017) A Network Solution in Cloud Data Center Based on SDN. *Telecom Engineering Technics and Standardization*, **30**, 25-28.

[18] Zhang, X.Y. (2016) Flow Schedling Optimization for Data Center Networks. Huazhong University of Science and Technology, Wuhan.

[19] Wang, Y.J., Zhang, J., Zhang, F.G., *et al.* (2017) VXLAN-Based Network in Cloud Data Center. *Communications Technology*, **50**, 78-83.

[20] Ma, S.L. and Li, S.Q. (2019) Study on Campus SDN Network Construction Technology Based on Overlay and VXLAN. *Proceedings of the* 23*rd Annual Meeting of Network New Technology and Application of China Computer Users Association in* 2019, Anhui, 309-312.