基于 NSX 的数据中心零信任网络建设

叶瑞哲　沙锋
（厦门理工学院　福建厦门　361024）

摘　要　本文以厦门理工学院数据中心为例，介绍了零信任网络模型在数据中心的部署应用情况。主要以虚拟机为最小单位，应用VMware NSX和SDN的技术实现了南北流量和东西流量的按策略全隔离，提升了数据中心的安全等级。主要思想是以零信任网络模型为蓝本，根据高校本身的特点，对安全设备、体系架构、规则规范进行了重新梳理和调整。

关键词　NSX；SDN；数据中心

Research on Construction of Zero Trust Network in Data Center Based on VMware NSX

Ye Ruizhe　Sha Feng
（Xiamen University of Technology, Xiamen, Fujian, 361024,China）

Abstract　This article takes the data center of Xiamen University of Technology as an example to introduce the deployment and application of the zero-trust network model in the data center. The application of VMware NSX and SDN technology to virtual machines as the smallest unit has achieved full isolation of north-south traffic and east-west traffic according to policies, which has improved the security level of the data center. The main idea is based on the zero-trust network model, and reorganized and adjusted the security equipment, system architecture, rules and regulations according to the characteristics of the universities themselves.

Keywords　NSX；SDN；Data Center

1　引言

高校数据中心承载了全校的信息化数据，数据之间的快速交互需求必然带来数据的快速流向。高校云数据中心的兴起造成的数据大集中也使数据流量面临着爆炸性的增长。传统千兆网络早已被万兆网络所取代，甚至40G、100G的网络也逐渐成为主流。数据流量的增加也引发了很多检测和监控方面的问题，网络带宽的增加也使得一些非法流量或异常流量被隐藏在合法流量底下而不易被察觉，网络边界的

模糊化更是造成了你中有我，我中有你的复杂环境。传统网络中基于边界安全的模型逐渐暴露出它的局限性，数据的流向基本是固定的，设备之间的通路也基本以串行为主。为保证数据中心的安全，数据中心网络的安全防护也逐渐转向零信任安全模型。借助SDN及NSX的组合，将使流量过滤、清洗或迁移成为可能。零信任网络模型改变了数据中心的传统安全理念，使得应对现有的安全威胁更加得心应手。

2 零信任安全模型

2.1 边界安全模型

边界安全模型主要是通过部署防火墙、IPS和WAF等这些传统的边界安全产品，对校内的网络设备和业务系统进行防护。目前，大多数高校的解决方案都是基于边界网络安全。其指导思想是分区防御，包括一直提倡的设立DMZ区域也是一种，分层、分级保护的思想。但是这种理念只注重边界防护，一旦外部攻击者成功侵入网络内层的某一个单位，就享有该区域的所有权限，因为区域内是基本上不设防的。同时该方案极大影响了业务的连续性，例如邮件系统、财务系统等。其Web服务、数据库、统一身份认证分属于不同等级的安全区域。当数据通过区域边界时避免不了被误拦的情况发生，同时数据流量也因为多重过滤而变得缓慢。当有新业务上线时，因业务需要进行区域间互访时，就需要不断地增加安全策略，不断地开例外。这样一来逐渐打破了原有设计的安全分区，同时，防火墙等设备的规则也变得越来越复杂。

2.2 零信任安全模型

零信任最早是约翰·金德维格提出的一个安全概念，核心是数据中心内的任何单位不应自动信任内部或外部的任何人、设备和事件。任何需要与数据中心进行的访问都应对需要访问的人、设备和事件进行验证后才给予授权。总之，零信任网络的原则就是不相信任何人。除非网络明确知道接入者的身份，否则都拒绝访问。不管IP、主机、网络设备等，不知道用户身份或者不清楚授权途径的，全部拒绝。[1, 2]

2.3 零信任安全模型与边界安全模型的对比

两种安全模型是有着本质理念上的区别的。边界安全模型的理念是在内部网络与互联网之间建立一道或几道隔离墙。主要用于防护外部对内部的攻击，对内部的互访基本是信任的。而零信任模型则认为危险无处不在，不能依靠建立区域墙来进行防护，让每个独立体都有自我防护的能力，加强自身的健壮性。

3 高校数据中心面临的挑战

我校数据中心已逐渐趋向于多云环境。目前对外服务资源仍以虚拟机为主力，但容器、K8S等云原生应用日渐增多。同时，基于混合云的应用如网盘、网上办事大厅等带来的问题使得校内外环境的互访问题错综复杂。Linux开源技术及目前迅速发展的K8S应用是天生依靠互联网而生的，随之带来的就是私有云和公有云的界限逐渐模糊。一句话，我们的校园网已经不那么纯粹了，再不能像以往那样只在边界建立防火墙进行隔离防护了。数据中心的威胁逐渐从南北向防护转向为内部的东西向流量的安全，如果按传统的思路就需要部署多台传统防火墙进行阻隔过滤，这在实际环境中是不现实的，不仅资产成本高，而且管理成本也高。因此，数据中心按照零信任安全模型进行安全防护变得十分迫切。

4 零信任安全的数据中心建设

4.1 SDN 与 NSX 的结合

网络虚拟化融合了虚拟化与SDN（Software

Defined Network，SDN）技术，典型的应用场景为网络架构扁平化和多路径环境。SDN软件定义网络是由美国斯坦福大学Clean State课题研究组提出的一种新型网络创新架构[3]，是网络虚拟化的一种实现方式。其核心技术OpenFlow通过将网络设备的控制平面和数据平面分离开来，从而实现了网络流量的灵活控制，使网络作为管道变得更加智能，这点十分契合零信任安全模型的理念。另一种可以实现控制平面和数据平面分离的就是VMware NSX[4, 5, 6]。NSX可以在软件中实现整个网络架构，基本上任何网络拓扑，都可以在短时间内创建和调配，做到了网络的集中控制，系统性的可视、监控和管理。它支持一系列逻辑网络元素和服务，其分布式防火墙功能是构建零信任安全网络的核心。

4.2　零信任安全模型在数据中心的实现

现阶段我校部署零信任安全模型并不是颠覆原有整个设备和整个体系架构，而是尽量保护原有的信息资产投资，调整原有设备在网络中的位置和功能。经评估后仅增加必需的安全组件和设备，实现整体架构的平稳过渡，尽量减少对现行网络业务的影响。最终我校的零信任安全模型为“迪普边界防火墙+SDN+NSX+亚信防病毒”，实现了三层安全防护。迪普防火墙负责外部互联网区域与内网区域南北向流量的安全审计、防护和过滤；NSX与SDN网络配合实现东西向流量安全审计、防护和过滤；亚信防病毒负责虚拟机的防病毒安全。这套模型严格遵循数据平面与控制平面分离的思想。

我校数据中心现有的服务器，存储、交换设备共250余台。它们承载着全校的信息化系统，运行范围包括网站群、人事系统、学工系统、教务系统和财务系统等不同的业务系统，这些系统都存在着与校内或校外的数据交换。目前有部分设备已纳入零信任安全模型部

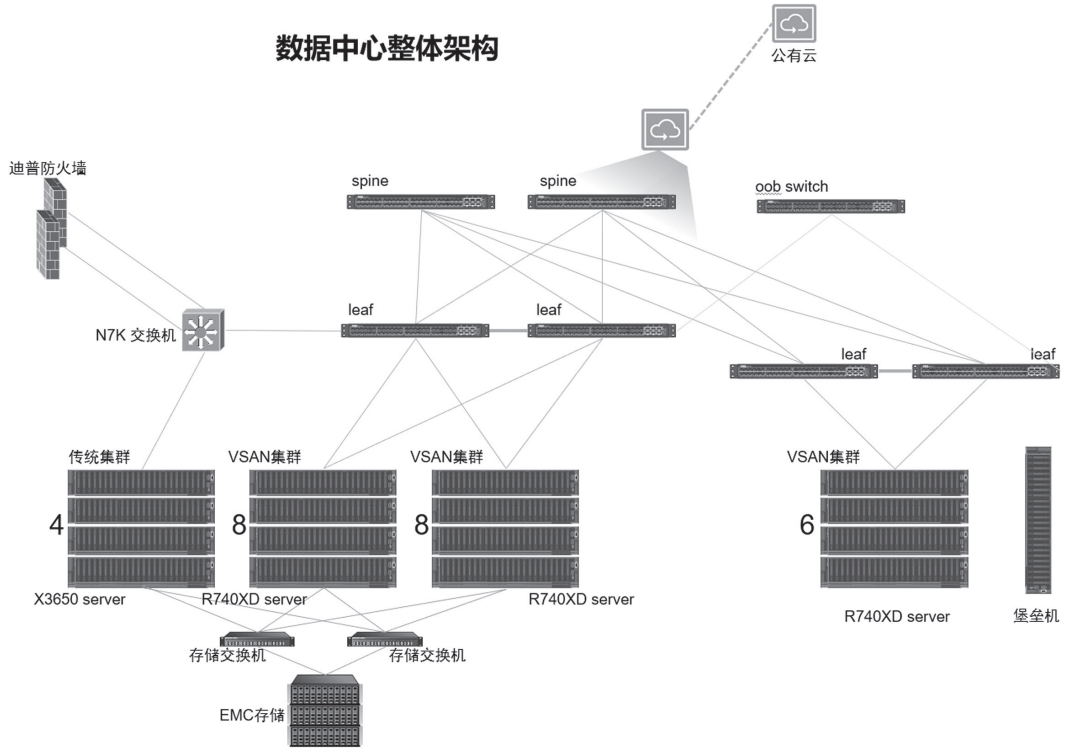

图 1　数据中心整体架构图

署，包括物理服务器26台，交换机10台和存储1套。虚拟化系统主要使用VMware vsphere虚拟化软件。学校目前以虚拟机为最小防护单元，同时，在未来保留容器环境下，配合容器网络可将最小防护单元设置为容器。

4.3 NSX 部署设计

数据中心新增的核心组件为VMware NSX。NSX所实现的一个最主要的功能就是主机防火墙，为了更有效地实现防火墙安全，需将主机防火墙与虚拟机解耦合，同时尽量靠近源。这样做有两个好处，一个是集中管理可以减少虚拟机对防火墙的误操作，增强主机防火墙的可靠性；另一个是避免无关流量进入网络，将非法流量阻挡在源头，减少网络带宽的损耗，特别是像DDOS这种对网络影响非常大的攻击手段。

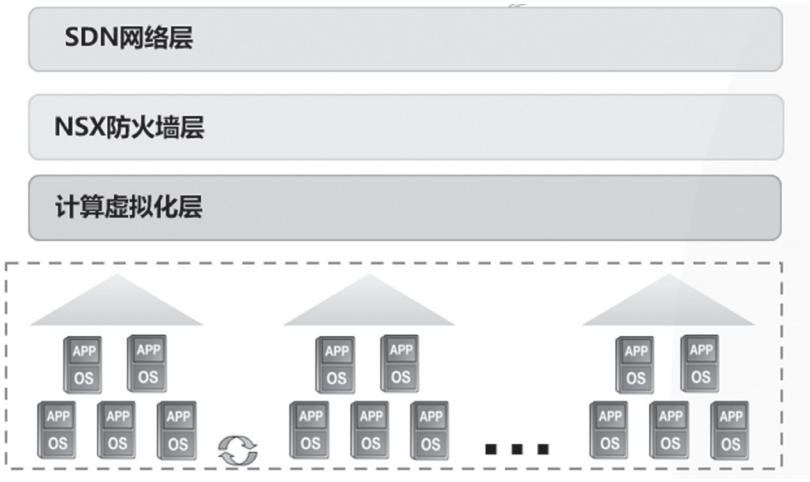

图 2　NSX 在数据中心的位置

图 3　NSX 配置范例

数据中心网络的一个关键危险点是同网段虚拟服务器间不受监督的互访。因此需解决让同网段之间的两台虚拟服务器在同网段不能无限制、无约束的互相访问的问题。一般黑客攻击都是先通过web传染恶意软件，所以web之间相互隔离可以达到提高安全性的目的。经研究表明，数据中心80%的流量都是东西向流量，包括web服务器与数据库之间，业务系统之间等。如果这部分流量不受监管和控制，会对数据中心造成安全隐患。我校采用的VMware NSX是VMware的网络虚拟化平台，可以过滤任何在虚拟网卡、SDN交换机中来往的流量。我校利用NSX分布式防火墙的可扩展性，在虚拟机之间创建了零信任安全。这个安全策略也可以在同一逻辑的二层网络上的主机之间创建。

基于VMware NSX的方法抽象了物理的零信任安全，同时使用基于虚拟化属性的分布式的网络覆盖。数据中心管理员可以在一个集中的关系系统中创建规则，未来边界防火墙策略下移到NSX防火墙后将可实现NSX防火墙的真正统一管理。NSX将可完全替代边界防火墙，而且可强制跨分布式防火墙设备。最终实现零信任网络防火墙集中管理的解决方案。

4.4 网络分析监控

我校数据中心使用流量采集平台，统一收集数据中心虚拟化集群流量，经过核心控制器聚合、筛选、过滤与复制，结合第三方分析平台，实现网络性能监控、安全分析、流量展示的功能[1]。从零信任安全网络的行动路线上来说，捕获现有数据中心网络中的所有流量是传统边界网络模型向零信任网络模型转变的首要解决的问题。通过对网络中的流量进行分类、筛选并长期记录以达到非侵入式的网络分析手段。通过分析可得知网络中存在何种类型的连接，存在何种网络协议，之间的占比如何，这将对现有网络迁入零信任网络提供科学的决策支持。这也将使从边界防火墙迁移至NSX防火墙所引发的网络不稳定性得到大大改善。

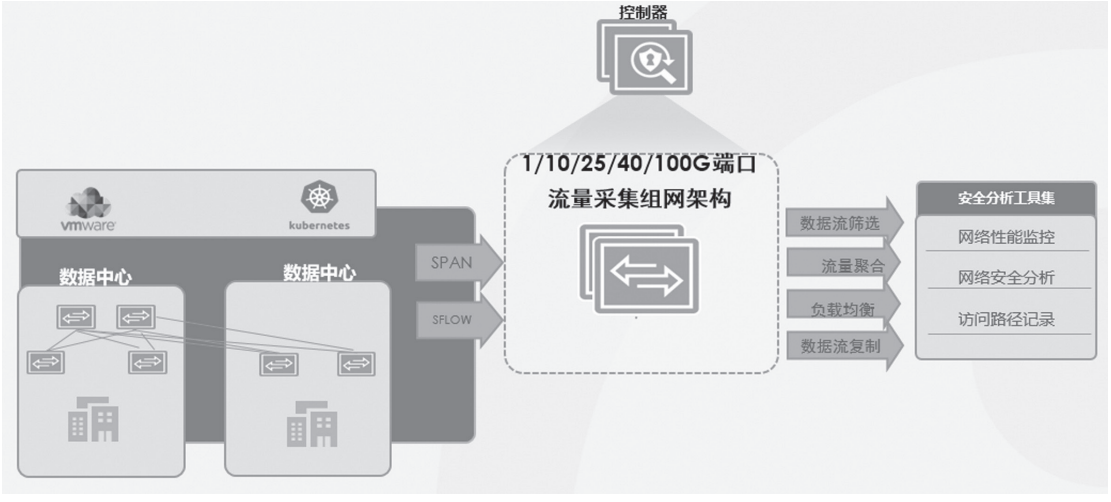

图 4　网络监控框图

5 结语

构建零信任安全网络不是简单的产品堆叠，其重要的核心是网络安全的理念和指导原则。零信任安全网络的构建过程不是一蹴而就的行为，是一点一滴逐步完善实现的。完整的零信任安全网络目前来说还是一个理想架构，刚启用时可根据所在高校自身的特点进行调整。零信任安全技术既是机遇又是挑战，作为网络安全的一个全新的解决方案，推动着信息社会的发展，逐步改变着信息使用者使用网络的行为和规范。在高等学校里构建合理的网络结构，可以满足教学科研的需求、提高信息化管理效率和质量。建设安全可信的高校信息化平台，对高校的发展有着重要的意义。

参考文献

[1] 埃文·吉尔曼，道格·巴斯.零信任网络在不可信网络中构建安全系统 [M]. 北京：人民邮电出版社，2019：161—163.

[2] 安全牛. “零信任”安全架构将成网络安全流行框架之一. [OL].

[3] 肖敏.云计算数据中心商用SDN方案比较分析 [J]. 绵阳师范学院学报，2019，38：2.

[4] 曹雅斌，苗春雨.网络安全应急响应 [M]. 北京：电子工业出版社，2020：91—92.

[5] 刘宇.基于VMware NSX技术在民航某单位虚拟化平台的优化 [J]. 电子技术与软件工程，2019 (16)：24—25。

[6] 李刚.基于NSX的高校数据中心网络虚拟化应用 [J]. 网络安全技术与应用，2016 (10)：32—33.