虚拟网络技术在计算机网络安全中的应用策略研究

王松滨
湖南司法警官职业学院

摘　要：计算机网络安全中的虚拟网络技术是一种在物理网络之上构建的逻辑网络，它通过在物理网络上划分多个虚拟网络，实现对网络资源的隔离和保护。虚拟网络技术可以在不改变物理网络结构的情况下，为用户提供更加灵活、安全和可管理的网络环境。基于此，文章将围绕虚拟网络技术在计算机网络安全中的应用意义与原则，对具体的应用策略进行研究。

关键词：计算机网络安全；虚拟网络技术；应用
【DOI】10.12252/j.issn.2096-627X.2023.06.118

引言

随着互联网技术的飞速发展，计算机网络已经成为现代社会生活、工作和学习的重要组成部分。然而，随着网络的普及和应用，网络安全问题也越来越突出。网络攻击、病毒、恶意软件等网络威胁不断涌现，给计算机网络安全带来了严重的挑战。在这样的背景下，虚拟网络技术应运而生。虚拟网络技术是一种在物理网络之上构建的逻辑网络，它通过在物理网络上划分多个虚拟网络，实现对网络资源的隔离和保护。

一、虚拟网络技术在计算机网络安全中的应用意义

（一）提高数据传输的安全性以及实现网络的隔离和划分

通过虚拟网络技术，可以建立起专用通道，对数据传输进行加密，确保数据在传输过程中不易被截获和破解，从而提升数据传输的安全性。同时，虚拟网络技术能够实现网络资源的逻辑划分和物理隔离，不同网络之间可以独立运作，将能够更好地防止网络间的干扰和攻击，增强了网络的稳定性和可靠性。

（二）增强网络的访问控制以及灵活适应网络需求变化

一方面，利用虚拟网络技术，可以实现对网络访问的严格控制，仅允许授权用户和设备访问特定的网络资源，有效防止未授权访问和网络攻击。另外一方面，虚拟网络技术可以根据实际需要动态调整网络资源，快速适应业务量的增减和网络需求的变化，提高网络的灵活性和可扩展性[1]。

（三）降低网络构建维护成本以及提供多样化的安全服务

通过虚拟化技术，可以在不增加物理硬件的情况下扩展网络资源，有效降低了网络构建和维护的成本。同时，虚拟网络技术支持多种安全服务，例如，防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等，为网络提供全面的安全保护。

（四）支持远程访问以及促进云计算和大数据的发展

一方面，虚拟网络技术使得远程访问和移动办公变得更加安全和便捷，通过VPN等技术，可以确保远程用户和移动设备安全地接入企业网络。另外一方面，在云计算和大数据时代，虚拟网络技术为数据中心的构建和管理提供了高效、安全的解决方案，有助于促进这些新兴技术的健康发展。

二、虚拟网络技术在计算机网络安全中的应用原则

（一）合规性与最小权限的原则

确保所有虚拟网络技术的应用都符合相关的法律法规和行业标准，包括数据保护法规、隐私保护法律以及网络安全法规等。同时，在虚拟网络中，应该遵循最小权限原则，即用户和程序只能获得完成其任务所必需的最小权限，有助于减少潜在的内部威胁和权限滥用。

（二）分层安全和网络隔离的原则

通过在虚拟网络中实施分层安全措施，例如，物理安全、网络安全、数据安全和应用程序安全，以提供多层次的保护。特别是在虚拟网络设计中，应该实现网络隔离，以防止不同网络之间的数据泄漏和攻击传播。这包括在虚拟网络内部实现逻辑隔离和在不同虚拟网络之间实现物理隔离。

（三）加密性与身份验证的原则

对于敏感数据传输，应使用强加密算法来保护数据不被未授权访问。这包括对虚拟网络中的数据传输进行端到端加密。确保所有访问虚拟网络的用户和设备都经过严格的身份验证和授权。使用多因素认证可以增强安全性[2]。

（四）深度防御与持续监控的原则

一方面，通过在虚拟网络的不同层次实施安全措施，包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等，以提供深度的防御。另外一方面，对虚拟网络进行持续的监控和日志记录，以便及时检测和响应安全事件和异常行为。

三、虚拟网络技术在计算机网络安全中的应用策略

（一）虚拟专用网络（VPN）

虚拟网络技术，尤其是虚拟专用网络（VPN），在计算机网络安全领域扮演着至关重要的角色。首先，建立安全连接。VPN技术可以创建加密的隧道，确保数据在传输过程中的安全性。当数据通过VPN连接传输时，它会经过加密处理，防止潜在的黑客或拦截者读取或篡改数据。这种加密方法保护了数据的机密性和完整性，无论是在有线还是无线网络环境中。其次，认证和授权。VPN可以实施强大的认证机制，包括密码、证书或生物识别技术，以确保只有经过授权的用户才能访问网络资源，进而防止未授权访问和潜在的安全威胁。此外，VPN还可以根据用户的身份和权限来限制对特定资源的访问，从而提供更细粒度的安全控制。最后，网络隔离。VPN技术可以在不同网络之间建立隔离，保护内部网络不受外部网络的威胁。通过将内部网络与外部网络隔离，VPN可以防止外部攻击者直接访问内部网络资源。这种隔离还可以防止内部网络中的敏感数据泄漏到外部网络，从而提供更高级别的安全保护[3]。

以“远程办公中的VPN应用”为例，假设一个公司有许多远程工作人员，他们需要从家中或移动地点安全地访问公司的内部网络资源。为了确保数据的安全和隐私，公司决定使用VPN技术来建立安全的远程连接。首先，公司为每位远程工作人员提供了VPN客户端软件，并设置了强密码和/或证书认证机制。工作人员在远程设备上安装VPN客户端并输入认证信息，建立起与公司内部网络的安全连接。当工作人员通过VPN连接访问公司网络时，数据传输过程中会经过加密处理。这意味着即使数据在传输过程中被拦截，拦截者也无法读取或篡改数据，因为数据是加密的。这样，公司的敏感信息，例如，客户数据、财务报表和商业计划等，都能得到充分保护。最后，VPN技术在远程工作人员和公司内部网络之间建立了隔离。这意味着外部网络无法直接访问公司内部网络资源，从而保护了内部网络免受外部威胁。同样，内部网络中的敏感数据也无法泄漏到外部网络，进一步增强了安全性。

（二）软件定义网络（SDN）

软件定义网络通过将控制平面（决定数据如何流动）与数据平面（实际转发数据包）分离，带来了网络管理的革命。第一，在SDN架构中，网络流量管理是通过一个集中的控制器来完成的。这个控制器负责制定网络流量的路由和转发策略。这种集中化的控制机制使得网络管理员能够更有效地实施安全策略，因为所有的安全决策都集中在一个地方。集中控制器可以提供更细粒度的安全控制。第二，SDN通过抽象化网络资源，包括交换机、路由器和防火墙，使得网络管理员可以在更高的层面上制定和执行安全策略。第三，SDN的动态性意味着网络流量和路径可以根据实时条件进行调整。这种能力对于应对安全威胁和漏洞至关重要[4]。

以“数据中心中的SDN应用”为例，假设一个大型数据中心需要管理大量的服务器和网络设备，以确保数据的安全和高效流动。为了提高网络的安全性和管理效率，数据中心决定采用软件定义网络（SDN）架构。首先，通过集中控制器，数据中心管理员能够更有效地实施安全策略。例如，他们可以根据用户身份、设备类型或数据内容来决定是否允许网络流量通过。此外，集中控制器还可以实时监控网络活动，快速响应潜在的安全威胁。其次，数据中心中的交换机、路由器和防火墙等网络设备被抽象化，使得管理员可以在更高的层面上制定和执行安全策略，意味着管理员不必担心底层硬件的具体细节，而是可以专注于建立和维护安全规则。例如，SDN可以允许管理员定义一个安全区域，并自动地将相应的安全策略应用到网络中的所有相关设备上。这种抽象化提高了安全策略的灵活性和可扩展性。最后，如果SDN控制器检测到某个网络设备受到恶意软件的感染，它可以立即调整网络流量，将该设备隔离，防止恶意流量传播到其他网络部分。同样，如果某个安全漏洞被发现，SDN可以迅速更新安全策略，确保网络流量不会经过易受攻击的路径。通过采用SDN架构，数据中心能够实现更细粒度的安全控制、灵活的安全策略制定和执行，以及实时响应安全威胁和漏洞的能力。

（三）网络功能虚拟化（NFV）

网络功能虚拟化（NFV）通过将传统的网络功能（如防火墙、入侵检测系统/入侵防御系统（IDS/IPS）等）虚拟化，带来了网络架构的革新。首先，NFV通过虚拟化传统的网络功能，提供了更灵活的安全部署选项。这意味着网络功能不再依赖于专用的硬件设备，而是可以以软件的形式运行在标准服务器上。这种虚拟化的网络功能可以快速部署、升级和扩展，从而提供更高的灵活性和可伸缩性。其次，NFV支持网络资源的池化，使得安全资源可以根据需求进行动态分配和扩展。在NFV环境中，网络资源（如带宽、虚拟网络功能实例等）被集中管理，并可以根据实际需求进行分配和调整。最后，通过整合SDN的集中控制和NFV的虚拟化网络功能，企业可以建立更加强大和灵活的安全架构。

以“某大型企业网络架构升级”为例，某大型企业拥有复杂的网络架构，面临着日益严峻的网络安全威胁。为了提高网络安全性、灵活性和可扩展性，企业决

定采用网络功能虚拟化（NFV）技术对网络架构进行升级。首先，企业将传统的网络功能虚拟化，使其以软件形式运行在标准服务器上，提高安全防护能力。例如，在面临安全威胁时，企业可以迅速部署额外的防火墙实例，而不需要购买额外的硬件设备。其次，通过NFV技术实现网络资源的池化。网络资源（如带宽、虚拟网络功能实例等）被集中管理，并根据实际需求进行动态分配和扩展，确保网络安全的弹性和可扩展性，提高资源利用率。最后，企业将NFV技术与软件定义网络（SDN）技术相结合。通过整合SDN的集中控制和NFV的虚拟化网络功能，企业建立了更加强大和灵活的安全架构。SDN控制器可以实时监控网络流量和威胁，并根据需要动态调整虚拟网络功能的配置和位置，以应对安全威胁和漏洞[5]。

（四）虚拟化云网络（VCN）

VCN通过虚拟化网络资源和安全服务，为云环境提供了一种高效的安全架构。一方面，VCN允许在云环境中构建安全网络，这些网络可以是跨越不同地理位置的虚拟网络。通过虚拟化技术，VCN可以在物理网络之上创建多个隔离的网络环境，每个环境都可以拥有独立的安全策略和控制措施，使得安全措施可以根据不同业务需求和应用场景进行优化。另外一方面，VCN支持多层次的安全策略，进而覆盖了网络层、传输层和应用层。

以“某电商平台的安全架构升级”为例，为了保护用户数据和交易安全，平台首先构建了一个基于VCN的云安全架构，该架构包括虚拟化的防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）和分布式拒绝服务（DDoS）防护。这些虚拟化的安全设备和服务可以根据需要动态扩展和收缩，以适应不断变化的业务需求。接着，平台实施了多层次的安全策略。在网络层，通过设置精细粒度的ACLs和防火墙规则来控制进出网络的流量。在传输层，使用SSL/TLS加密来保护用户数据在传输过程中的安全。在应用层，集成了WAF来防止SQL注入、跨站脚本（XSS）等常见的Web攻击。

（五）微分段

微分段通过在网络内部创建更小的、更可控的子网来提高网络的安全性。这种技术有助于限制攻击的扩散和影响，同时可以更精确地控制访问权限。一方面，微分段通过在网络内部创建逻辑上的边界，将网络划分为更小的区域。这些区域可以是基于物理位置、网络功能、业务需求或其他标准。另外一方面，微分段技术可以帮助实施更精确的访问控制策略。通过定义每个子网的访问权限，可以确保只有授权的用户和设备能够访问特定的网络资源，有助于减少潜在的内部威胁[6]。

以“某金融机构的网络微分段实施”为例，该机构拥有多个业务线和大量的网络设备，包括服务器、工作站、移动设备等。首先，金融机构的网络团队对其网络进行了细分，基于业务需求和物理位置，创建了多个子网。例如，交易处理系统被放置在一个独立的子网中，而客户服务系统则在另一个子网中。这样，即使交易处理系统受到攻击，客户服务系统仍然可以正常运行，不会受到影响。接着，网络团队实施了精确的访问控制策略。每个子网都有一套独立的访问控制列表（ACLs），定义了哪些用户和设备可以访问该子网中的资源。此外，对于移动设备和非固定工作站，采用了802.1X身份验证来确保只有授权用户才能接入网络。通过实施微分段，该金融机构显著提高了网络安全性。攻击的扩散被有效限制，内部威胁也得到了有效控制。此外，由于访问控制更加精确，员工的操作权限得到了明确界定，减少了潜在的内部滥用风险。总体而言，微分段技术帮助该金融机构建立了一个更加安全、可控的网络环境。

三、结语

总的来说，虚拟网络技术在计算机网络安全中的应用，不仅提升了网络安全防护能力，还提高了网络资源的利用效率和灵活性，对于保障网络信息安全、推动网络技术发展具有重要作用。遵循上述原则，组织可以更有效地利用虚拟网络技术来增强计算机网络安全，减少安全风险，并确保业务连续性。

参考文献

[1]李强.计算机网络安全应用虚拟网络技术的研究[J].软件，2022，43（12）：174-176.

[2]宋尊锋.浅析计算机网络安全中虚拟网络技术的作用[J].网络安全技术与应用，2022（09）：25-27.

[3]王华永.计算机网络信息安全中虚拟专用网络技术的应用[J].黑龙江科学，2022，13（14）：106-108.

[4]巴根.浅谈计算机网络安全中虚拟网络技术的作用效果[J].科技风，2022（18）：52-54.

[5]阿迪娅·扎曼别克.计算机网络安全中虚拟网络技术的应用研究[J].中国设备工程，2022（12）：189-191.

[6]许镭.虚拟网络技术在计算机网络安全中的应用[J].网络安全技术与应用，2022（06）：33-34.

作者简介：王松滨，1970-9，女，汉，河北正定人，大学本科，讲师，计算机网络。