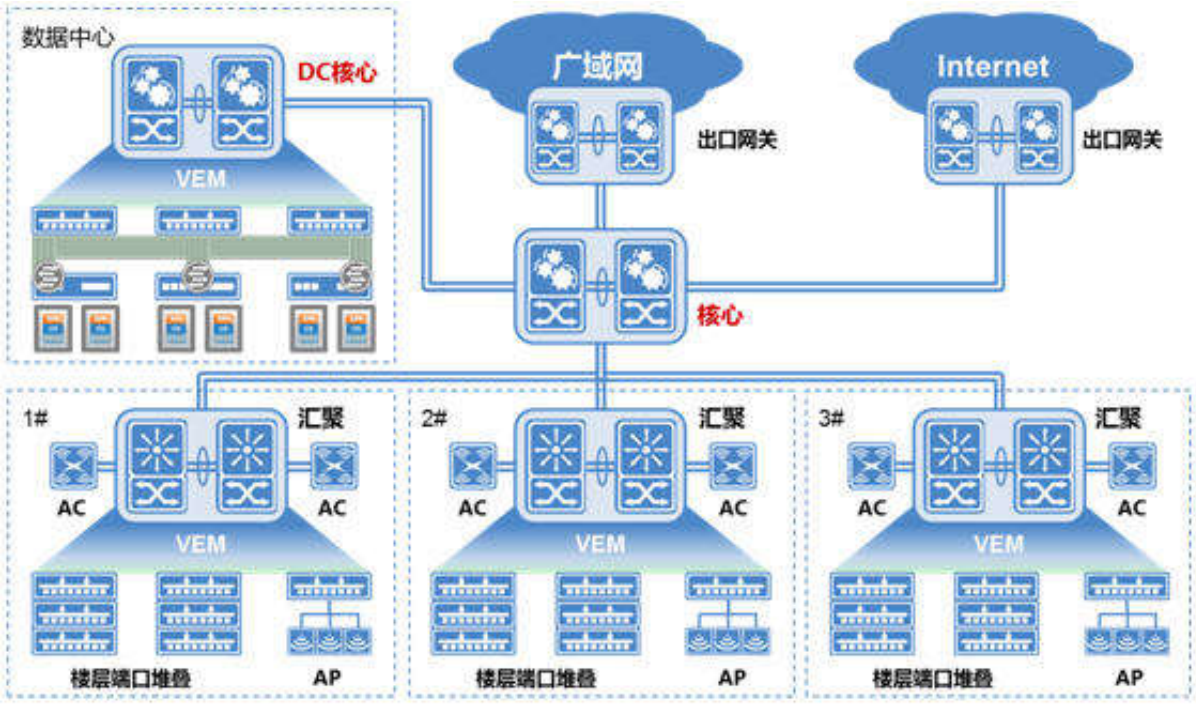
DP xCampus安全虚拟园区网解决方案

迪普科技凭借自身的技术积累以及对于应用的理解，推出了DP xCampus安全虚拟园区网解决方案。DP xCampus安全虚拟园区网解决方案立足于园区网的建设目标和建设需求，结合迪普科技领先的“应用即网络”技术理念和技术实现，为用户提供简单、智能、可靠的安全虚拟园区网建设方案。

DP xCampus安全虚拟园区网解决方案框架如下图所示：



DP xCampus安全虚拟园区网解决方案框架

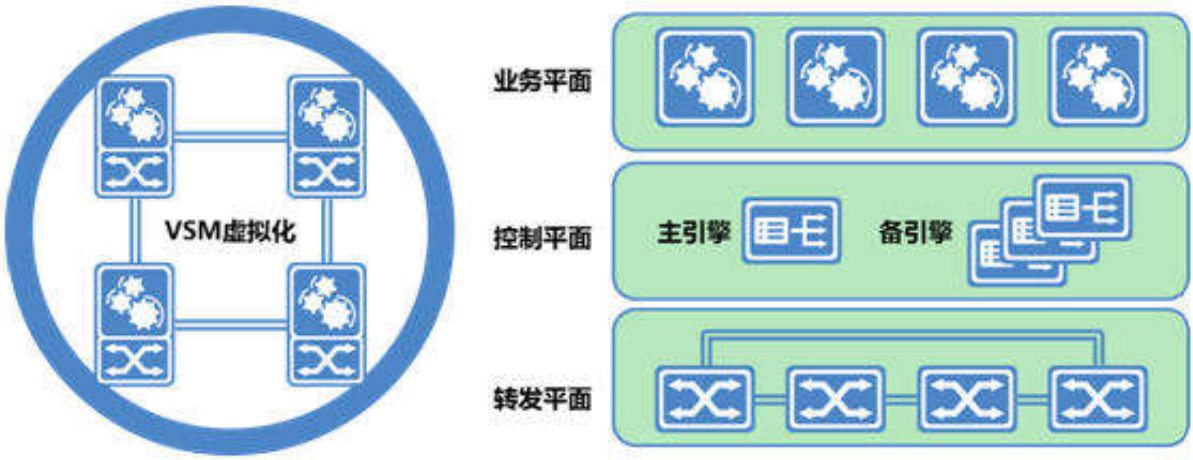
DP xCampus安全虚拟园区网解决方案提供虚拟化基础架构，通过VSM虚拟交换矩阵技术和VEM虚拟扩展矩阵技术将每个二层域简化为一台逻辑设备，整网简化为几台逻辑设备，从而简化管理。通过OVC操作系统级虚拟化技术构建虚拟业务网，实现一张物理网络承载所有应用，并能按需提供精细化的网络策略。通过在核心和汇聚设备上部署的安全业务板卡以及L2~7融合和L2~7虚拟化，可以为应用提供一体化安全防护，并可以通过智能流定义，按需提供精细化的安全策略。

3.1 虚拟化基础架构

如前所述，一张物理网络上承载所有应用的建设模式存在网络规模庞大、建设复杂的问题，虚拟化基础架构是十分有效的解决方法。迪普科技虚拟化基础架构由VSM（Virtual Switching Matrix）虚拟交换矩阵技术和VEM（Virtual Extension Matrix）虚拟扩展矩阵技术实现。

通过VSM技术，可以将多台核心设备虚拟成一台逻辑设备，实现控制平面的统一。迪普科技VSM技术是L2~7全面的虚拟化技术，不仅可以实现网络资源的虚拟化，还创新地实现安全和应用交付资源的虚拟化。通过VSM技术虚拟化后，园区网的核心设备虚拟成一台逻辑设备，每个二层域的汇聚交换机分别虚拟成一台逻辑设备。通过VSM虚拟化后，实现了接入层设备上行链路的跨设备链路聚合,消除了二层环路，STP对网络的影响降到最低，同时三层也无需运行VRRP协议。此外，在运行VSM技术的虚拟化组内，多台设备性能可以负载分担，与传统主备模式相比，设备的利用率大大提升，节省用户投资。

VSM技术在很大程度上简化网络，但对数量庞大、地理位置分散的接入层设备而言，IT管理员仍需一台台地配置、调试、管理，这些重复性的工作消耗大量了的精力，极大降低了工作效率。同时接入层设备的功能没有核心、汇聚层设备功能丰富，这也影响了整网的业务处理能力。



迪普科技创新的VEM虚拟扩展矩阵技术，可以很好的解决以上问题。VEM技术可以将汇聚、接入层设备虚拟化为一台逻辑设备。虚拟化后，汇聚层设备成为虚拟化组的主设备，接入层设备成为虚拟化组的扩展设备。主设备对多台下联的扩展设备进行统一的控制管理，所有的数据转发也由主设备完成。扩展设备则相当于主设备的接口板。通过VEM技术，扩展设备的配置维护均在主设备上操作，接入层设备无需一台一台分别配置维护，极大简化了网络的运维管理。

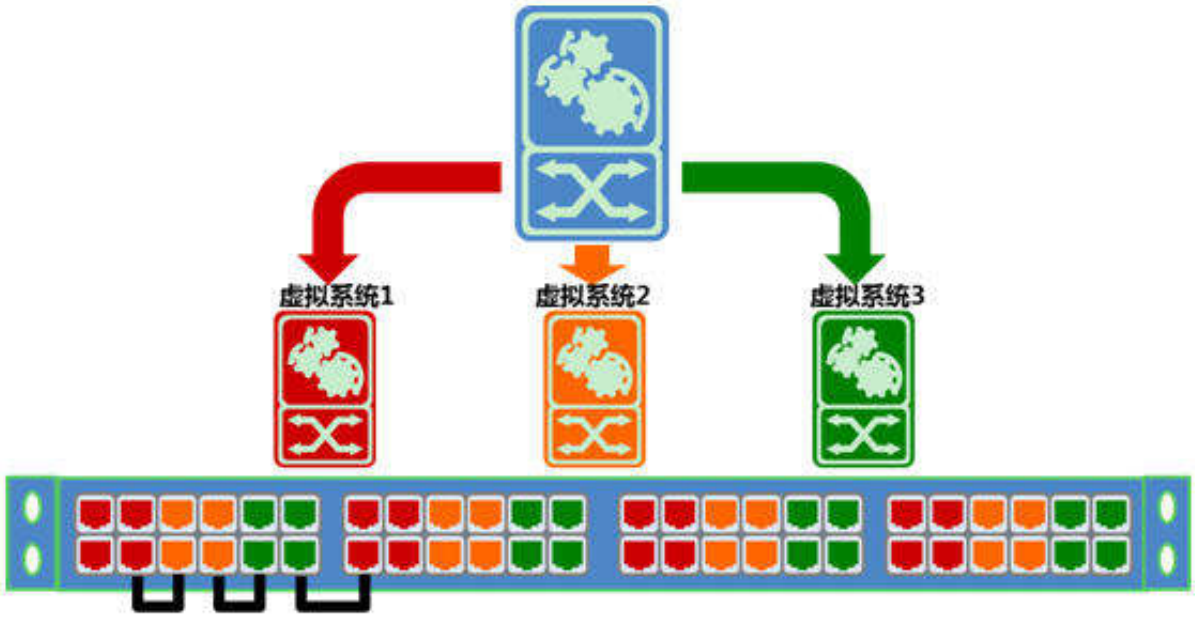
对于大型园区网，核心层通过VSM技术虚拟化成一台逻辑设备；汇聚层、接入层通过VSM+VEM技术，每个二层域虚拟化成一台逻辑设备，整网简化成几台逻辑设备的连接。对于中小型园区网，核心层、接入层通过VSM+VEM技术，整网虚拟化成一台逻辑设备，实现1-Tier组网。

综上所述，通过虚拟化基础架构，网络结构极大简化，运维管理成本大大降低。

3.2 虚拟业务网

虚拟化基础架构极大地简化了网络，但面对不同应用的不同需求，还需要建立不同的虚拟业务网。可以根据应用的安全要求、功能属性、用户群体等因素，将应用分为几类，每一类应用通过单独的虚拟业务网进行承载。每张虚拟业务网类似于单独的一张物理网络，与其他网络之间完全独立。在虚拟业务网内，根据应用的需求部署网络策略和安全策略，包括VLAN、路由、QoS、组播策略、访问控制策略、安全功能组合等等。这样，就可以在一张物理网络上承载所有应用，并且满足不同应用对安全和网络策略的不同要求。

虚拟业务网的实现是通过迪普科技创新的OVC（OS-level Virtual Context）操作系统级虚拟化技术，结合认证、访问控制等技术来实现的。其中的关键技术包括：



1) OVC。OVC技术可以将一台设备虚拟成多台逻辑设备（虚拟系统）。每个虚拟系统拥有独立的硬件、软件、管理资源，包括转发表项、控制进程、内存、CPU资源等等。管理上，每个虚拟系统拥有独立的管理员、管理界面。不同虚拟系统间实现操作系统级的隔离。迪普科技OVC技术是L2~7全面的虚拟化技术，不仅可以实现网络资源的虚拟化，还创新地实现安全和应用交付资源的虚拟化。通过OVC技术，可以实现网络核心层、汇聚层以及安全资源的划分。

2) 端口划分。运行VEM技术后，接入层设备作为主设备的网络资源（接口板）存在，由主设备进行控制和管理。因此，当通过OVC技术将一台设备虚拟化成不同虚拟业务网的设备时，可以对主设备的资源，包括接入层设备进行划分，可以将接入层设备的不同接口划分给不同的虚拟系统，进而实现接入层的端口隔离。通过VEM+OVC技术，可以将接入层的每个端口分配到相应的虚拟业务网内，并且隔离级别是操作系统级，从而创新地实现了接入层资源的划分，应用的安全性更加有保障。

3) 用户划分。通过迪普科技TAC终端接入控制，可识别不同用户的身份，根据用户身份选择对应的虚拟业务网。当用户的物理位置变化后，TAC会确保用户仍然选择到相同的虚拟业务网，并且网络策略不变。因此，通过TAC终端接入控制，实现不同虚拟业务网的用户划分。

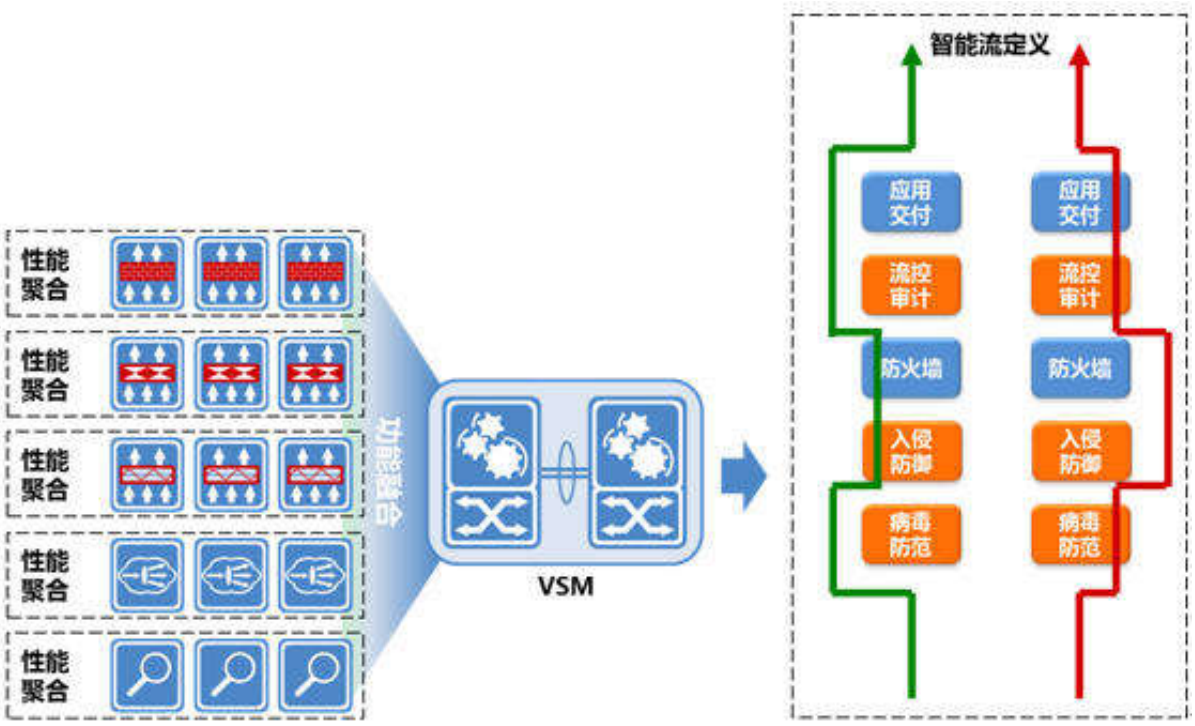
综上所述，在虚拟化基础架构之上，通过OVC操作系统级虚拟化技术，结合认证、访问控制等技术，不仅可以将一张物理网络的网络资源划分给不同的虚拟业务网，也可以对安全资源进行划分。不同虚拟业务网从核心、汇聚、接入层到安全资源完全独立，从硬件、软件到管理完全独立，从而满足不同应用的不同网络和安全要求。

DP xCampus安全虚拟园区网解决方案不仅可以承载多个虚拟业务网，而且能根据应用的变化，实现虚拟业务网的动态扩展，更好地满足应用不断增加和变化的发展趋势。当要新增一套虚拟业务网时，可通过OVC技术，在现有的资源池中，为新的应用划分出独立的核心层、汇聚层、接入层的网络资源，以及安全资源。当应用需要的网络、安全资源增加时，可将更多的资源划分给虚拟业务网，实现虚拟业务网的扩容；当应用所需的资源减少时，可将虚拟业务网的部分资源释放；当应用废弃时，可将对应的虚拟业务网删除；这样，便可在一套物理网络上，根据应用的变化及时作出调整，网络具备很强的适应能力。

综上所述，通过迪普科技的VSM+VEM+OVC+TAC技术，可在一套物理网络上虚拟出多套虚拟业务网，进行不同应用的承载，虚拟业务网间实现类似多套物理网络的隔离。在此基础上，能进一步实现网络的动态扩展，很好地应对应用增加的发展趋势。

3.3 安全体系架构

如前所述，园区网的安全防护体系应该根据应用需要提供针对性的防护，防护粒度更加细致，同时满足等保要求。



迪普科技可以提供访问控制、入侵防御、病毒防范、流量控制、行为审计在内完善的安全防护，既保障虚拟业务网内应用的安全，又保障虚拟业务网间安全的互连，同时满足等保的相关要求。

迪普科技的核心层、汇聚层产品支持多种类型的安全业务板卡，在与网络融合的基础上，这些板卡可以提供丰富的安全功能。通过迪普科技创新的智能流定义技术，可以指定特定的数据流通过特定的业务板卡，业务板卡的通过顺序也可自行定义。这样就可以针对不同应用提供不同的安全防护。同时，智能流定义通过图形化配置，配置过程十分简单，极大地简化安全策略的部署。

通过L2~7的VSM虚拟化技术，同类型的业务板卡可以虚拟成为一块逻辑板卡，从而简化管理，提高性能和可靠性。而VEM技术可以将流量从接入层牵引至核心层，再结合智能流定义技术，就可以对所有端口间的访问流量进行安全防护。与传统安全防护体系主要对VLAN间流量防护相比，迪普科技通过VEM+VSM，以及多种类型的安全业务板卡，可以将防护粒度从VLAN间提升至VLAN内，大大增强了网络的安全性。

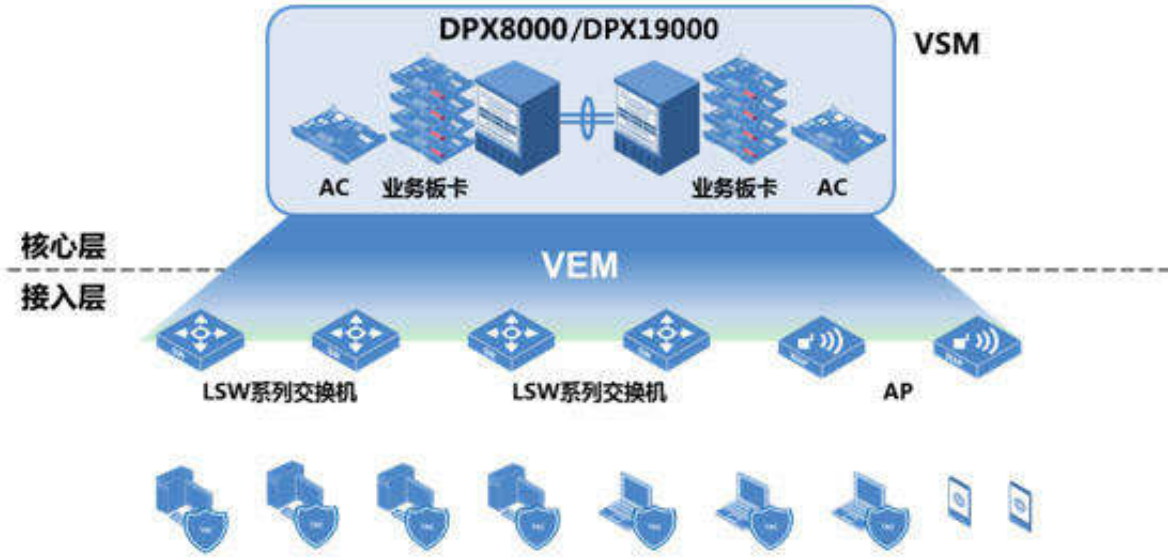
无论是针对不同应用进行针对性防护，还是防护细粒度的提升，都对安全防护体系的性能提出了很高的要求。迪普科技通过创新的产品设计，提供整机最大3.2Tbps（64字节）业务处理性能、32亿并发连接和1.28亿每秒新建连接的业务处理能力，领先业界平均水平10倍以上，让安全防护体系无性能之忧。

综上所述，迪普科技通过L2~7融合、L2~7虚拟化、智能流定义、VEM技术，对园区网中所有流量都可以提供L2~7全面的安全防护，防护功能按需定义，防护粒度达到VLAN内，同时满足信息等保的相关要求。

四、 安全虚拟园区网方案设计

■ 中小型园区网方案设计

中小型园区网的方案设计较为简单，采用“核心-接入”的扁平化组网模式，整网为一个二层域。通过部署无线AP、AC提供灵活的无线接入，并实现有线无线一体化。通过在核心部署业务板卡实现安全防护所需的功能。
方案拓扑如下图所示：



中小型园区网方案的设计要点如下：

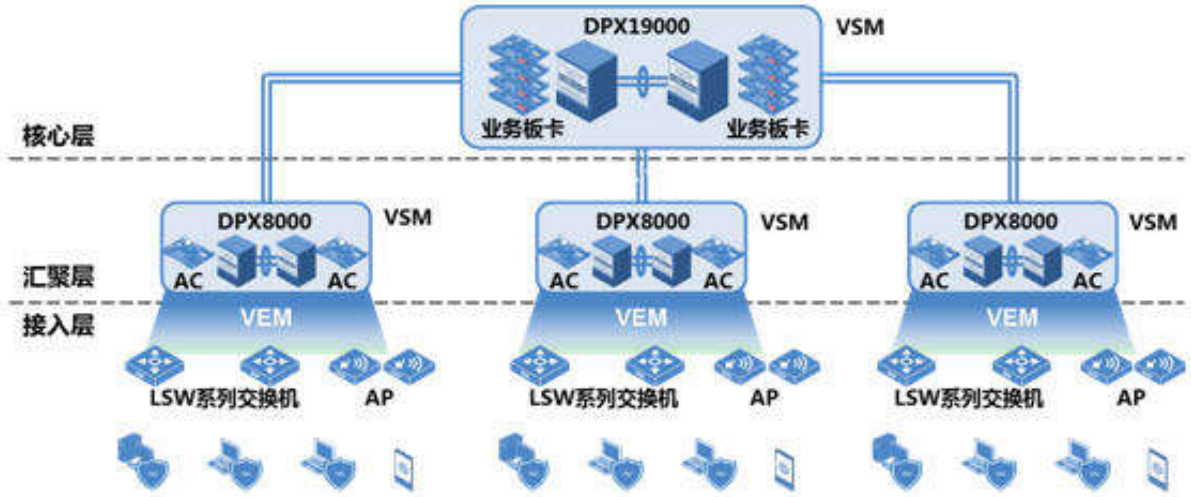
√ 1-Tier组网，整网虚拟化为一台逻辑设备

√ 虚拟业务网，不同应用通过不同的虚拟业务网承载

√ L2~7层安全防护，按需提供安全防护，实现VLAN内防护

■ 大型园区网方案设计

大型园区网的方案是在中小型园区网方案的基础上，增加二层域的数量，二层域与核心层通过路由互通，并实现有线无线一体化。通过在核心部署业务板卡实现安全防护所需的功能。方案拓扑如下图所示：



大型园区网方案的设计要点如下：

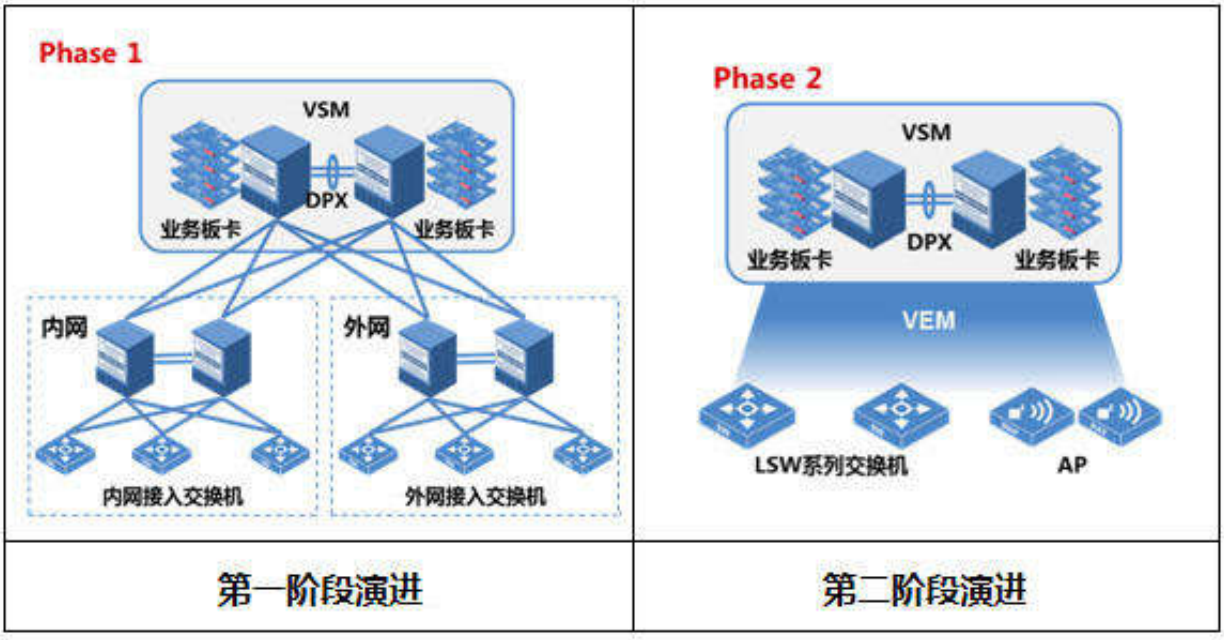
√ 虚拟化组网，整网虚拟化为一台核心层设备与几台汇聚设备的相连

√ 虚拟业务网，实现不同应用的操作系统级隔离，隔离到边

√ 安全体系架构，建立安全资源池，提供自定义的安全防护

■ 演进方案

对于非新建园区，迪普科技提供演进性的解决方案。在演进的第一阶段，部署一体化的安全核心，通过在安全核心上部署的多种安全业务板卡实现安全防护的功能。在实际部署时，可以通过OVC技术将安全核心一分为二，分别为内网和外网提供安全防护，网络核心与安全核心分离。



当后续网络扩容时，可以在安全核心上增加交换板卡，新建网络采用VEM技术，实现网络核心与安全核心的融合。有网络达到使用年限以后，再行替换。从而最大程度减少对网络的改动，保护投资，实现网络的平滑演进。

演进方案的设计要点如下：
√ 安全防护，提供L2~7层安全防护，满足等保要求
√ 按需防护，根据应用需要提供针对性的防护
√ 平滑演进，满足网络扩容需求，对现网改动最小

总之，DP xCampus安全虚拟园区网解决方案不但能够满足园区网需要的极大简化、虚拟隔离、安全防护等需求，而且能够提供网络安全融合的部署方案，以及灵活的租户自组网能力。DP xCampus安全虚拟园区网解决方案能够给客户提供不可替代的价值。