Azure 网络安全

Microsoft

摘要

本白皮书介绍了如何通过增强网络通讯安全性以更好地保护 Azure 中部署的虚拟基础架构，以及数据和应用程序。

本白皮书的目标读者包括：

- 对于在 Azure 中部署应用程序感兴趣的 IT 和网络管理员
- 对于创建在 Azure 中运行的应用程序感兴趣的开发者
- 考虑用 Azure 为新增或现有服务提供支持的技术决策者（TDM）

注意：本文包含的一些建议可能增加数据、网络，或计算资源的使用量，进而导致您的许可或订阅成本增加。

第 3 版，发布于 2015 年 2 月

目录

1 概述

Azure 网络提供了将虚拟机（VM）安全地连接在一起所需的基础架构，可充当云环境和 on-premises 数据中心之间的桥梁。

Azure 的网络服务按照设计可提供最大程度的灵活性、可用性、适应性、安全性以及完整性。本白皮书详细介绍了 Azure 的网络功能，并告诉客户如何使用 Azure 的原生安全功能保护自己的信息资产。

2 Azure 虚拟机保护指南

由世纪互联运营的 Microsoft Azure 是一个多租户平台，使用位于北京和上海的数据中心的共享基础架构为客户的并发访问提供支持。因为 Azure 的共享基础架构中运行着大量的活跃虚拟机，网络通讯的安全和机密性保护就显得尤为重要。

Azure 虚拟网络配合使用逻辑隔离、防火墙、访问控制、身份验证，以及加密技术保护传输中的客户数据。Azure 数据中心的运营遵循了一整套完善的信息安全策略和流程，使用了标准化的行业控制框架，例如 ISO 27001。第三方审计师会定期审核 Azure 基础架构中物理和虚拟部分对这些标准的遵守情况。

在传统数据中心模式下，公司的信息技术（IT）部门控制着联网的系统，包括对网络设备的物理访问。公司员工或承包商承担部署、配置，以及管理职责，例如网络拓扑的物理调整，路由器设置的改动，防火墙设备的部署等。

在云服务模式下，网络的保护和管理职责是由云服务供应商和客户共同承担的。客户没有物理访问权限，他们无法进入云服务供应商的数据中心调整服务器机架的接线，但客户可以通过来宾操作系统（OS）防火墙、虚拟网络网关配置，以及虚拟私有网络等工具在自己的云环境内部进行类似的逻辑实施。这种物理和逻辑的分离使得客户在构建自己的基础架构时能够充分使用 Azure 提供的一些基础安全功能。

2.1 私有网络

在公有云中对客户的基础架构进行逻辑隔离，这是维持安全性的关键。Azure 主要通过分布式虚拟防火墙实现这一点。此外，客户可以部署多个逻辑上相互隔离的私有网络。这些进一步细化的网络主要可分为两个类别：

- **部署网络：**每个部署可在网络层面与其他部署相互隔离。一个部署中的多个虚拟机可通过私有 IP 地址相互通讯。
- **虚拟网络：**每个虚拟网络可与其他虚拟网络相互隔离。同一订阅中的多个部署可位于同一个虚拟网络中，这样即可通过私有 IP 地址相互通讯。

图 1 演示了一个虚拟网络拓扑的范例。

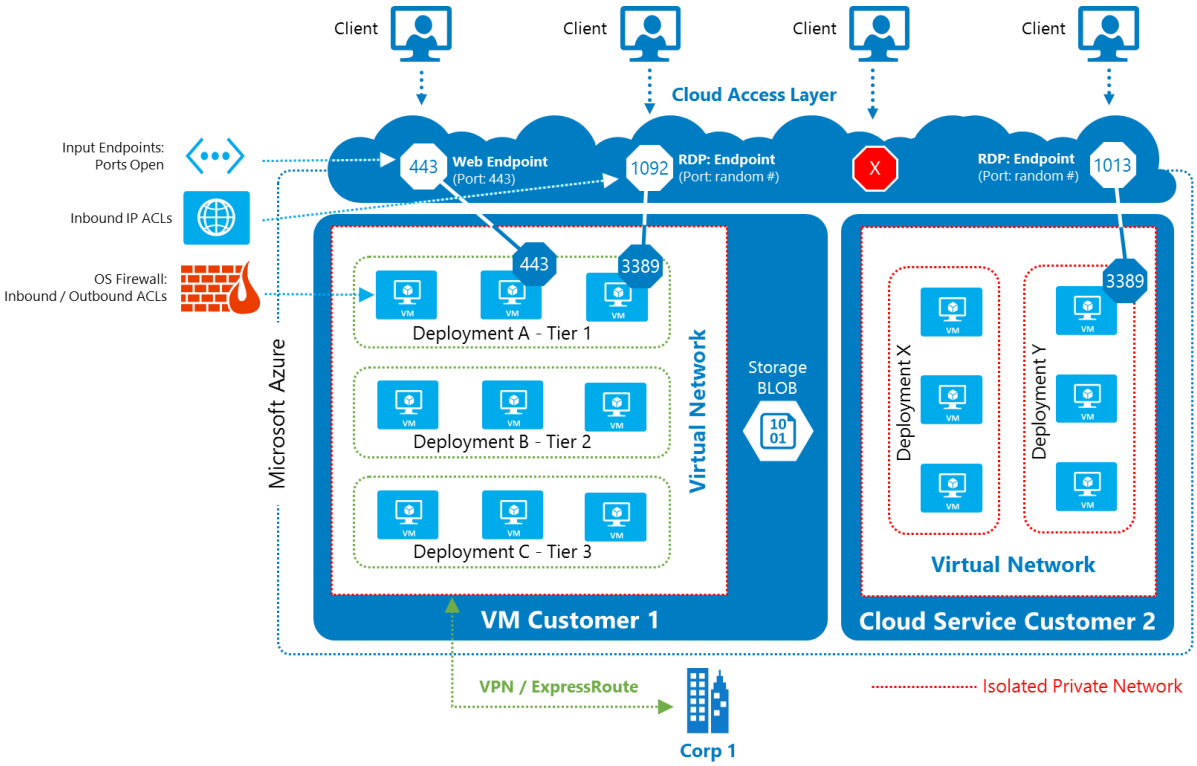

图 1 Azure 中托管的多层 IaaS 应用程序隔离范例。

网络管理员可以用与 on-premises 私有网络中类似的方法管理这些相互隔离的私有网络。

供管理员在 Azure 私有网络中管理网络安全所需的机制位于 Azure 云访问层中，这一概念类似于企业网络中面向互联网的边缘网络。云访问层包含了防火墙、负载平衡器，以及网络地址转换（NAT）功能，这些功能可由客户的管理员负责管理。

2.1.1 启用互联网通讯

默认情况下，私有网络中的虚拟机无法接收来自互联网的 inbound 通讯。管理员可以用下列三种方法之一启用互联网通讯：

- 管理员可以定义 input endpoint，借此定义虚拟机的哪个映射端口可以接收来自该部署隔离网络之外的 inbound 通讯，包括来自互联网的通讯和来自 Azure 中其他虚拟机的通讯。
- 管理员可以通过定义 Azure 安全组，指定哪个 IP 地址可以接收来自虚拟网络外部的 inbound 通讯，借此进一步提高安全性。请注意，管理员可以定义 input endpoint 访问控制列表（ACL）或安全组，但这两者只能择一使用，不能同时使用。
- 管理员可为虚拟机分配 instance 级别的公共 IP 地址，随后该虚拟机的所有端口都将可以访问互联网。

注意：本文中使用的“inbound 通讯”这一术语代表由互联网上的计算机，或客户 Azure 私有网络之外的计算机主动发起的通讯。为了将其与针对请求做出的回应所产生的 inbound 信息，也就是主动请求的 inbound 通讯区分开来，这种通讯也可以叫做未经主动请求的 inbound 通讯。

2.1.2 通讯的保护

保护私有网络内部虚拟机之间的通讯	部署网络内部的虚拟机可以通过私有 IP 地址进行内部通讯。一个订阅中多个部署内的虚拟机之间的通讯安全可通过使用虚拟网络进行加强。 如果应用程序需要通过内部私有网络发送或接收敏感数据，例如通过 VPN，则可使用 IPsec、SSL/TLS，或其他应用程序层加密技术对数据进行加密。对保密性或隐私有更高要求的客户（例如需要遵守不同行业制度和标准的客户）需确保一个区域内虚拟机之间的所有私有通讯都是被加密的。 有关虚拟网络加密功能配置的详细信息，请参阅 MSDN 上的 Azure 虚拟网络文档。
保护来自互联网的 inbound 通讯	默认情况下，对于通过 Azure 管理门户创建的虚拟机，除了远程管理端口，Azure 会阻止所有来自互联网的 inbound 通讯。 管理员可以决定虚拟机的哪些端口和 IP 地址可以通过 inbound 通讯从互联网访问。此外，管理员可以更改一系列配置，借此在网络层对从互联网到虚拟机或 VNET 端口进行的远程访问加以保护，这些配置包括： • 在云访问层定义 input endpoint，仅在需要时打开端口。管理员可以为 input endpoint 指定访问控制列表（ACL），借此控制虚拟机可以允许通讯的源 IP 地址。 • 定义安全组，将允许的 inbound 通讯限制在虚拟网络中特定虚拟机上。管理员可以定义 input endpoint ACL 或安全组，但这两者只能择一使用，不能同时使用。 • 使用虚拟机中运行的第三方代理防火墙对通往其他虚拟机的通讯进行筛选。将虚拟机加入虚拟网络，随后即可为代理防火墙的端口定义 input endpoint。 • 为虚拟机中来宾操作系统的防火墙定义开放的端口。 如果管理员打开 input endpoint 或 IP 地址，随后就必须像对待在互联网上开放运行的虚拟机那样采取必要的安全保护。如果应用程序需要通过 input endpoint 发送或接收任何敏感数据，那么所有 input endpoint 都应使用服务器和客户端身份验证机制，并应对通讯进行加密。如果应用程序需要通过公共网络（包括通过公共 IP 地址通讯）发送或接收敏感数据，则应对通讯进行 SSL 加密或应用其他类似的应用程序层加密技术。
保护跨订阅的通讯	客户可能有多个订阅，并可能需要让不同订阅中的虚拟机进行通讯。在这种情况下，虚拟机可配置为通过公共虚拟 IP 地址进行通讯。此外，可能需要在 input endpoint 上配置 IP ACLs，以便允许虚拟机相互之间发起通讯。 此时务必要使用保留的 IP 地址作为公共虚拟 IP 地址，这样才无需更改 IP 地址 ACL。

保护到 on-premises 网络的通讯

如果工作负载需要在 Azure 虚拟网络和 on-premises 系统之间建立安全的通讯，此时最好使用虚拟网络网关保护这些通道。此时有两种部署场景：

1. **内部多层应用程序：**部署在 Azure 中的多层应用程序（例如基于 Web 的记录处理系统），应用程序无需接受任何来自互联网的 inbound 连接，但需要连接至客户 on-premises 网络中的服务器和应用程序，如图 2 所示。

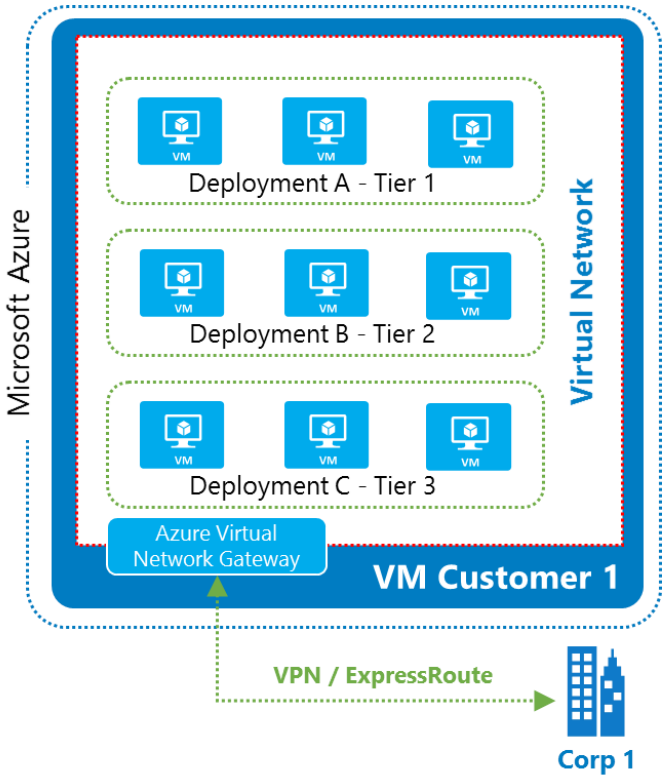

图 2 企业网络和 Azure 之间的 VPN 连接。

如果管理员需要创建 VNET 到 VNET 连接，此时可以创建一个虚拟网络，并将应用程序层的虚拟机加入该虚拟网络，但无需定义任何 input endpoints。另外，管理员还可以：

- 删除远程管理 input endpoints，或使用下文“隔离虚拟网络中的虚拟机以实现纵深防御”一节提供的指南将其锁定，借此保护管理 endpoints。

2. **对外的多层应用程序：**Azure 中部署的多层应用程序，其中前端层需要接受来自互联网的 inbound 连接（使用 SSL 的 443 端口）。后端层无需接受来自互联网的 inbound 连接，但需要连接至客户的企业内部网络，如图 3 所示。

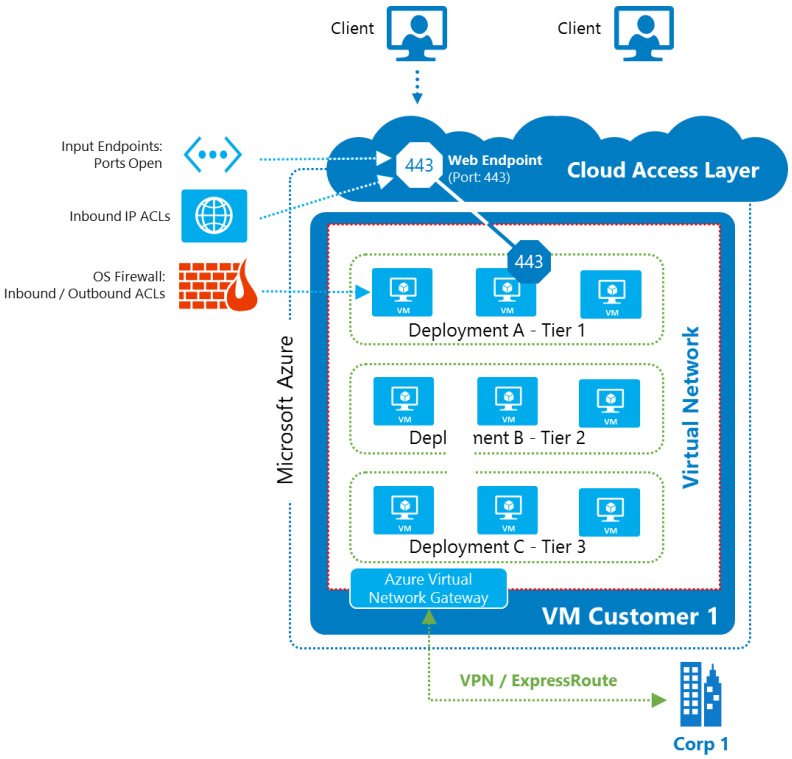

图 3 额外增加的面向互联网的 input endpoint 使得前端层可从互联网访问。

在这种情况下，管理员应当：

- 使用每个应用程序层的相应虚拟机创建一个虚拟网络。
- 为前端层虚拟机的 inbound 互联网通讯定义 input endpoints。
- 删除所有虚拟机的远程管理 input endpoints，或将其锁定。
- 配置虚拟网络网关，让通往企业内部网络的通讯通过 VPN 连接进入企业网络。

虚拟网络网关建立的 IPsec 隧道可对虚拟网络和客户的 VPN 设备之间的通讯进行路由。这里的 VPN 可以是硬件 VPN 设备或软件 VPN，例如 Windows Server 2012 路由和远程访问服务。

在 Azure 中创建虚拟私有网络，借此您就可以用更安全的方式将 on-premises 网络扩展至 Azure。这样的连接可以使用站点到站点，或点到站点 VPN。

如果某一区域内的 VPN 通过虚拟网络网关从互联网连接至企业网络，相关通讯将使用 AES-256 等标准默认进行加密，不过具体配置取决于企业网络的站点到站点 VPN 网关配置。

需要更高安全性的客户可使用 IPsec、TLS，或其他应用程序级别的加密技术对通讯进行加密，例如在移动虚拟磁盘（VHD）文件时使用 BitLocker 加密。

2.2 安全管理和威胁防范

保护虚拟机的远程管理通讯

管理员可以使用 Azure 管理门户或 Windows PowerShell 创建虚拟机。

当使用 Azure 管理门户创建虚拟机时，默认将启用远程桌面协议（RDP）和远程 Windows PowerShell 端口。随后为了降低密码字典攻击的概率，Azure 管理门户会为 RDP 和远程 Windows PowerShell 功能分配随机端口。

当管理员使用 Windows PowerShell 创建虚拟机时，RDP 和远程 Windows PowerShell 端口必须明确开启。

- 管理员可以选择将 RDP 和远程 Windows PowerShell 端口面向互联网开启，但对于允许创建 RDP 和远程 Windows PowerShell 连接的账户，至少应使用强密码进行保护。
- 管理员还可以考虑使用上文提到的常规选项保护来自互联网的 inbound 通讯。

保护防范 DDoS

为了保护 Azure 平台服务，Azure 提供了分布式拒绝服务（DoS）防御系统，该系统已成为 Azure 持续监控流程的一部分，并会通过渗透实验进行持续的改进。按照设计，Azure 的 DDoS 防御系统不仅可以承受来自外部的攻击，而且可以防御来自其他 Azure 租户的攻击：

1. 网络层高容量攻击。这些攻击会用数据包堵塞整个网络，耗尽网络线路和数据包处理容量。Azure DDoS 防御技术具备 SYN cookie、速率限制，以及连接限制等检测和减缓技术，可确保此类攻击不会对客户环境造成影响。
2. 应用程序层攻击。这些攻击可针对客户的虚拟机发起。Azure 没有提供能够减缓或主动阻止影响特定客户部署的网络通讯的机制，因为基础架构无法判断对于客户的应用程序来说，哪些行为是合理的。在这种情况下，与 on-premises 环境类似，可考虑下列减缓措施：
   - 在负载平衡的公共 IP 地址之后运行多个虚拟机 instance。
   - 使用防火墙代理设备终止通讯，或将通讯转发至虚拟机的 endpoints。这种方式可防范一系列 DoS 和其他攻击，例如低速率、HTTP，以及其他应用程序层威胁。此外可使用一些虚拟化解决方案执行入侵检测和预防操作。
   - 保护防范某种类型 DoS 攻击的 Web 服务器加载项。
   - 网络 ACL，可防止来自某些 IP 地址的数据包到达虚拟机。

如果客户发现自己的应用程序被攻击，可立即联系世纪互联客户支持以获得协助，客户支持人员会优先处理此类请求。

使用内部 DNS 保护内部虚拟机的名称

为了对云服务中的虚拟机寻址，Azure 提供了内部 DNS 服务。虚拟机的名称可解析为云服务中的私有 IP 地址，并且就算同一订阅中的多个云服务，相互之间也可维持隐私。

分配给云服务角色和虚拟机的私有 IP 地址在修复云基础架构的过程中可能会变化。因此 Azure 托管服务中不同角色之间的通讯必须通过 DNS 名称进行解析，而不能使用 IP 地址。这一规则有一个例外，即虚拟网络使用自定义 IP 地址空间的时候。在这种情况下，IP 地址是静态的。此外，因为私有 IP 地址可能会变化，DNS 响应的 DNS 存活时间（TTL）值应以客户端设置为准。

隔离虚拟网络中的虚拟机以实现纵深防御

管理员可以使用网络安全组在虚拟网络的网络层对内部通讯进行划分。网络安全组可应用于虚拟网络的子网。

图 4 展示了一种多层应用程序部署范例。

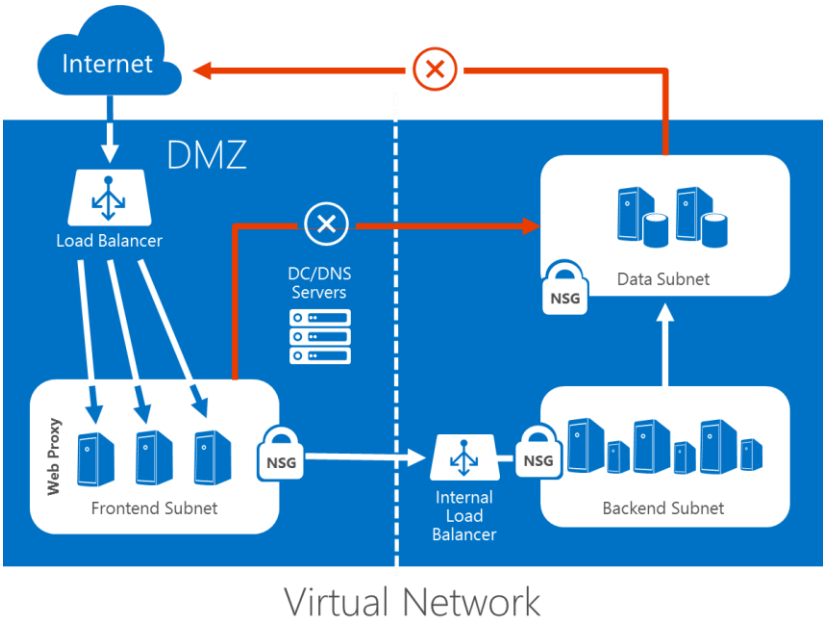

图 4 网络安全组在多层应用程序 VNET 中的应用。

除了对内部通讯进行划分，还可借助网络安全组（NSG）对发往和来自互联网的通讯进行控制。

网络安全组可应用于虚拟机或子网，某些情况下可同时应用于这两者。NSG 的一些重要注意事项包括：

- NSG 规则包含 5 个组成部分（源 IP、源端口、目标 IP、目标端口，协议），如图 5 所示。
- NSG 规则是有状态的。因此如果有一条入站规则允许某端口进行通讯，则无需在出站端创建相对应的规则，即可让数据包通过同一端口传输。
- 每个 NSG 包含的默认规则可以让虚拟网络内部建立连接并出站访问互联网。客户的管理员可以修改这些默认规则。
- NSG 会根据优先级处理多个规则。优先级数值较小（意味着优先级高）的规则会先于优先级数值较大（意味着优先级低）的规则处理。
- Azure 提供了默认标签，例如 INTERNET 和 VIRTUAL_NETWORK，这两个标签分别代表虚拟网络外部的公共 IP 地址空间，以及客户的整个网络地址空间。标签可用于访问控制规则中。

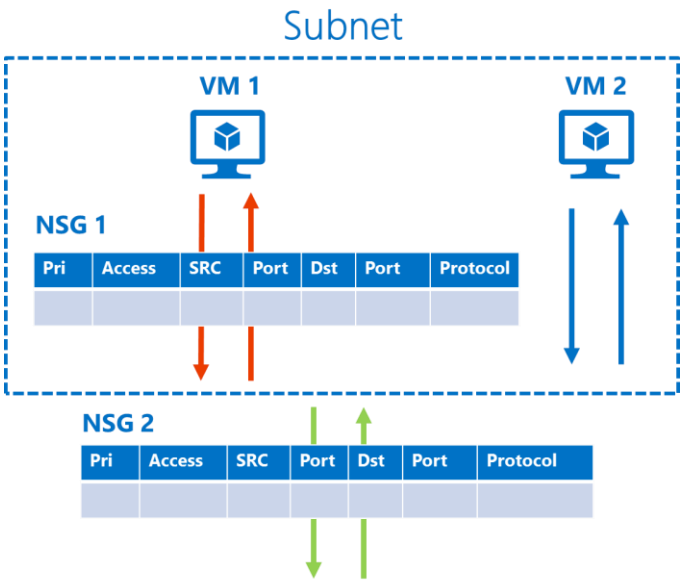

图 5 在虚拟网络中处理的五元规则。

保护从虚拟机到 Azure SQL 数据库的通讯

Azure SQL 数据库内建了可对 inbound 通讯进行筛选的防火墙。初始状态下，所有到 SQL 数据库的通讯都会被阻止。为了启用与数据库的通讯，管理员必须在 Azure SQL 数据库中定义防火墙规则，允许 Azure 中虚拟机的公共 IP 地址与数据源通讯。

此外，如果公共虚拟地址在任何时候发生变化，管理员必须更新 IP 地址 ACL。这一过程可能导致服务中断，进而增加管理员的工作负担。另外，在虚拟机关闭或部署被删除后，公共虚拟 IP 地址可在计算资源重新分配后进行更改。

然而通过 in-place 升级，管理员将可以在不更改虚拟机公共 IP 地址的情况下部署新版本的服务。

3 Azure 云服务保护指南

上述适用于 Azure 虚拟机和 VNET 的指南同样适用于 Azure 云服务 Web roles 和 Worker roles。

与虚拟机类似，通过 Azure 门户创建的每个云服务角色默认情况下也会阻止来自互联网和远程管理端口的 inbound 通讯流。当管理员针对某一角色启用远程桌面服务器后，RDP 端口会被开启。RDP 端口号会使用随机数分配（如图 6 所示），这样可降低全面扫描/密码字典攻击的成功率。

客户可以选择将 RDP 端口面向互联网开放，但至少应使用强密码对允许使用该功能的账户加强保护。

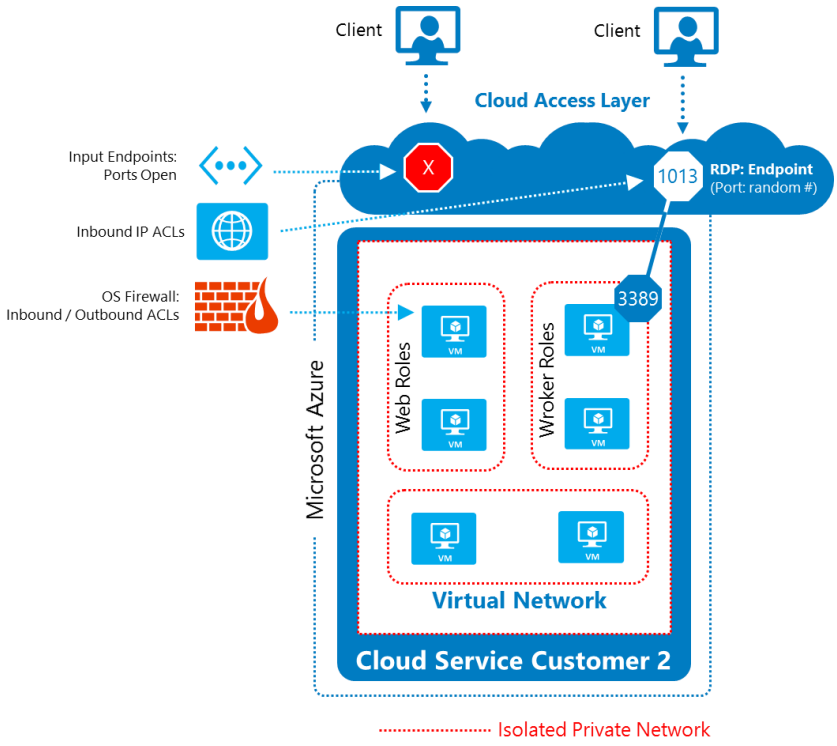

图 6　Azure 云服务虚拟网络拓扑

在使用 RDP 时，可通过 Azure 门户启用 RDP 端口，但应在使用完毕后将其禁用。类似的，建议只有在服务定义文件（.csdef）的 WebRole 或 WorkerRole 架构中的 Endpoints 元素中定义之后，再开启其他端口。详细信息请参阅 MSDN 上的 WebRole 架构和 WorkerRole 架构指南。

4 总结

下表列出了 Azure 虚拟网络有关配置，及借此改善安全性的更多参考信息。

功能	技术	建议	详细信息
加密	SSL / TLS	保护到虚拟机的 inbound 互联网通讯	http://www.azure.cn/documentation/articles/cloud-services-configure-ssl-certificate/
	IPsec	配置 VPN 以实现安全的跨界连接	https://msdn.microsoft.com/zh-cn/library/azure/dn133798.aspx
主机防火墙	IP ACLs	创建 input endpoints 以控制到虚拟机的通讯流	http://www.azure.cn/documentation/articles/virtual-machines-set-up-endpoints/
隔离	ExpressRoute	使用专属光纤链路保护远程网络通讯	http://azure.microsoft.com/en-us/services/expressroute/
来宾防火墙	Windows 防火墙	配置虚拟机中的防火墙，借此仅允许必要的终结点	http://www.azure.cn/documentation/articles/virtual-machines-set-up-endpoints/

5 参考资源和后续阅读

下列资源提供了有关 Azure 和相关微软服务，以及正文中提及的部分概念的常规信息：

- Azure 主页 – 有关 Azure 的常规信息和链接
  - http://www.azure.cn/
- Azure 文档中心 – 开发者指南和信息
  - http://www.azure.cn/documentation/
- Azure 信任中心
  - http://www.azure.cn/support/trust-center/
- Azure 网络服务
  - https://msdn.microsoft.com/zh-cn/library/azure/jj156007.aspx
- Azure 网络安全白皮书配套视频
  - http://channel9.msdn.com/Blogs/Windows-Azure/Companion-video-for-the-Windows-Azure-Network-Security-white-paper?format=html5

6 附件：深入了解 Azure 网络安全

本节进一步深入介绍了 Azure 的网络安全机制，以及 Azure 提供的一些安全服务的使用指南。

6.1 多层保护

图 7 展示了 Azure 中不同层面的网络保护机制。

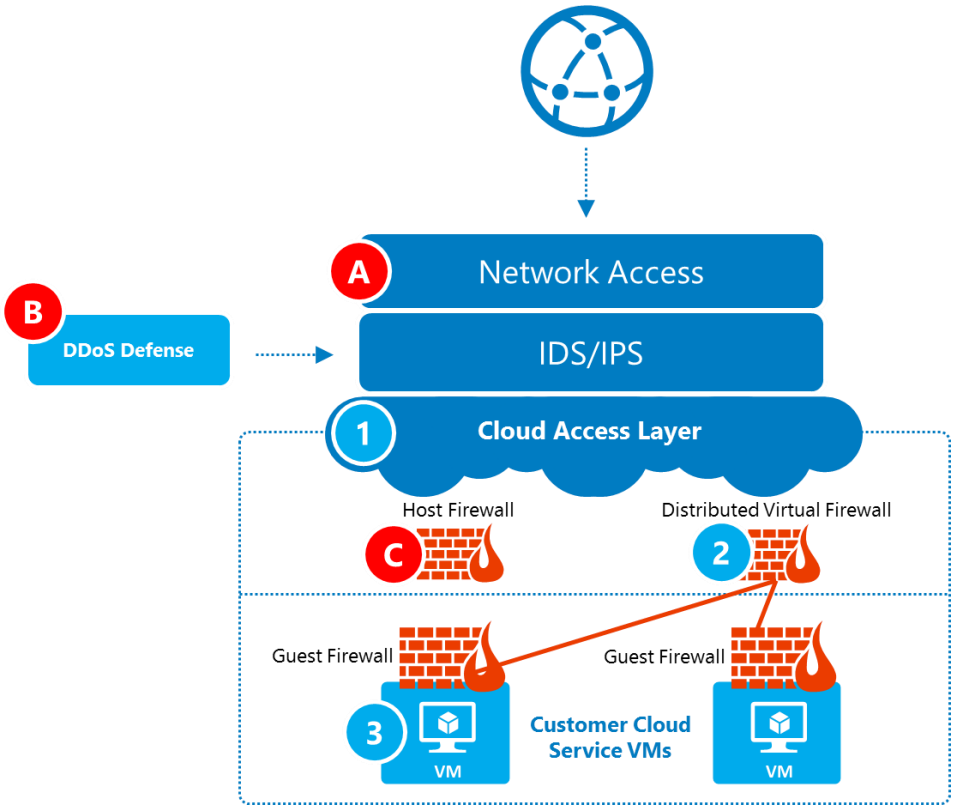

图 7 为客户和 Azure 基础架构提供保护的防御层。

这些保护措施可分为两个不同领域：对基础架构的保护，以及对客户的保护。

1. 对 Azure 平台服务基础架构的保护：
    a. A 层：网络访问层将 Azure 私有网络与互联网隔离。
    b. B 层：Azure 的 DDoS/DOS/IDS 层，使用与 on-premises 环境截然不同的方法和技术实现类似的安全保护目标。
    c. C 层：为所有主机提供保护的主机防火墙，以及为重要资产提供额外保护的 VLAN。
    d. D 层：安全与隐私需求的合规保护，包括运营者的双重身份验证。

2. 对客户的保护：

a. 第 1-2 层：在网络层面将不同客户的部署环境进行隔离的分布式防火墙。多个部署可位于同一个虚拟网络中，每个虚拟网络可与其他虚拟网络相互隔离。云访问层充当了互联网和被隔离网络之间的网关，并提供了可由客户进行配置的负载平衡、NAT 以及防火墙功能。

b. 第 3 层：虚拟网络可用与 on-premises 私有网络类似的方式进行管理。

   i. 虚拟机内部：可在虚拟机的来宾操做系统 on-premises 防火墙、IDS 以及 DoS 解决方案。

   ii. 虚拟网络装置：基于代理的设备可终止通讯，或将通讯转发至终结点，在虚拟机内部运行这样的装置即可保护防范更广泛的 DoS 和其他攻击（例如慢速率、HTTP，以及应用程序层威胁）。如果需要使用桥接模式的安全装置，管理员可以将 Azure 虚拟网络连接至 on-premises 网络（例如通过 VPN），并通过这样的设备将通讯发往企业内部。

6.2 隔离

Azure 为每个部署提供了网络隔离功能。通过使用 input endpoint，客户可控制哪些端口能够从互联网访问。

虚拟机之间的通讯始终通过可信赖的数据包筛选器进行遍历。

a. 地址解析协议（ARP）和动态主机配置协议（DHCP）等协议，以及来自虚拟机的其他 OSI 第二层通讯都可使用速率限制和反欺骗保护进行控制。

b. 虚拟机无法捕获任何目标地址非自己的网络通讯。

- 客户的虚拟机无法将通讯发往 Azure 的私有接口或其他客户的虚拟机，也无法发往 Azure 基础架构服务。客户的虚拟机只能与相同客户所拥有或控制的虚拟机，以及用于公共通讯的 Azure 基础架构服务终结点通讯。
- 当客户将虚拟机放入虚拟私有网络后，这些虚拟机将获得自己的，完全不可见的地址空间，此时将无法从部署或虚拟网络之外的虚拟机访问（除非通过公共 IP 地址配置为可见）。客户环境将只通过明确指定为可公共访问的端口开放，如果虚拟机定义了公共 IP 地址，则所有端口将能接受公开访问。