FORTINET

Fortinet

AWS云安全场景化解决方案

CONTENTS

执行摘要

公有云是云计算的经典且普遍的场景。云服务提供商通过互联网为企业提供基础设施、存储和服务器等资源。而第三方供应商通过拥有并运营共享物理硬件的方式，根据各企业的需求将服务提供给它们。这种多租户环境有助于更轻松地将基础设施成本分摊给多个用户。全球范围的企业通过采用云服务来获得如下核心能力：

成本效率

通过使用云基础设施，客户无需投入大量资金购买和维护设备。这极大的降低资本支出（CapEx）成本，帮助企业节省资源和时间，使企业能够更加快速地投资建立实体、或投资其它硬件设备或建立大型数据中心来专注发展业务。

容灾

数据丢失是所有企业的主要顾虑。将客户数据存储在云端可确保数据始终可用，即使笔记本电脑或 PC 等设备损坏也不受影响。基于云的服务在紧急情况（严重如自然灾害或普通的停电）发生时进行快速数据和业务恢复。

扩展性

基于云的解决方案非常适合带宽需求不断增长和弹性需求的企业。如果业务需求增加，客户可以轻松地增加其云容量，而无需投资更多物理基础架构。这样的 敏捷性将成为企业超越竞争对手的关键优势。

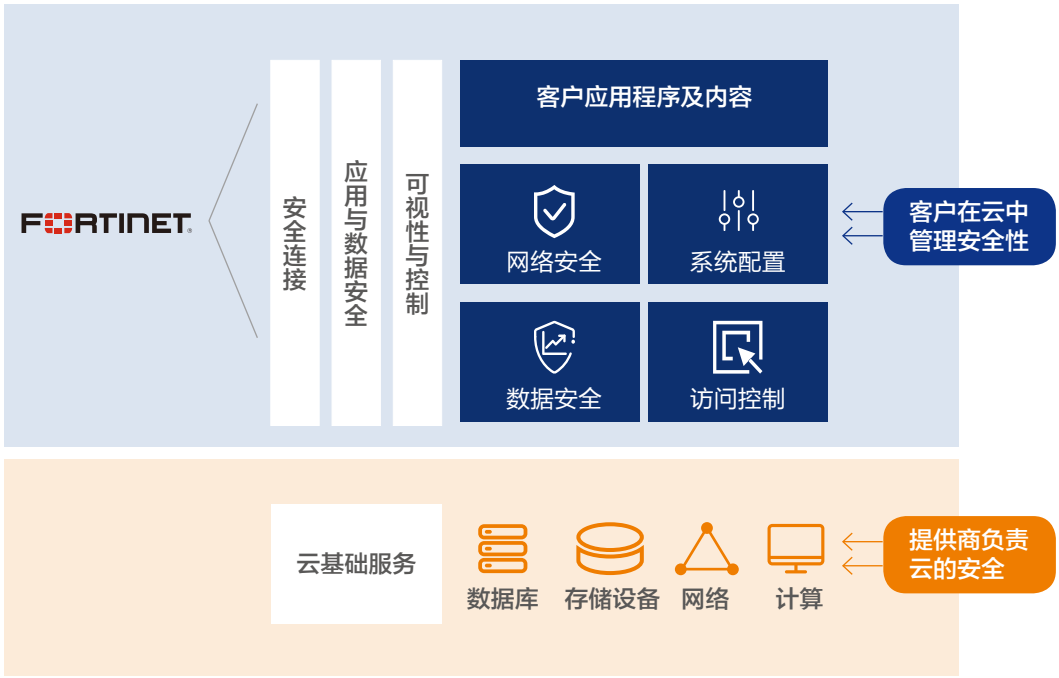
提高生产效率

如今，企业通过不断发展和改进其流程、工具、技术和政策来提高生产效率。高敏捷性使企业能够更快地做出决策并确定工作的优先顺序和确保客户满意度。借助云，企业可以体验到更好的交付、更好的协作，以更快地推出新业务。

责任共担模型

虽然云提供商会负责管理云基础设施的安全，但云上业务的安全要由客户自己来负责。客户可自行决定选择实施哪些安全措施来保护其云上的环境和应用程序。

云服务提供商运营、管理和控制从主机操作系统和虚拟化层到服务运行设施的物理安全性的各种组件。但是，客户保留其数据的所有权和控制权，并负责在其环境中的配置和部署安全。



Fortinet
守护客户 AWS 云端之旅

Fortinet 是公有云安全的最佳补充

AWS 是企业上云的最普遍选择之一。公有云自身安全服务有许多功能是缺失的，这也引入了“责任共担”的安全治理模型的原因，Fortinet 建议用户可以边界 / 边缘、内部环境以及已知威胁、未知威胁等不同的方向和维度来进行云安全架构设计，这需要通过安全产品的协同联动来同时保护网络内部和边界，例如通过集中的安全日志报表和相关的联动实现对已知威胁的保护，通过沙箱、蜜罐、主机安全、威胁情报及态势感知等能力来实现对未知威胁的防护。

API 驱动的弹性，可靠与自动化

云的弹性赋予了其按需使用按量付费的特点。通过 DevOps 实现的业务环境资源弹性扩缩来优化成本是云资源管理最佳实践之一，用户自然不希望还像传统方式一样采用全手工的方式来运维基础设施。就像在 AWS 中使用脚本自动化操作存储、计算、网络资源的弹性扩缩一样，用户认为云上的安全也应该是这样，包括云上的第三方安全产品，如 Fortinet。然而，第三方产品在云上的自动化并不像想象中的那么简单，甚至有些琐碎。

Fortinet 通过 Fabric Connector 云原生驱动器与 AWS 十余种服务进行 API 集成，并预开发和配置完成了一系列 AWS CloudFormation 和 Terraform 模板，使用了 AWS Auto Scaling 服务来实现 FortiGate 和 FortiWeb 等顶级水平的企业安全产品的自动化弹性扩缩，跨 AZ 和跨 Region 的 HA。在 FortiGate 中，用户还可以使用内置的 Security Fabric 流程引擎来编排和定义管理和安全事件的触发条件及响应动作，比如通过获取 Amazon GuardDuty 事件来触发 Lambda 脚本定义好的一些列操作，这种方式极大的扩展了用户使用 AWS 和 Fortinet 产品解决方案的可能性。

目前 Fortinet 已经完成与 AWS 如下服务的 API 集成：Amazon GuardDuty，AWS Lambda， AWS CloudFormation，AWS Auto Scaling，Amazon Virtual Private Cloud，Amazon EC2，AWS Security Hub，AWS ECS，AWS WAF，Amazon S3 等。权。及时用户已经在线下数据中心中使用了 Fortinet 云产品授权，也可以很方便的迁移到云端，而无需重复投资。

为什么在 AWS 上使用 Fortinet 解决方案

Fortinet 是全球前三大网络安全公司之一，Fortinet Security Fabric 安全平台通过全面的产品线覆盖数字化攻击面，紧密集成的解决方案消除单点作战与系统复杂度，并通过自动化工作流提升网络安全防御 / 检测 / 响应的效率，帮助企业进行数字创新。

通过使用 AWS，用户可以获得方便的资源弹性扩缩，而不用投入精力管理物理服务器及其产生的相关直接和间接成本。Fortinet 充分发挥了云计算按需使用按量付费的优势，在云上提供多种授权模式：按小时，按年，和永久授权。及时用户已经在线下数据中心中使用了 Fortinet 云产品授权，也可以很方便的迁移到云端，而无需重复投资。

Fortinet 中国具有最多数量的 AWS 专家认证，提供全面、专业及积极的安全专家咨询、部署与售后服务支撑。

Fortinet 中国区 AWS 专家认证及数量：

10	2	1
Solution Architect Professional	DevOps Engineer Professional	Security Specialty

Fortinet AWS 安全产品简介

Fortinet 提供丰富、多元且可协同并整合的安全解决方案，上架 AWS 全球及中国 Marketplace。

这些产品具备即插即用、远程部署、集中管理等优势，不仅能够单独提供给用户，而且还能够集成为统一的解决方案，可以执行全网一致的安全策略，对防火墙等设备进行集中管理，全网感知安全态势，从而降低安全风险，支持企业用户获得涵盖运维、策略控制、安全、扩展、网络支持在内的一站式安全服务，在虚拟基础设施内实施关键的安全控制，实现高价值的安全保护。

Fortinet 在 AWS 上的核心安全产品

FortiGate NGFW

FortiGate NGFW 通过将状态检测与一整套强大的安全功能相结合，提供完整的内容和网络保护同时保持了高度的可视化管理与易用性。其可实现应用程序控制、防病毒、IPS，Web 过滤和 VPN 以及高级安全功能，如高危威胁数据库，漏洞管理和基于流的检查工作，以识别和缓解最新的复杂安全威胁。 FortiGate 基于加载的 FortiOS 操作系统专门用于检测和识别恶意软件，并支持 SR-IOV，以实现更高和更一致的性能。

FortiWeb WAF
Web 应用防火墙

基于人工智能和机器学习技术的下一代 WAF，可提供针对 Web 应用程序的保护，大大缩短防护系统的部署时间，并简化安全管理。

FotiManager
集中管理平台

可以管理任意数量的 Fortinet 设备，通过将设备进行分组到不同的管理域（ADOM）进一步简化多设备安全部署与管理；

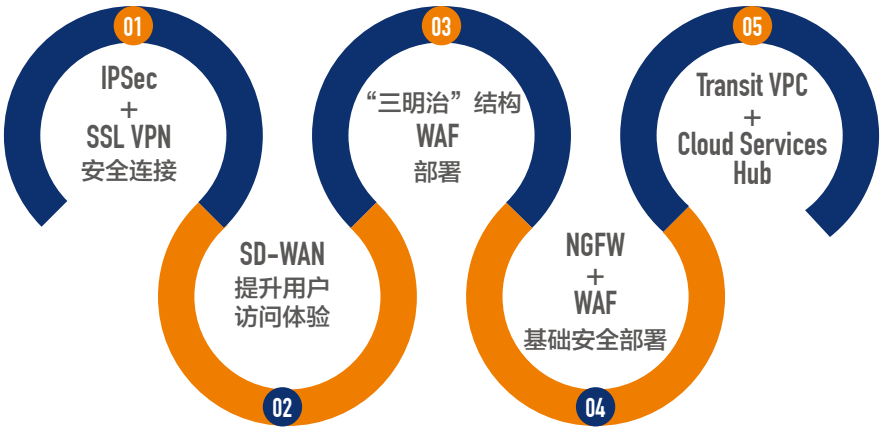
FortiAnayzer
日志收集与分析平台

可从 Fortinet 设备或其他的 syslog 兼容设备上聚集日志数据，提供网络范围内的可视性和合规性；

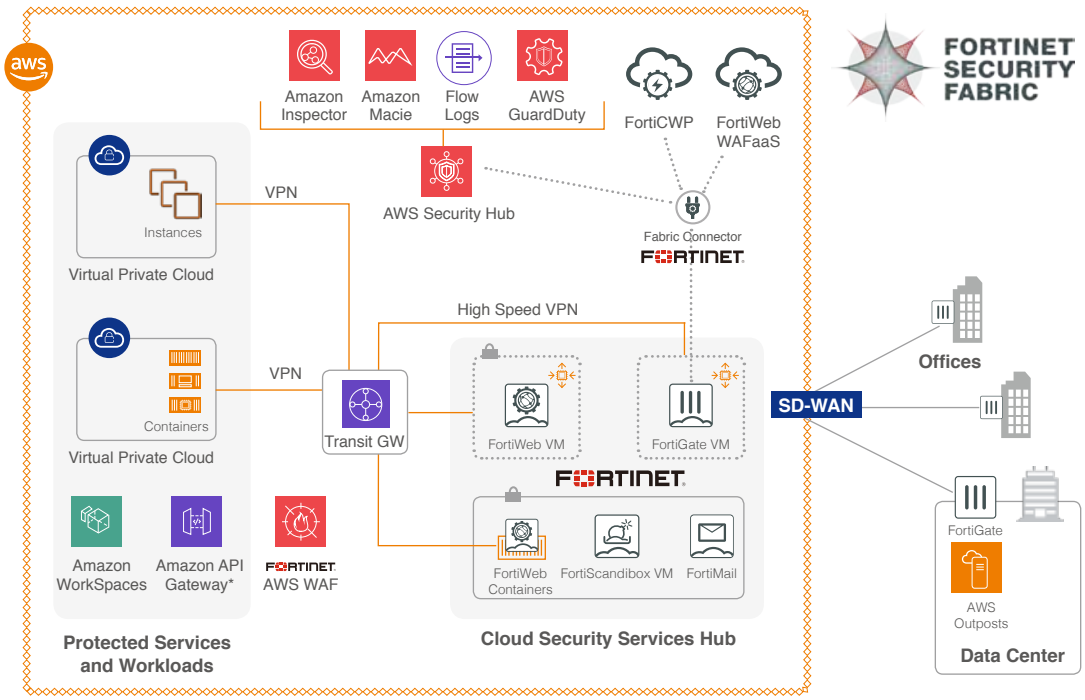
FortiAuthenticator
身份管理与认证产品

帮助用户构建统一的身份管理与认证体系，并快速构建 SSO 单点登录，双因子认证用户体验友好、安全级别高的认证机制；还可以与企业现有认证系统集成，如 LDAP，AD，RADIUS 等等；

Fortinet 解决方案
在 AWS 应用的五大场景解读



Fortinet on AWS 解决方案全景图



Fortinet on AWS 解决方案全景图

场景中包含的主要环境：VPC、Transit Gateway、Cloud Services Hub、企业办公网、企业数据中心、AWS 其他服务。

在 AWS Global 环境中：

01 企业在本地数据中心、办公室和 AWS 上分别部署 FortiGate 下一代防火墙，通过 IPSec VPN 将多个网络环境进行安全连接；

02 在 AWS 中创建 VPC 作为 Fortinet Cloud Services Hub，可以根据实际需求在其中部署 FortiWeb 基于人工智能和机器学习的下一代 WAF，FortiGate 下一代防火墙，FortiSandbox 未知威胁检测系统，FortiMail 反垃圾邮件系统等安全服务；

03 AWS 环境中的多个 VPC 和 Fortinet 多种安全服务组成 Cloud Services Hub 通过 Transit Gateway 进行连接；

04 在 FortiGate 上使用 Fabric Connector 和 AWS 源生安全服务进行情报集成：AWS Inspector、Macie、Flow Log、GuardDuty 等等，以增强安全检测和响应能力；

05 如果用户使用了 AWS 的源生 WAF 服务，可以额外部署 Fortinet 的 Managed Rules (OWASP Top10, SQLi/XSS, Malicious Bot 等等)；

用户还可以使用 FortiCWP 来进行针对 AWS 基础设施服务的配置安全检查与修复，流量检测，合规审计。

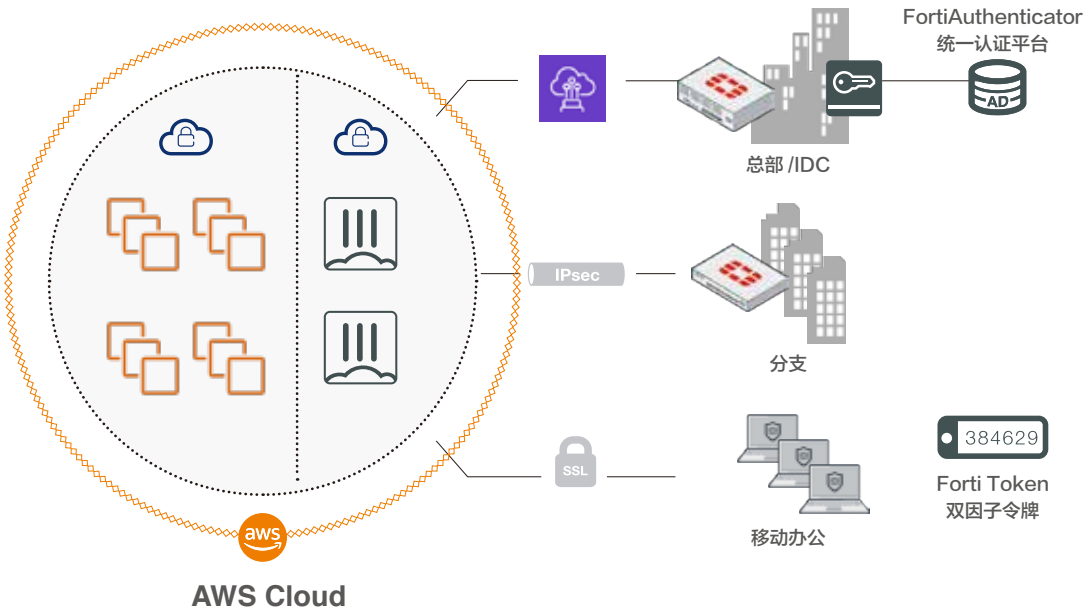
Fortinet on AWS 的五大场景解读

1 2345 IPSEC+ SSL VPN 安全连接

保 障 安 全 访 问

本地环境和云上环境的安全连接是企业使用公有云时的最基础安全场景。用户可以通过在本地和云端分别部署 FortiGate 下一代防火墙，并建立 IPSec VPN 隧道，即可实现本地办公网或数据中心到 AWS 环境的安全连接；针对在外办公又需要直接访问 AWS 云上资源的用户，可以在终端（电脑或手机）上安装 FortiClient 终端安全软件，通过 SSL VPN 连接到 AWS 中部署的 FortiGate，然后就可以访问 AWS 内部的资源了。

如果需要进行远程 SSL VPN 连接的用户数较多，或者需要和企业内部原有认证系统集成（如 AD），可以部署 FortiAuthenticator 认证服务器。此外，对于身份安全有高安全需求的用户，Fortinet 还提供了 FortiToken 双因子认证令牌，提升访问的安全性。

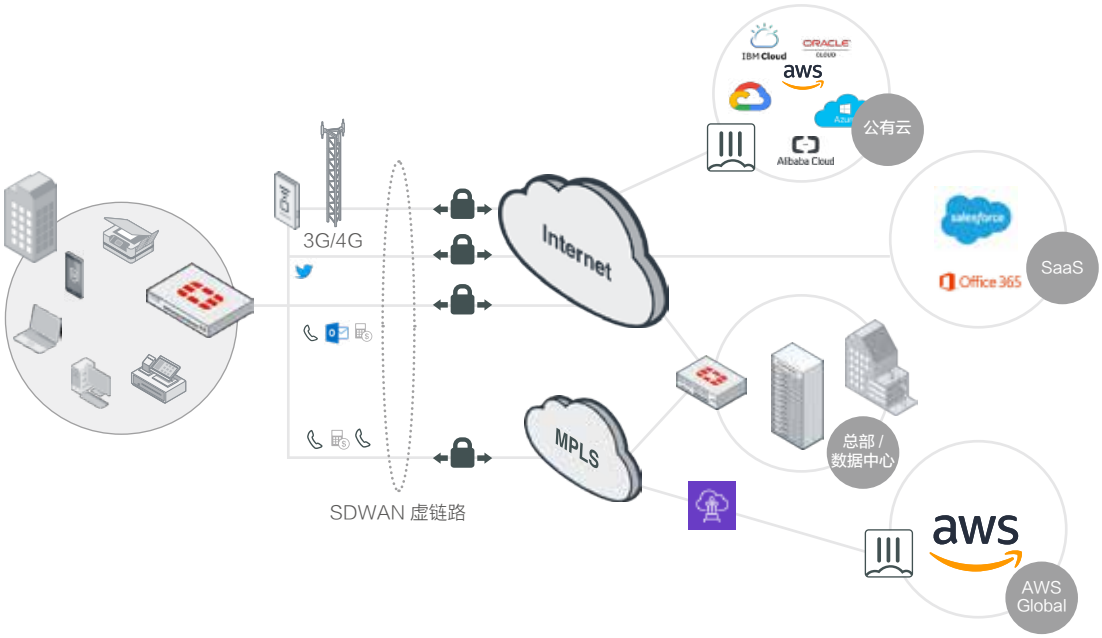


12345 应用 SD-WAN 技术
提升访问体验与品质

一旦业务上云，与 AWS 的交互流量就成了办公网出口中最重要的流量。

如果 AWS 的访问品质出状况，业务访问势必会受影响，正常办公就成了问题。针对越来越多的 AWS Global 访问品质的诉求，Fortinet 推出的 SD-WAN 解决方案可以提升用户对于 AWS 的访问体验。这套方案整合了大量网络优化和业务品质保障的关键技术，为解决 AWS，尤其是海外区域的访问体验问题提供了最具性价比的解决方案。

通过对链路进行丢包 / 延迟 / 抖动等维度的探测，始终让用户访问 AWS 指定站点的流量走当前质量最佳的链路。



通过 Fortinet SD-WAN 解决方案，让用户可以充分利用现有网络线路，大幅提升访问体验：

01 用户目前没有专线，通过 Fortinet SD-WAN 可以持续让访问 AWS 的流量选择质量最佳的线路，并持续监控链路健康状态；

02 用户目前有专线，通过 Fortinet SD-WAN 可以让关键应用、延迟敏感应用流量进入专线，其他流量仍然遵循最优链路选择，降低专线采购成本，均衡应用访问体验；

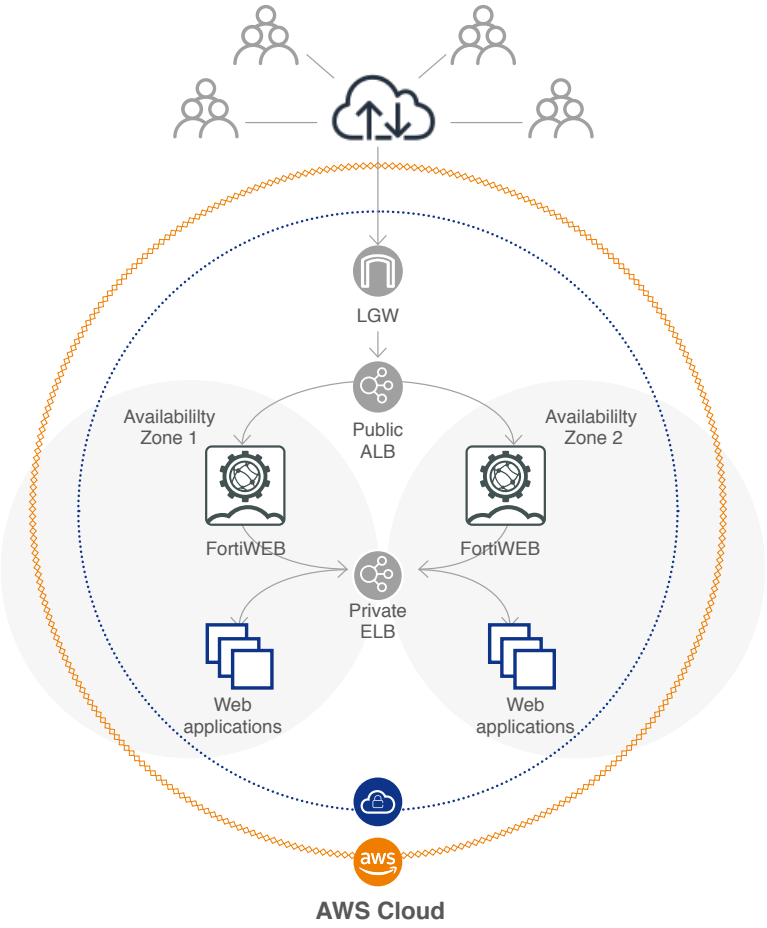
3 WEB 应用安全

基于机器学习的WEB应用防护

企业在采用公有云的早期，普遍会把面向互联网的业务应用迁移到公有云上。因此，Web 安全就成为了企业在考虑公有云安全的时候，仅次于接入安全的内容。Fortinet 的 FortiWeb 是一款十分先进的基于人工智能和机器学习的下一代 Web 应用防火墙（WAF）。

FortiWeb 具备三种机器学习模型：机器学习建立正向异常检测模型，支持联动 FortiGuard 威胁情报生成的机器学习模型，以及支持基于机器学习建立自动识别机器人（bot）动态检测模型。

与在传统环境中部署 WAF 不同，在公有云上 WAF 部署的最佳实践为“三明治”架构，如右图所示：

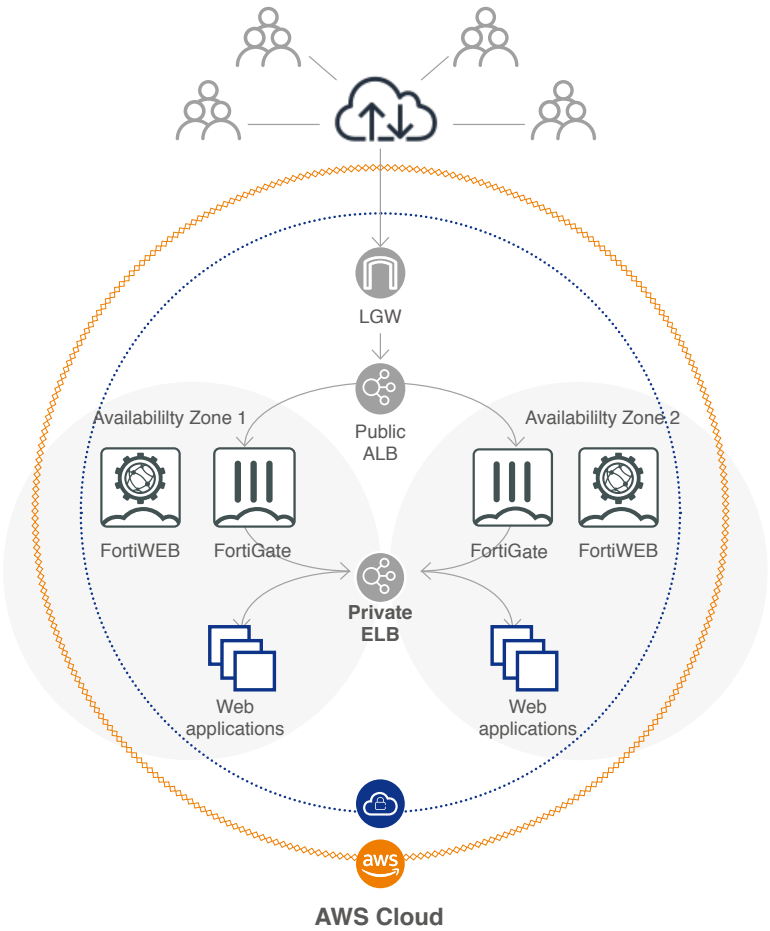


入向流量通过 ALB 负载，并基于内容分流，WAF 专注于管理高级 WEB 安全配置，在访问流量清洗完成后，再通过内部 ELB 将流量分发给应用所在的计算资源（如 EC2）。

FortiWeb Web 应用防火墙适合的场景：

- **攻击场景：**对于网站的常见攻击 SQL 注入，XSS，命令执行等及被挂马，博彩，被篡改。
- **未知攻击场景：**FortiWeb 采取双层机器学习高级安全防御技术和 Sandbox 联动实现对于 0day 攻击防御，恶意上传 0day 攻击文件，如：挖矿程序，勒索软件等。
- **风控场景：**恶意爬虫爬取相关内容及恶意程序访问网站如：恶意刷票 / 抢票，刷赞，恶意注册，撞库等。
- **一体化防御场景：**重要静态页面的防篡改，Web 程序的漏洞扫描，API 的安全防护，防病毒等 Web 安全的立体化防护方案。

4 网络接入与应用安全的组合防御



在将完全面向互联网的应用迁移到云上之后，企业会进行更多内部应用的迁移，比如开发和测试环境、OA 系统、邮件系统，甚至是如 ERP 这样的重型系统。这些应用的共同特点都是只有内部授权用户才能访问。所以在访问安全、网络安全和 Web 安全等方面都需要进行针对性保护。

在架构上，与单纯 WAF 部署一样采用“三明治”结构，如左图所示：

企业内部用户通过本地办公网与云端构建的 IPSec VPN 进行安全连接，远程用户通过安装 FortiClient 进行 SSL VPN 连接到云端，并可以使用双因子令牌增强身份安全。

在 AWS 内部，流量通过 ELB 将负载分摊到两个 AZ 的 FortiGate，在 FortiGate 上启用下一代防火墙的威胁检测和内容识别功能，FortiGate 再将流量映射至内部 ELB FQDN。

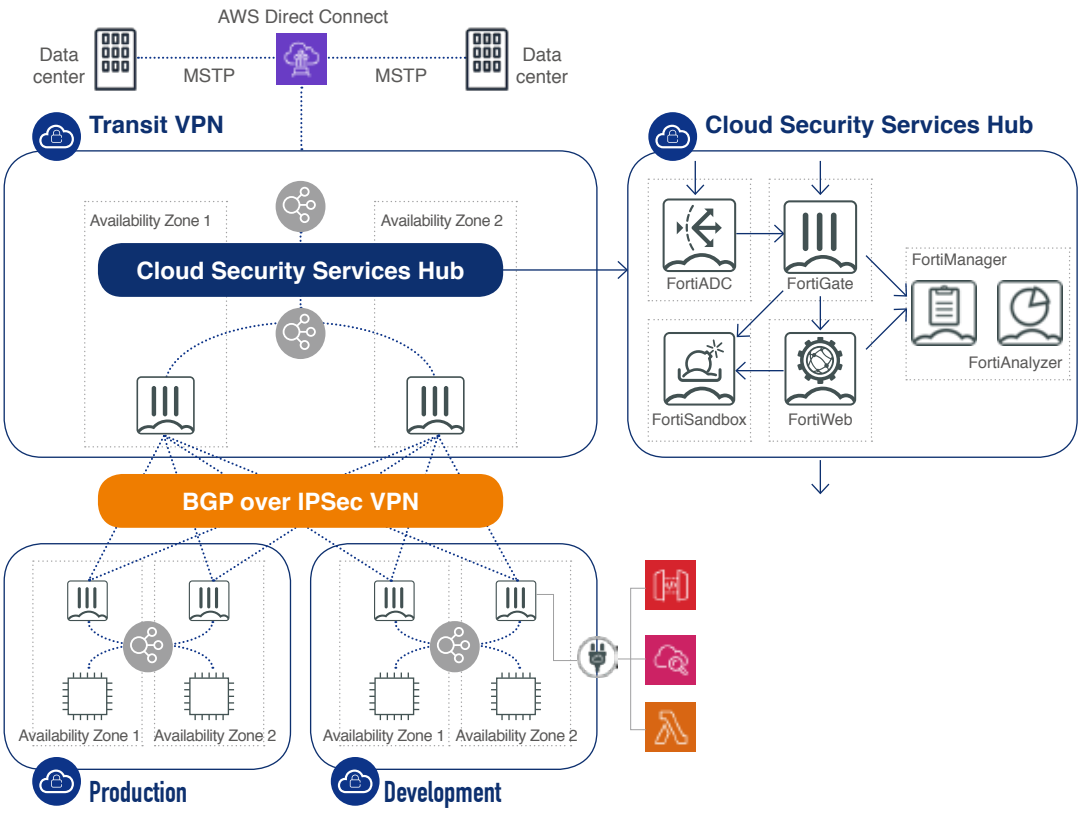
在 FortiGate 下一代防火墙和 FortiWebWeb 应用防火墙的组合部署模式下，FortiGate 会自动将 HTTP/HTTPS 流量转发给 FortiWeb 进行 Web 应用深度安全检查，之后 FortiWeb 将 Web 流量映射至内部 ELB。

5 TRANSIT VPC + CLOUD SERVICES HUB

Transit VPC 是大型企业使用公有云的典型架构，方便进行集中管控。在 Transit VPC 内部部署多种网络和安全产品，直接升级为 Cloud Services Hub，方便进行集中化、多维度、深层次的安全检查，提升安全管理水平。

Transit VPC 的适用场景：对组网有严格的要求；应用场景复杂，有多 VPC 的需求；对于安全策略的管理有严格的要求，需要集中管控；

Transit VPC 能够满足的安全需求：对于应用系统以及 Web 应用的安全的严格安全检查，能够将系统安全和业务安全分离；安全策略的管理严格统一；能够监控 VPC 之间的流量业务安全；



用户可以轻松从 Transit VPC 架构扩展到 Fortinet Cloud Services Hub 架构，即在 Transit VPC 中部署多种 Fortinet 安全产品，如 FortiGate 下一代防火墙、FortiWeb 下一代 WAF、FortiADC 全能负载均衡、FortiSandbox 未知威胁检测系统等等。

部署案例

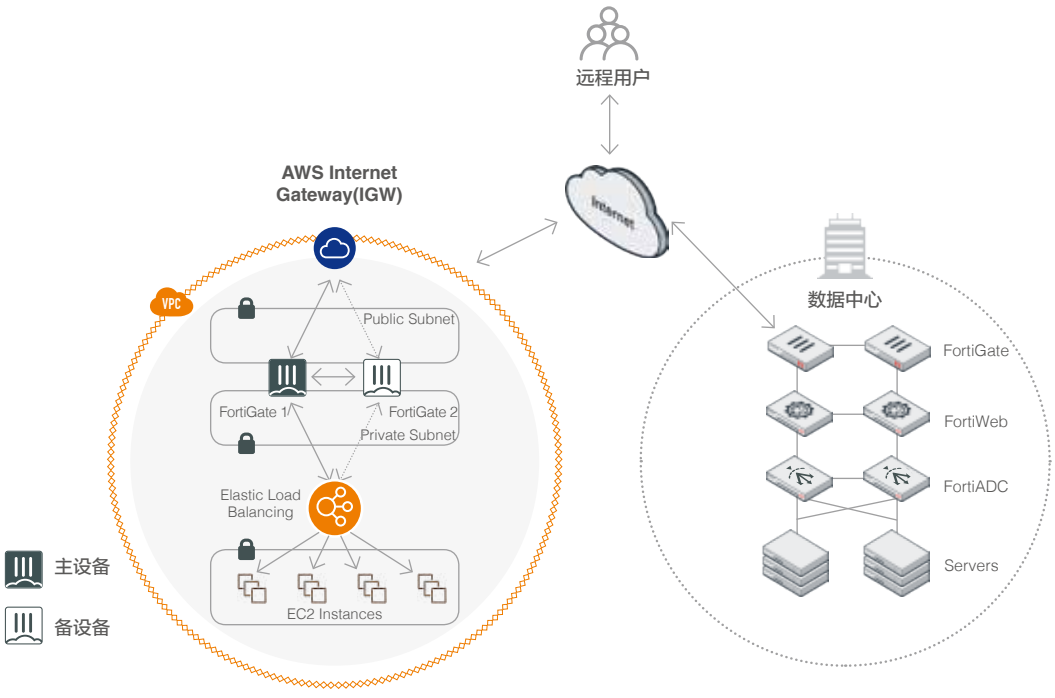
案例一：零售行业客户

由于业务发展的需要，某零售客户需要让门店用户访问位于数据中心和 AWS 云上的系统，需要一套安全可靠的远程拨入系统，Fortinet 使用 FortiGate 防火墙部署在 AWS 云端以实现：

01 FortiGate 提供多因子认证的 SSLVPN 功能（免费），可以提供给远程接入的供应商远程访问 AWS 中资源，并且可以审计用户拨入后的所有行为，解决了安全性需求；

02 FortiGate 与物理数据中心的出口设备建立起 IPSec，将本地数据中心与 AWS 网络打通，组成混合云，解决了互联互通的需求；

03 FortiGate 可以支持在 AWS 的网络中部署为 HA（高可用）模式，最大限度的保证业务连续性（切换时间几乎毫无感知），解决了可靠性的需求；



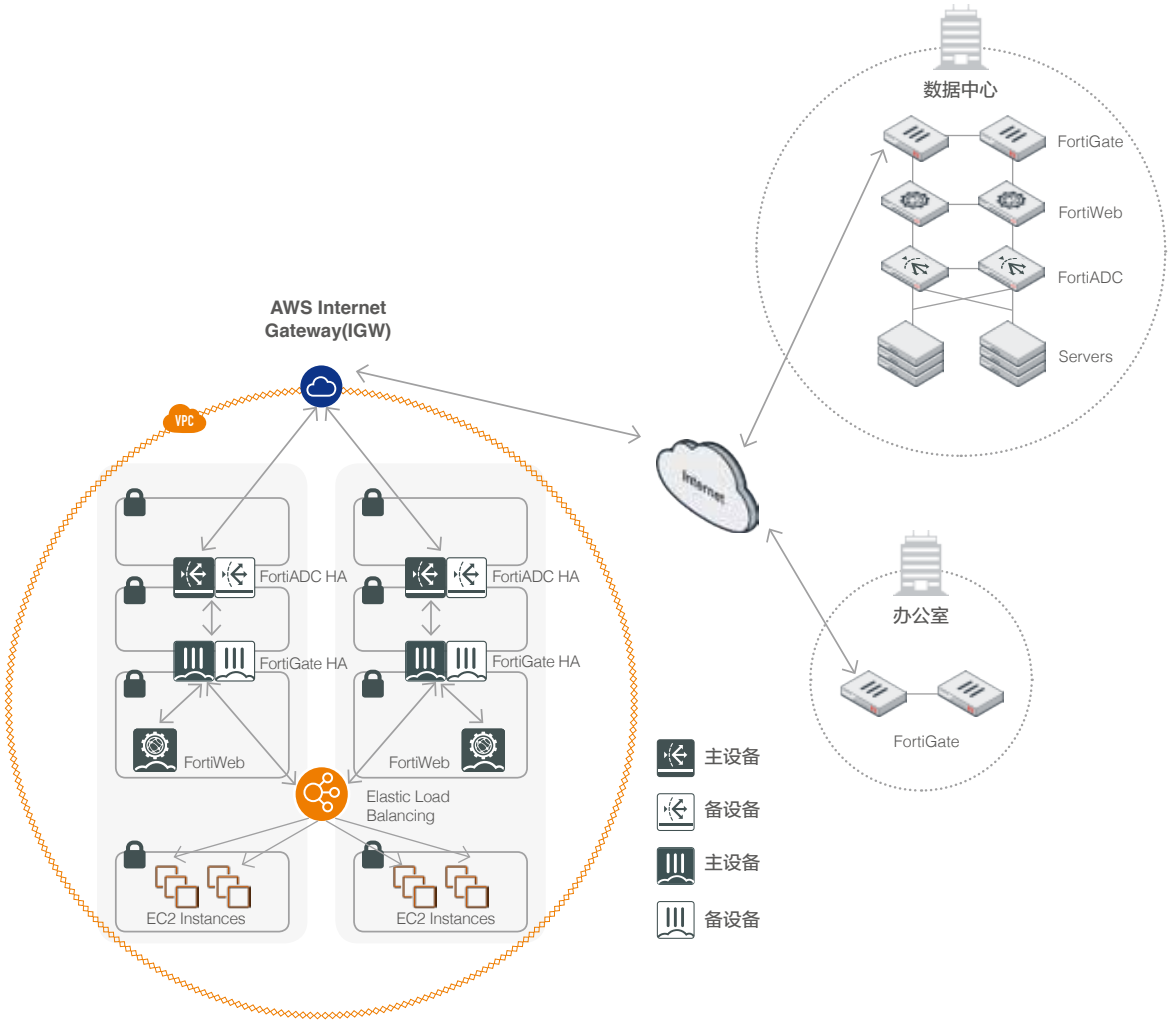
案例二：一般企业客户

某企业客户需要迁移部分业务至 AWS 并且对外提供 Web 服务，需要一套基于 AWS VPC 的整体组网和安全解决方案，Fortinet 使用了 FortiADC（GSLB）、FortiGate（NGFW）、FortiWeb（WAF）三种产品实现了客户需求：

01 FortiADC 启用全局负载均衡功能，使两个 AZ 的流量可以互为备份，并且同时可用，通过这样的部署提高了负载量和冗余性；

02 FortiGate 对外部访问流量进行 NGFW 检测，HTTP 流量检测后会通过私有协议转发给 FortiWeb（WAF）进行应用层代码级别的黑客攻击检测，然后再转发给 ELB 及后台 EC2；提高的 Web 服务器的安全防护能力；

03 除了跨 AZ 的切换之外，FortiADC 与 FortiGate 都支持 HA 方案，并且 HA 不需要借助第三方的 worknode 就可以实现，加强了整体设计的冗余性；



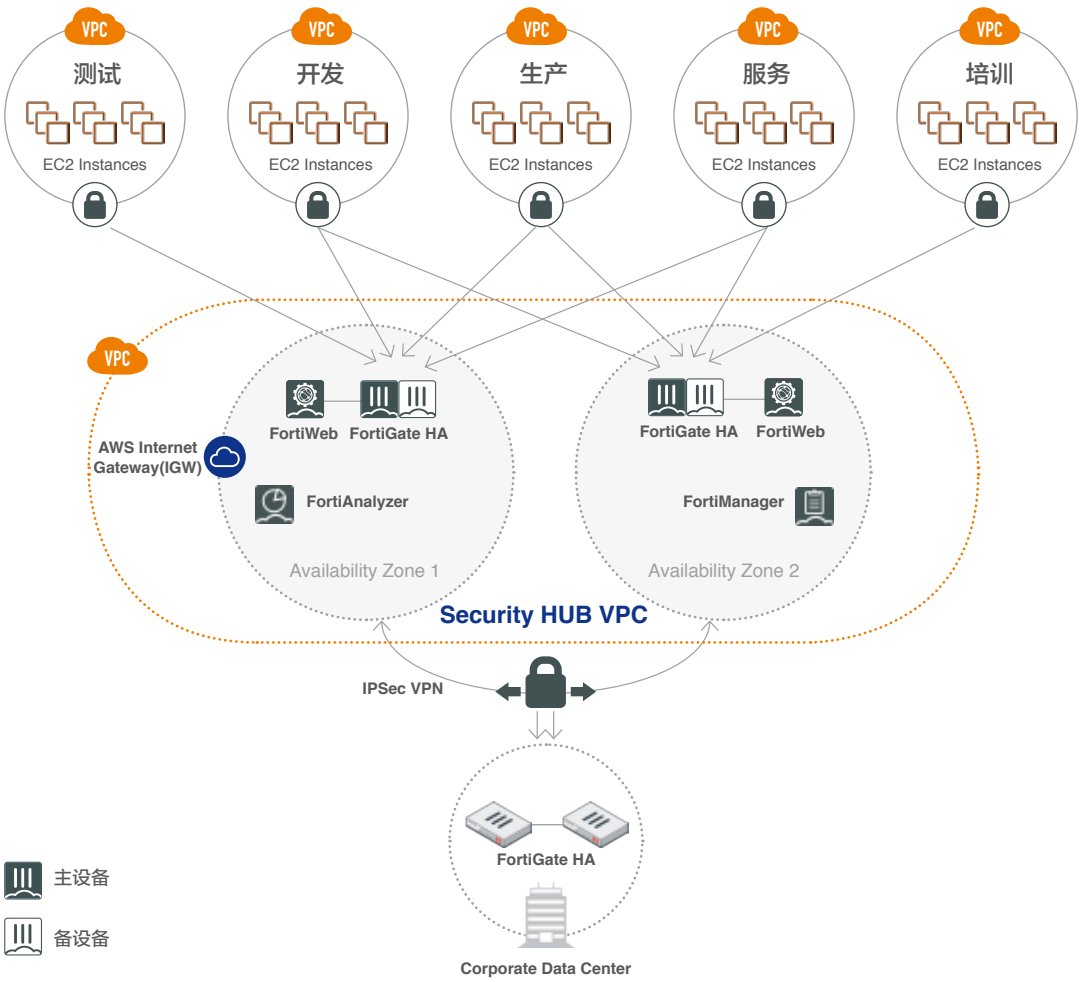
案例三：能源行业客户

某能源行业客户在 AWS 上将不同的业务分别部署在不同的 VPC 中实现隔离，不同的 VPC 互访需求使网络访问缺少统一的安全控制与审计：

01 通过设计一个 Security HUB VPC，在其中部署 NGFW（FortiGate）与 WAF（FortiWeb），再由 FortiGate 用 IPsec 和各个 VPC 的 VGW 打通流量实现了 Security HUB VPC，通过这样的部署所有的流量都会经过 Security HUB 来过滤，实现安全访问控制策略；

02 FortiGate 的 HA 功能最大限度的保证业务连续性，解决了单点故障的后顾之忧；

03 在 VPC 中部署 FortiManager 极大提升了管理效率，由于 Security HUB 的部署 FortiAnalyzer 上可以审计所有访问的流量日志及安全事件日志，根本上保障了业务整体安全性；



通过 AWS Marketplace 进行快速构建

Fortinet 是 AWS Marketplace 中提供安全服务涉及面最广，付费模式最灵活的合作伙伴。通过与 AWS 进行的云原生集成，使用户可以获得同样足够弹性和可靠的安全方案部署。用户现在可以同时在 AWS Marketplace China 和 AWS Marketplace Global 上快速构建属于自己的云安全能力。Fortinet 在 AWS 上交付的核心安全能力包括下一代防火墙，入侵防御，Web 安全，SD-WAN，IPSec/SSL VPN，安全 Web 网关，统一管理平台，日志分析平台，统一身份管理与认证，沙箱等都能够以 AMI 的形式在 AWS Marketplace 中直接启用。Fortinet 还提供了预开发的 CloudFormation 模板来加速用户进行 DevOps 相关的高阶构建。

aws marketplace

AWS Marketplace 是一种数字化产品目录，收录了来自独立软件供应商的数千种软件产品，可让客户轻松查找、测试、购买和部署在 AWS 上运行的软件。AWS Marketplace 上的每种产品都经过精挑细选。

目前 Fortinet 在 AWS Marketplace China 已经上架的产品：

FortiGate-VM (BYOL)	Fortinet 旗舰产品，融合下一代防火墙，SD-WAN CPE，IPSec/SSL VPN 网关于一身。
FortiWeb-VM (BYOL)	基于机器学习的下一代 Web 应用防火墙。
FortiAuthenticator (BYOL)	统一认证服务器，可以结合 FortiToken 实现双因子认证。
FortiAnalyzer (BYOL)	为 Fortinet 安全产品提供统一的日志收集、分析和实时合规审计。
FortiManager (BYOL)	为 Fortinet 安全产品提供统一的管理平台，快速部署、配置变更推送、版本维护等等。
FortiADC (BYOL)	全面的负载均衡产品，包含链路负载，服务器负载，全局负载，智能 DNS 等功能。
FortiSandbox (BYOL)	未知威胁检测，高级恶意软件检测，与 S3 紧密集成，保护文件存储安全。

了解更多 Fortinet 在 AWS 上的产品信息，可以访问 **AWS Marketplace** 网站中列出的 Fortinet 相关产品。

FORTINET®

北京
北京市海淀区北四环西路 58 号理想国际大厦 713 室
电话：010-62960376

上海
上海市徐汇区凯滨路 183 号保利西岸中心 B 座 601 室
电话：021-64261500

广州
广州市天河区珠江西路 15 号珠江城大厦 1608
电话：020-38105509

官 方 网 站 **www.fortinet.com/cn**
技术支持中心 **support.fortinet.com.cn**
咨 询 热 线 **400 600 5255**