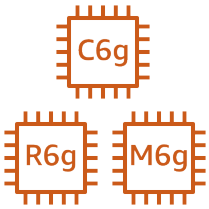
FORTINET

FortiGate在亚马逊云科技上的五大应用场景

www.fortinet.com

亚马逊云科技

首款在中国区域 Marketplace 支持 PAYG 订阅模式的 SD-WAN 与下一代防火墙



首款在全球和中国区域支持 Graviton2 系列实例的 SD-WAN 与下一代防火墙

与如下亚马逊云科技服务紧密集成

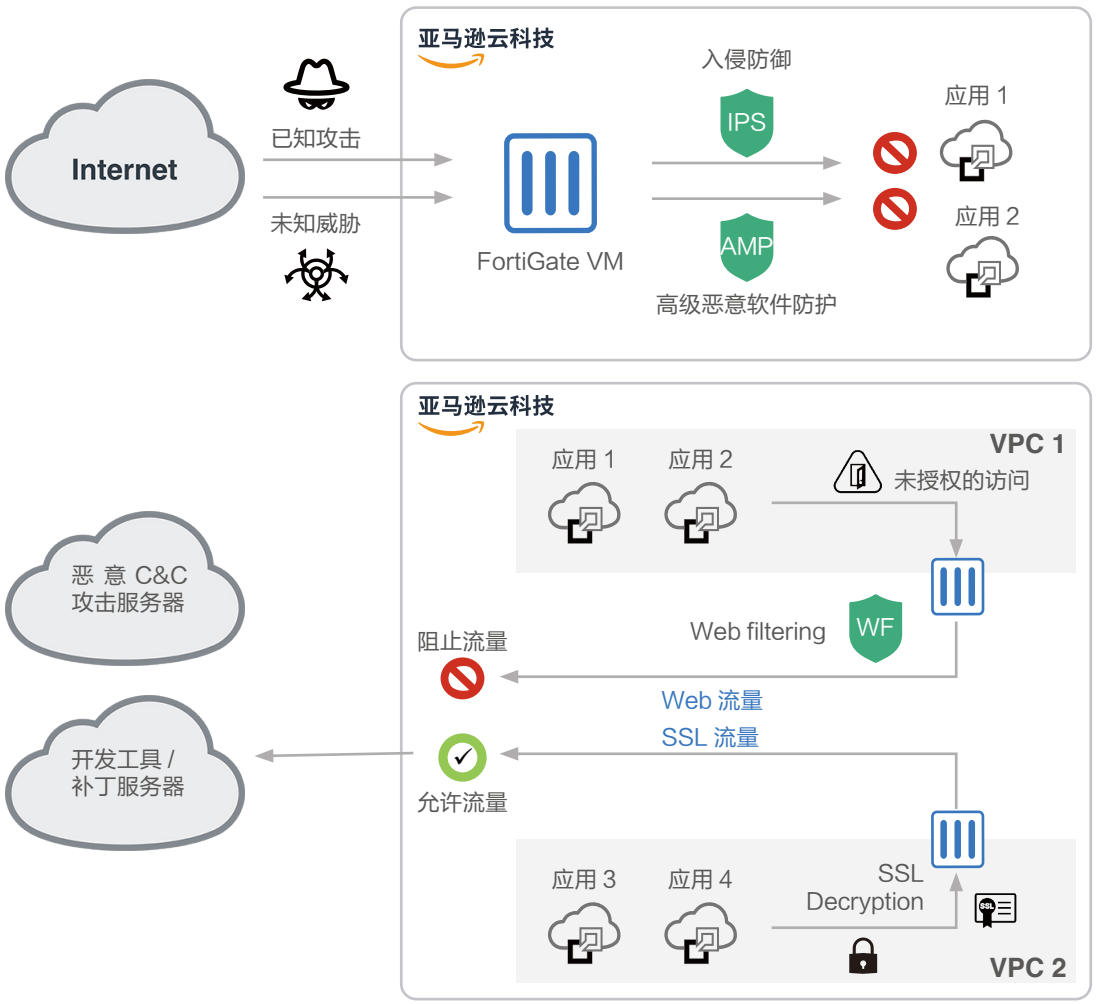
- 亚马逊云科技 Transit Gateway (TGW)
- 亚马逊云科技 Lambda
- 亚马逊云科技 Cloud WAN
- 亚马逊云科技 Gateway Loadbalancer (GWLB)
- Amazon VPC Traffic Mirroring
- Amazon GuardDuty
- Amazon Elastic Kubernetes Service (EKS)

CONTENTS / 目录

FortiGate 是集防火墙、入侵检测与防御、高性能 SSL/IPSec VPN 网关、SD-WAN、零信任于一身的全功能防火墙产品，也是唯一同时入围 Gartner 企业防火墙和 SD-WAN 魔力象限双料领导者的产品，具有性能高，安全效果好，功能丰富等特点。如用户在本地和云端进行安全组网、安全隔离、流量检查、行为监测、全球加速、私有应用保护等场景，FortiGate 将是理想选择。

FortiGate 与亚马逊云科技平台进行了 API 级别的集成，能够支持同 AZ 和跨 AZ 的主备 / 双主高可用部署模式。FortiGate 同时支持中转网关（TGW），网关负载均衡（GWLB），流量镜像（Traffic Mirroring）等服务集成，能够用来帮助用户构建云安全服务中心来实现安全集中管控与关键资产的流量与威胁可视化。在自动化响应方面，FortiGate 可以通过 API 获取实例 ID，实例类型，子网，安全组，AZ，标签等等信息，并通过内置的轻量级编排引擎，自定义触发条件（如实例连接到恶意 IP）并执行自动化响应动作（如调用 Lambda 脚本隔离实例）。

1. 云边界安全网关—NGFW



使用场景

不论是办公室，园区网，数据中心，还是公有云，边界安全网关是企业网络安全建设的第一步，也是必不可少的一步。虽然亚马逊云科技为客户提供了基础的网络隔离功能，可以通过 Network ACL 和 Security Group 分别对子网和 EC2 进行流量的访问控制，但是功能过于简单，无法承担边界安全网关的职能。

在亚马逊云科技云边界，用户需要一个功能丰富的云边界安全网关，能够同时支持网络防火墙，流量威胁检测，NAT 网络地址转换，IPsec VPN，SSL VPN，SD-WAN，甚至是应用安全代理等功能，通过一个界面对在云边界需要的功能进行一站式配置、监控、检测与可视化。

FortiGate 优势

FortiGate 是长达 10 余年 Gartner 网络防火墙魔力象限领导者，出货量占有全球安全网关 38% 的份额，深受各种行业和各种规模客户的一致好评。作为云边界安全网关，FortiGate-VM 可以为用户提供全面的网络与安全功能，并和亚马逊云科技网关负载均衡（GWLB）服务进行集成，以提升部署灵活性，提供可线性扩展的性能，进而保护客户业务连续性。

用户部署 FortiGate-VM，即可获得下一代防火墙，入侵检测与防御，IPSec VPN，SSL VPN，SD-WAN，零信任网络访问 ZTNA，网络地址转换 NAT 等功能。基于 FortiGate 内置的云连接器和自动化引擎，用户可以根据亚马逊云科技上的属性信息来定义自适应的防火墙策略，摆脱传统基于 IP 的策略定义，大幅减小运维工作量。

客户价值

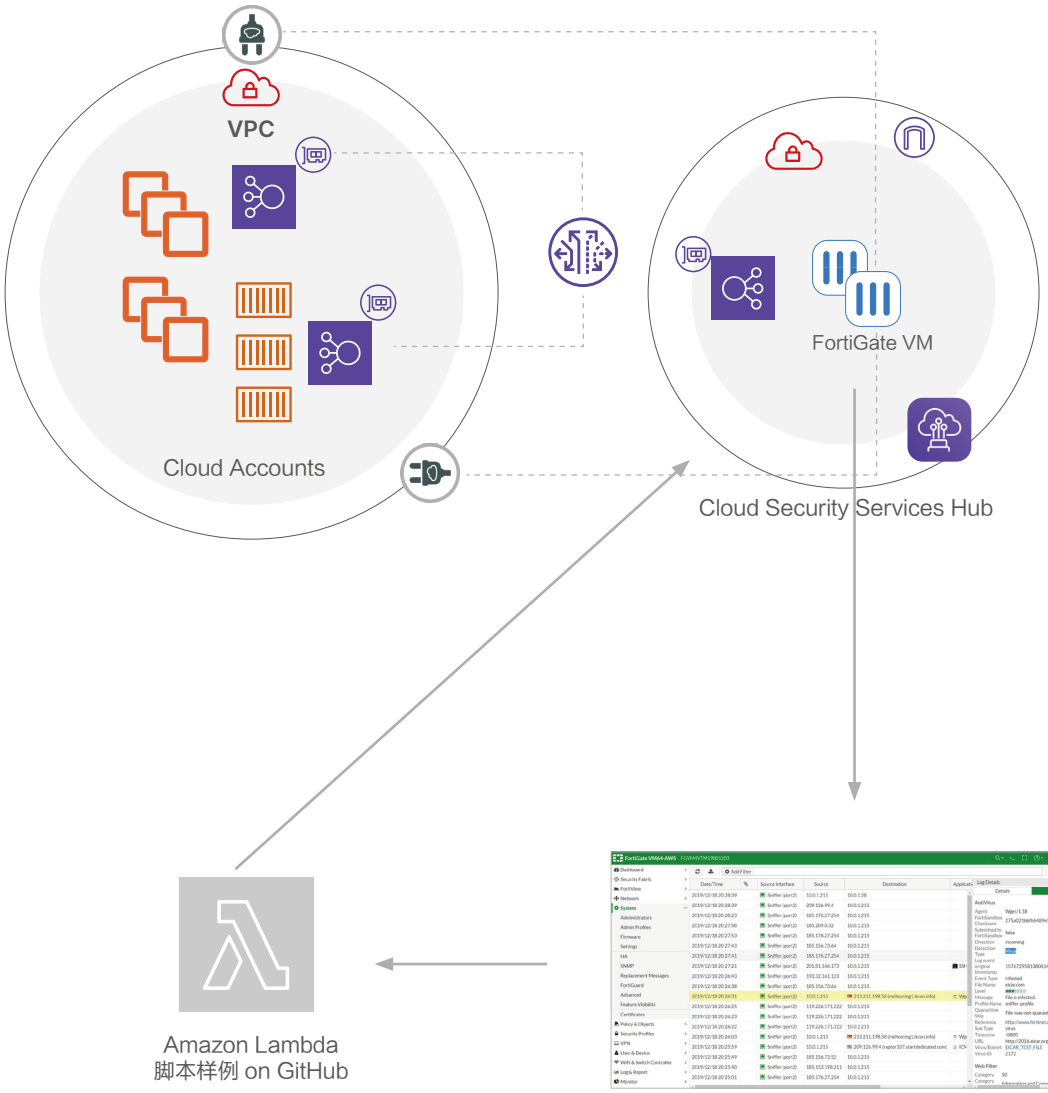
用户需要组合亚马逊云科技提供的多项服务才可以实现一部分云边界网关的功能，而相关的组网功能（如 SD-WAN，IPSec VPN），安全访问功能（SSL VPN，ZTNA）在亚马逊云科技中国甚至全球区域都是不具备的。

在亚马逊云科技 Marketplace 上订阅及部署 FortiGate-VM 后，用户可以通过 FortiGate 简单易用的管理控制界面配置所需的网络和安全功能，同时获得全面的流量和威胁可见性。

2. 云内威胁检测与响应—IPS

Sniffer mode | Scale out | Automation Stitches

VPC Traffic Mirroring



使用场景

与数据中心一样，公有云上也部署着企业关键业务应用，对企业生产力起着至关重要的作用。现代化应用需要使用大量组件，或商业，或开源，来构建整个企业应用，其中必然包含已知或未知漏洞，成功的漏洞利用，必然产生数据泄露，或应用宕机，这都是应该着力避免的。使用入侵防御系统 (IPS) 可以防止针对云上工作负载中已知漏洞的攻击，并为暂时无法修复的新漏洞提供虚拟补丁，以达到缓解攻击的目的。

FortiGate 优势

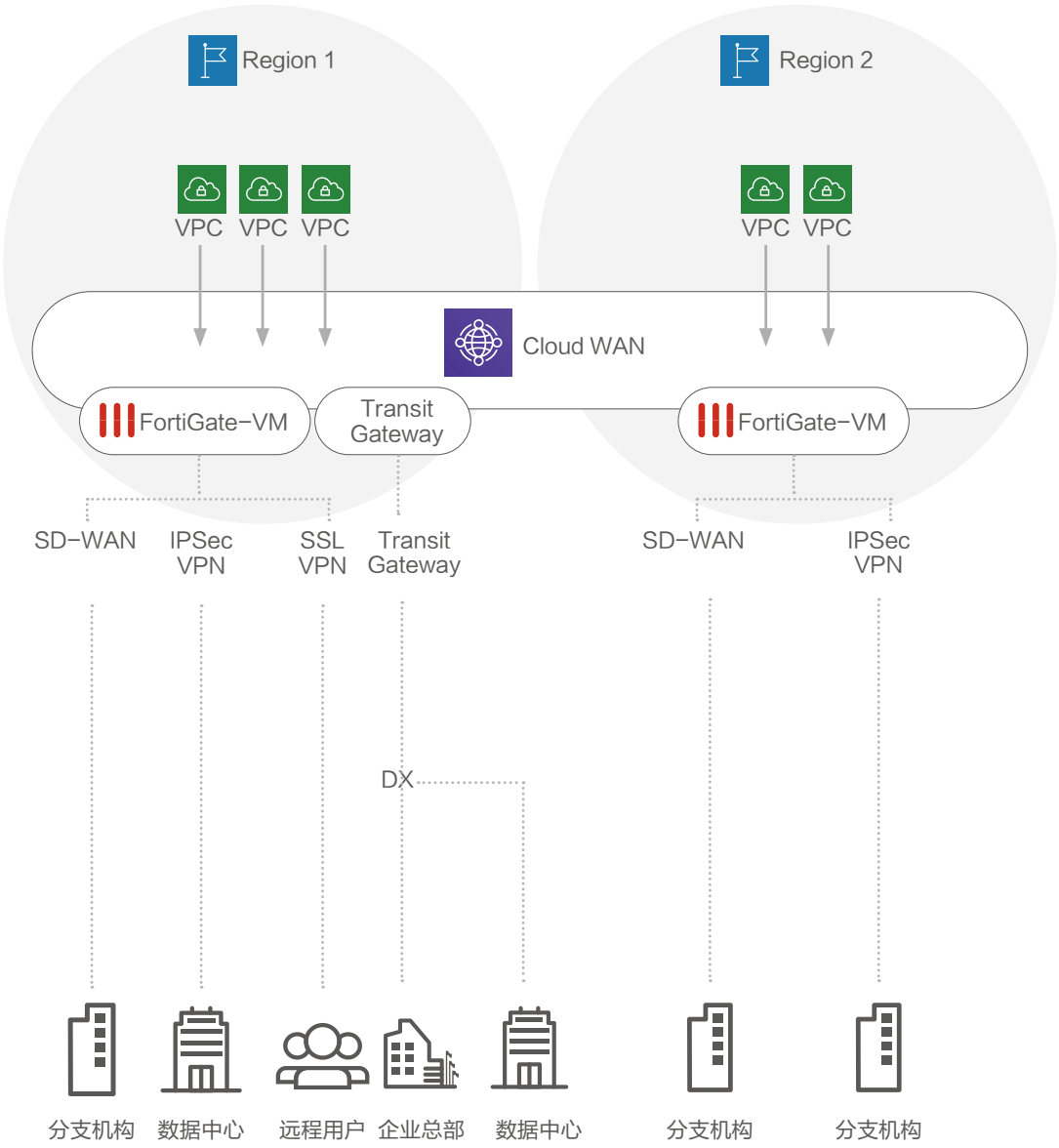
Fortinet FortiGuard 实验室为 FortiGate 提供近乎实时的攻击情报，具有数千条 IPS 规则，可在已知和零日威胁到达设备之前检测并阻止它们。FortiGate IPS 在检测针对应用漏洞的攻击之外，还可以检测主机流量中是否有僵尸网络的连接，同样依赖于 FortiGuard 提供的全球威胁情报，提供实时检测与阻断。

FortiGate 可以串行部署在用户亚马逊云科技 VPC 中，如集成网关负载均衡（GWLB），也可以与亚马逊云科技 Traffic Mirroring 服务集成，进行旁路检测，这样用户无需变更当前架构即可使用 FortiGate IPS 能力实现针对关键资产的威胁检测。如需进行响应，用户可以使用 FortiGate 内置的自动化引擎调用预定义亚马逊云科技 Lambda 对受感染或受攻击主机进行隔离操作。

客户价值

提升 VPC 内和 VPC 间的流量可见性，并提供友好的可视化展示，并与亚马逊云科技 Lambda 集成，实现旁路威胁检测的同时进行自动化安全响应。有效补充亚马逊云科技在流量威胁检测方面的不足，同时灵活的部署选择，可以最大程度降低引入安全解决方案对业务产生的影响。

3. 出海加速与混合 IT 组网—SD-WAN



使用场景

教育、医疗、生命科学及高科技、金融科技、跨境贸易与电商、跨境营销等行业在日常科研及办公活动中通常需要访问全球学术资源、公有云 SaaS 服务以及相关应用等等。而互联网天然无法保障传输的可靠性、稳定性和安全性，自然无法提供确定性的应用体验。

此外，混合 IT 是用户当前主要采用的模式，公有云 IaaS，私有云，数据中心，总部和分支办公室等位置都需要实现全面的可靠且安全的连接，从而为员工提供良好的应用访问体验，以及部署在不同位置的应用间进行稳定连接。

FortiGate 优势

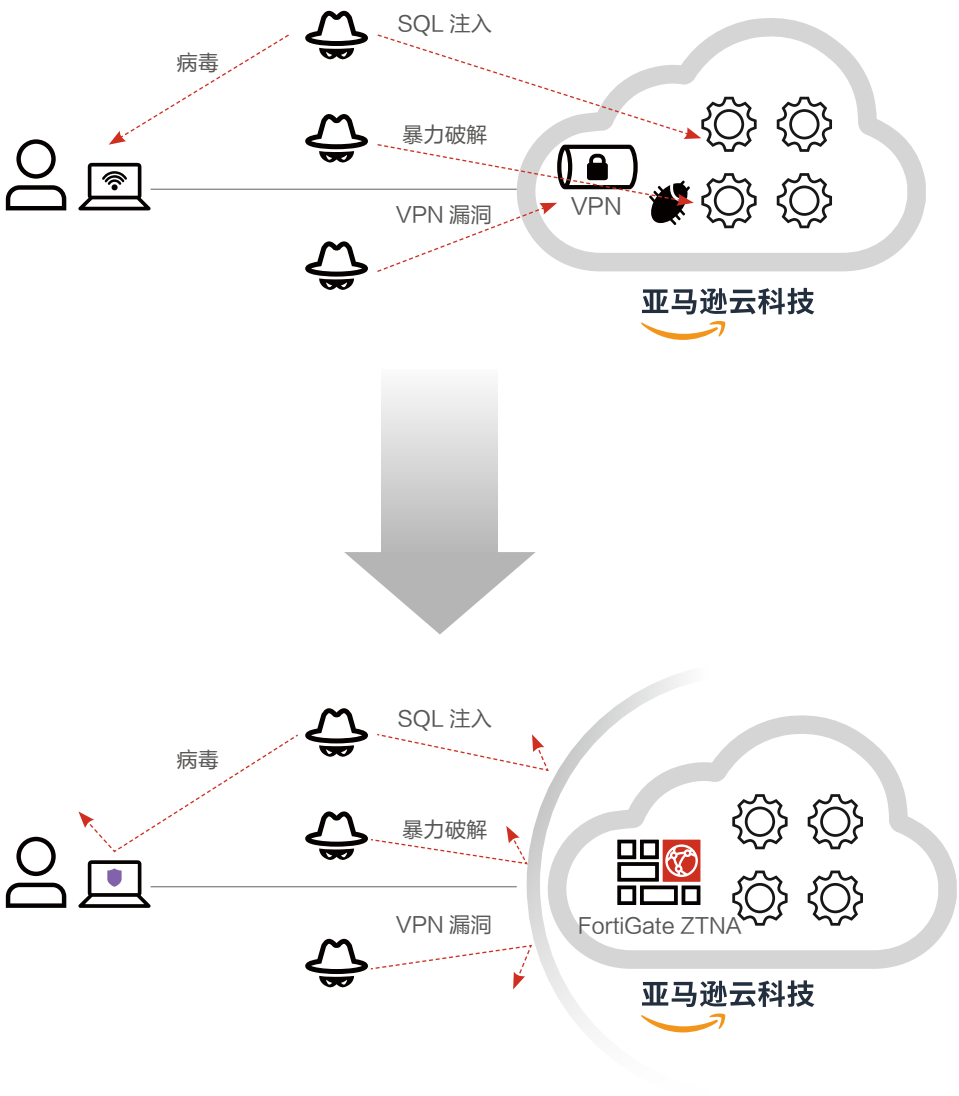
FortiGate 是唯一同时入围 Gartner 企业防火墙与 SD-WAN 魔力象限领导者的产品。依托于业界领先的应用级路由优化技术，FortiGate 可以为用户提供可靠的应用访问质量保障，以及可观测的网络性能关键指标（如：延迟、抖动、丢包）。确保用户的关键业务流量可以被稳定的路由到高质量精品线路，确保应用访问体验得到足够的优化。

FortiGate 可以与亚马逊云科技中转网关（TGW）以及 cloud WAN 进行集成，将亚马逊云科技 VPC 与用户本地网络实现便捷连接，且无需使用多个管理控制台，实现运维简化。即使作为 SD-WAN 设备，FortiGate 仍然可以是一台极其强大的防火墙，且无需支付额外成本，帮助用户实现 SD-WAN 组网的情况一下，提供全面的安全保护，如入侵防御，反病毒，僵尸网络阻断等等。

客户价值

无需在亚马逊云科技平台手工配置大量静态路由策略，使用 FortiGate 一台设备，一个管理界面，基于动态路由，应用感知路由，可观测的监控，自适应修复等技术，实现全球应用加速，混合 IT 组网与安全管理，大幅降低运维复杂度，提升生产力。

4. 零信任访问应用网关—ZTNA



使用场景

当前企业通常在公有云和本地都有部署业务，若要让远程用户安全访问部署在多个位置的业务应用，则需要首先把多地网络进行安全连接，因为传统的 SSL VPN 只能同时连接一个 VPN 网关，无疑会产生流量绕路的情况，不仅会影响使用体验，也会增加企业互联网带宽压力。而且 SSL VPN 也无法根据终端安全态势进行动态授权。与此同时，暴露在互联网上的企业私有应用，也会遇到大量攻击，增加应用安全风险。

因此企业需要能够直接和应用建立安全隧道的远程访问方法，并结合多维度精细化的访问权限管控和持续的安全检查，即 ZTNA- 零信任网络访问。在实现精细化应用访问安全控制的情况下，为原本暴露在互联网上的应用进行“隐身”，使其免受来自互联网的多种攻击影响。

FortiGate 优势

FortiGate 是唯一支持完整 SD-WAN 和 ZTNA 的下一代防火墙产品。因此可以实现在云边界网关的位置上同时承担 ZTNA 代理网关的角色。FortiGate 可以为安装 FortiClient VPN/ZTNA 客户端的用户同时提供 SSL VPN 和 ZTNA 功能，为用户提供最大化的便利并保障安全。

与常见的 ZTNA 方案不同的是，FortiGate 不只是零信任访问应用网关，同时也为来自终端的访问流量进行流量深层检测，以发现并遏制攻击。

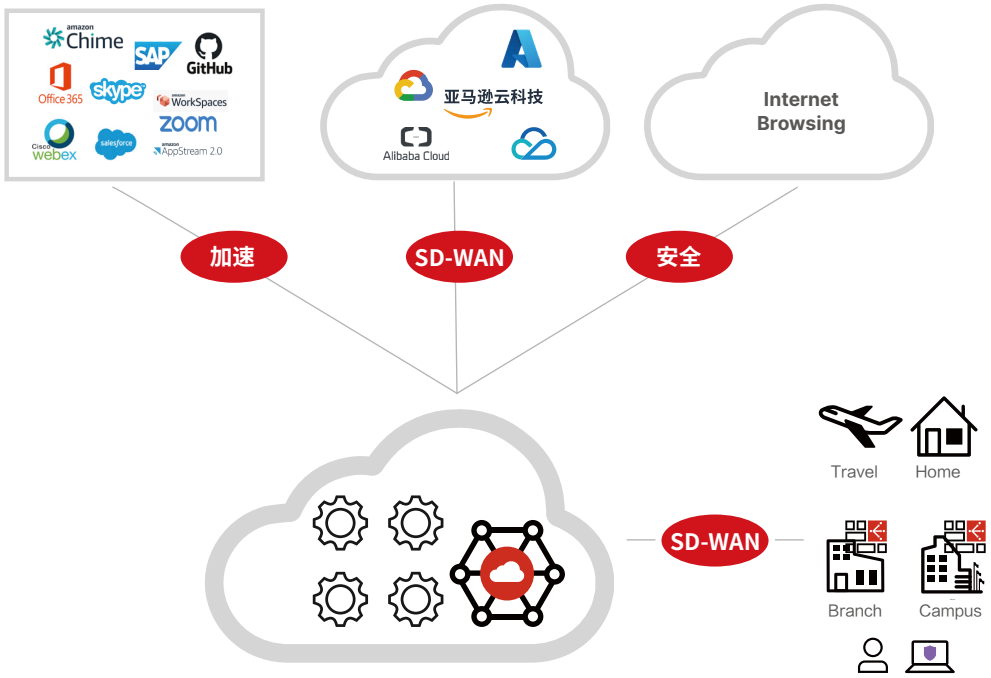
用户使用 FortiGate，即可获得 ZTNA 能力，无需采购额外软硬件及授权，甚至无需变更当前网络架构。同时支持单点登录和多因子认证，也可与客户现有身份平台轻松集成（如 AD, LDAP 等等）

客户价值

用户不仅可以获得 ZTNA 零信任访问应用网关，还同时获得业界领导者地位的下一代防火墙及 SD-WAN。如用户已经部署 FortiGate 在边界网关处，即可直接获得 ZTNA 能力，实现投资回报率最大化。

原有暴露在互联网上的私有应用可以实现从互联网隐身，免受泛滥的扫描攻击，及针对性攻击的影响。也可以让远程用户同时使用 SSLVPN 和 ZTNA 实现安全远程访问，确保应用访问安全，并获得最佳应用访问体验。

5. 私有化 SASE 平台



URL 过滤	应用控制
反病毒 支持云沙箱	下一代防火墙 FW+IPS
QoS 带宽控制	SD-WAN 基于应用的路由
数据泄露防护	代理 支持 SSL 深度检测

混合办公安全
互联网访问

应用隐身	设备安全态势
应用隔离	每会话检测
ZTNA 策略 Tag based	流量检测 IPS/AV
动态双因子 2FA	增强型 SSLVPN

混合办公安全
私有应用访问

使用场景

为保障远程办公人员访问互联网安全，企业当前通常会选择将总部办公室或数据中心作为 SSL VPN 网关所在地，所有远程办公人员的所有流量都需要回到总部网关，即使是非内网应用访问的普通互联网流量或 SaaS 访问流量。这样不仅增加了本地互联网带宽的压力，也会带来额外的延迟，以及本地硬件网关设备的性能压力，一旦远程办公需求激增，本地带宽和硬件以及相关授权又不能弹性扩展，必然会影响员工生产效率。

因此企业可以在云上部署可以弹性扩展的互联网访问安全网关，以满足远程办公的安全需求，并兼顾访问体验。

FortiGate 优势

FortiGate 在防火墙，IPS，SD-WAN，ZTNA 之外还拥有拥有众多功能，以保护互联网访问安全，如：Web 过滤（90+ 分类，上千万条 URL），应用控制（5500+ 应用签名），DNS 过滤，IP 信誉，僵尸网络防御等等。

FortiGate 还可以使用 IPSec VPN 与企业本地环境进行安全互联，解决远程用户在访问互联网的同时还需要访问本地资源的需求。

客户价值

可以为远程办公人员提供可以弹性扩展的互联网访问安全网关，降低本地带宽压力与成本，提升员工办公体验。

可以同时获得零信任访问应用网关—ZTNA，一个平台，一个管理界面即可保护互联网访问和私有应用访问安全。

关于高可用性

FortiGate-VM for 亚马逊云科技支持高可用性 (HA) 方法如下：

- FortiGate-VM 双主 HA
- 基于 ELB 的 HA/ 负载均衡
- 单 AZ 主备 HA
- 多 AZ 主备 HA

与亚马逊云科技集成的服务

- 亚马逊云科技 Transit Gateway (亚马逊云科技 TGW)
- 亚马逊云科技 Lambda
- 亚马逊云科技 Cloud WAN
- 亚马逊云科技 Gateway Loadbalancer (亚马逊云科技 GWLB)
- Amazon VPC Traffic Mirroring
- Amazon GuardDuty
- Amazon Elastic Kubernetes Service (EKS)

与亚马逊云科技集成的 FortiGate SDN 连接器

以下 SDN 连接器集成可用于使用 SDN 连接器自动更新亚马逊云科技的动态地址：

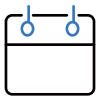
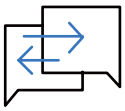
- 基于证书的 SDN 连接器集成
- 使用 IAM 角色配置亚马逊云科技 SDN 连接器

以下是亚马逊云科技提供的其他 SDN 连接器集成选项：

- 亚马逊云科技 Kubernetes (EKS) SDN 连接器
- 接收从 GuardDuty 推送的威胁信标
- 使用亚马逊云科技 Lambda 实现流水线自动化
- 使用动态地址对象配置 FortiGate-VM 负载均衡器
- 使用 SDN 连接器通过 VPN 访问云服务器
- 支持亚马逊云科技 STS 的 sdn 连接器

FortiGate-VM 支持的订阅模型

最具灵活性的网络安全融合平台，满足客户多样的使用需求

PAYGO		BYOL		
				
按小时或按年订阅	按月付费	永久许可 + 按年服务	1 年或多年订阅	按天计费按月付费

新增支持：亚马逊云科技中国区域

授权方式

云实例


计量收费 VM


按小时计费

PAYG(即付即用)
按月或按年付费

亚马逊云科技市场

适用于
单一云应用场景

永久许可


FG-VM


FG-VMv


一次性付费

预付费
无期限限制

BYOL(自带许可)

适用于
长期静态本地应用场景

定期许可


FG-VM-S


1 年 /3 年 /5 年

预付费
固定合同期限

BYOL

适用于
稳定可预测用量场景

Flex-VM 企业版


Flex-VM


按天计费

预付费 + PAYG
固定合同期限

BYOL

适用于
混合云及多云环境应用场景

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

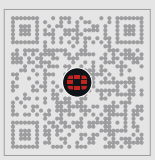
上海
上海市徐汇区凯滨路183号保利西岸中心B座601室
电话：021-64261500

广州
广州市天河区珠江西路15号珠江城大厦4301
电话：020-38105507

南京
南京市玄武区中山路18号德基广场二期写字楼24楼2420室
电话：025-85953896

杭州
杭州市西湖区学院路28号德力西大厦1号楼9楼901,903,904室
电话：0571-28091288

深圳
深圳市南山区科发路19号华润置地大厦D座5层127室



官　方　网　站 www.fortinet.com/cn
技术支持中心 support.fortinet.com.cn
售　后　服　务 400 600 5255
产品及方案咨询 010-62960376转1　BDR_cn@fortinet.com