下一代防火墙
VPN网关

技术参数
基于AWS的FortiGate®-VM

基于AWS的FortiGate-VM所提供的下一代防火墙及VPN功能，适用于不同规模的企业与组织在AWS云上的安全防护部署选择。FortiGate-VM具有出色的性能、高效的安全效能的同时提供了深度的网络可视化。

安全能力：

- 利用FortiGuard威胁研究与响应实验室发布的安全服务与威胁情报持续不断针对已知与未知漏洞利用、以及恶意软件提供动态防御
- 识别超过5000的应用程序，包括云应用程序，对网络流量进行深度检查
- 利用动态分析主动防御未知攻击，并通过自动化流程阻断攻击
- 对来自AWS GuardDuty威胁检测服务进行自动化事件响应与威胁情报利用

第三方认证与认可：

- Fortinet解决方案所提供的安全有效性及性能均经过权威第三方测试与验证
- 获得NSS Labs、ICSA及Virus Bulletin与AV Comparatives等机构的认证
- Fortinet 是AWS（Security Competency）安全能力级合作伙伴

网络功能：

- 提供全面的路由、交换及VPN功能
- 针对AWS健康度检查的高可用性设计

管理功能：

- 虚拟设备及物理设备均可以通过统一管理窗口管理
- 根据EC2自动伸缩安全配置
- 全面的许可证选择可适用于任何基础架构的需求
- 支持多租户环境的VDOM模式（只限BYOL许可证支持VDOM）

Security Fabric安全架构协同：

- Fortinet Security Fabric安全架构支持多产品及开放式合作伙伴之间的协同于联动，使安全能力能够覆盖到整个攻击平面。

Fortinet在AWS云上具有完整且综合的安全解决方案。

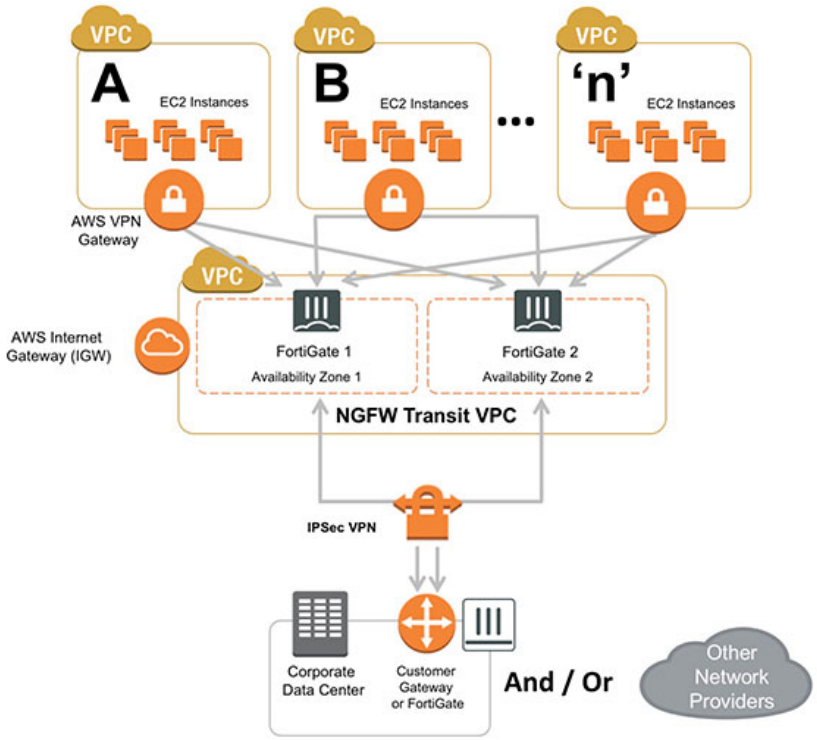
部署

下一代防火 墙(NGFW))

- 将全面的威胁防御能力整合并应用到AWS内的FortiGate实例
- 企业级拓扑构建能力，提供细粒度的设备、用户及威胁信息可视化;极大降低部署复杂性
- 多次获奖的入侵防御系统可深度检测网络流量的应用层内容，识别并阻断威胁与入侵
- 通过Security Fabric安全架构的联动与协同能力可扩展安全防御的平面

VPN网关

- 利用SSL与IPSe VPN构建连接安全
- VPC之间通过VPN建立安全的连接
- 支持混合云之间站点到站点的IPsec VPN
- 远程拨号VPN安全连入AWS VPC



FortiGate-VM on AWS部署为下一代防火墙和VPN网关

AWS集成

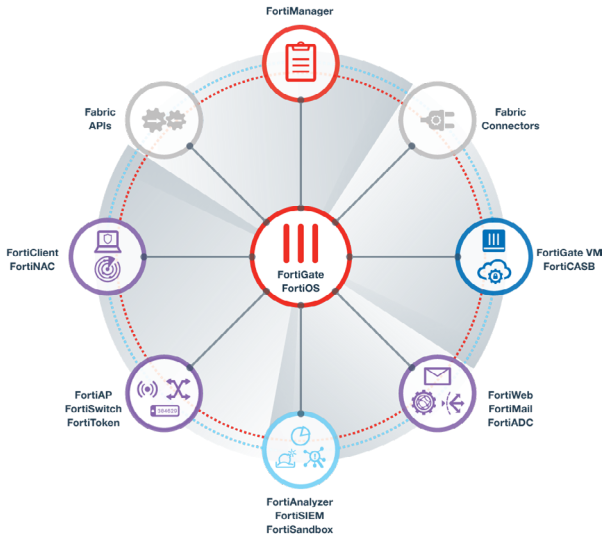
- Fortinet将AWS最新的自动伸缩功能与FortiGate CloudFormation 模版配置嵌入到Security Fabric安全架构中，提供基于云工作负载资源需求的自动化。
- 自动将恶意IP或DNS地址同步到动态FortiGate策略，与AWS GuardDuty联动，有效防护新威胁。
- 支持通过AWS原生的流量负载提供弹性服务。

Fortinet Security Fabric

安全架构

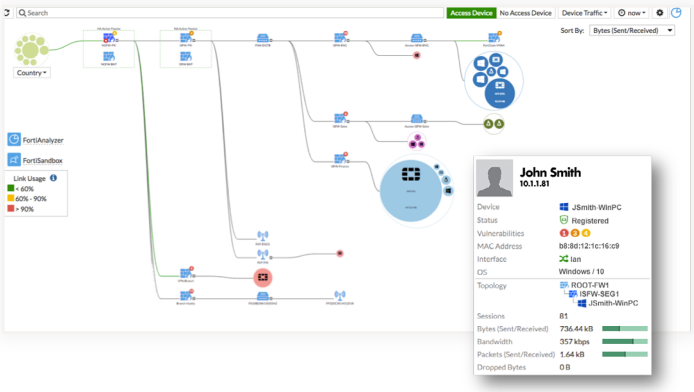
Security Fabric安全架构极具开放与整合能力，可在所有 Fortinet 设备及其系统组件的部署中提供广泛的可视性，集成了具有 AI 驱动的违规检测与防御能力，可自动操作，编制策略以及响应威胁。整个安全性能可以随着工作的负载和数据的增加动态扩展并弹性适应。对于整个网络，包括物联网、设备和云环境之间的数据、用户和应用程序做到无缝跟查并保护。所有这些领先的安全功能都在一个统一控制台下紧密地集成，大大降低了整个系统的复杂性。

FortiGate NGFW是 Security Fabric安全架构的基础，通过它可与其他 Fortinet 安全产品和 Fabric-就绪的技术伙伴解决方案紧密集成与协同联动，建立整个网络的可见性和与可控，并进一步扩展安全性。



FortiOS 操作系统

FortiOS是FortiGate NGFW的操作系统，它通用于所有FortiGate系列设备包括虚拟设备平台，该操作系统提供FortiGate所具备的全部网络与安全功能与服务，以及极致的可视化能力，从而降低复杂性，减少运营费用，节约时间成本，提升安全部署效率。



- 一个高度集成的平台通过单一操作系统和统一控制台管理所有 FortiGate 平台上的全部安全和网络服务。
- 行业领先的防护功能:安全防护效果和性能获得 NSS Labs 推荐并通过 VB100、AV Comparatives 和 ICSA 等机构验证。且同时支持最新的安全技术应用，例如基于欺骗的安全防护。
- 真正支持 TLS 1.3，而且还可以基于上亿个实时 URL 评级、及数千个应用识别与控制，阻断最新漏洞利用并过滤网络流量。
- 基于AI驱动的违规预防和高级威胁防护，能够在数分钟内自动预防，检测和缓解高级攻击。
- 安全原生的SD-WAN功能扩展，以及基于意图的网络微隔离的检测，遏制和隔离威胁的能力，提升用户体验。

服务

FortiGuard ™ 安全服务

FortiGuard Labs威胁研究与响应实验室提供实时可执行的威胁情报，在整个 Fortinet 解决方案的覆盖范围内推送全面的安全更新。我们的专家团队由超过200名的威胁研究分析师、安全工程师和电子取证专家组成，并与世界领先的威胁组织联盟，及其他网络安全供应商通力协作，共享安全态势与威胁情报。

FortiCare 支持服务

我们的 FortiCare 客户支持团队为所有 Fortinet 产品提供全球范围的技术支持。遍布美洲，欧洲，中W东和亚洲地区的 FortiCare TAC支持人员可以满足各种规模企业的服务需求。

详细信息请参阅 forti.net/fortiguard和forti.net/forticare

许可

面向AWS的FortiGate-VM支持按需许可(PAYG)和自带许可(BYOL)两种许可模型，适用于各种私有和公共云部署的多种部署方式。

PAYG对于初始部署和按需扩展都是一个非常灵活的选项。得益于众多受支持的实例类型，每个用例都有一个解决方案。该许可下可提供NGFW以及Threat Protection服务包。

如果迁移用例中现有的私有云部署被迁移到公共云部署，则BYOL非常适合这种情形。当使用现有许可时，唯一额外成本是购买AWS EC2实例的价格。

规格

所有地区都可以购买FortiGate-VM，包括AWS GovCloud和AWS中国。

以下是BYOL许可的系统要求：

	VM-00	VM-01/01V	VM-02/02V	VM-04/04V
系统要求				
vCPU（最少/最多）	1 / 1	1 / 1	1 / 2	1 / 4
技术规格				
支持网络接口（最少/最多）[1]	1 / 18	1 / 18	1 / 18	1 / 18
虚拟域（默认/最大）**	2 / 2	10 / 10	10 / 25	10 / 50
防火墙策略	10,000	10,000	10,000	200,000
FortiToken最大数量[2]	1,000	1,000	1,000	5,000
系统性能			ENA驱动程序 – 是	ENA驱动程序 – 是
实例机型			C5n.large	C5n.xlarge
AWS带宽[3]			最高25Gbps	最高25Gbps
防火墙吞吐速率（UDP数据包），以Mbps为单位			6,200	20,000
新建会话/秒（TCP）			92,000	210,000
IPS吞吐速率，以Mbps为单位[4]			9,000	13,000
IPS HTTP 1M，以Mbps为单位[4]			9,000	13,150
应用程序控制吞吐速率，以Mbps为单位[5]			8,400	13,200
NGFW吞吐速率[6]			1,100	2,100
威胁防护吞吐速率7			950	1,800
IPsec VPN吞吐速率（SHA2-256），采用UDP1518 bytes			1,600	1,960

实际性能可能因网络和系统配置而异。
使用FortiGate-VM BYOL实例（使用AWS上运行的FOS v6.2.1和FortiTester-VM）观察性能指标。
1.可用的网络接口数量取决于AWS实例类型/大小。
2.所有的OS版本均支持FortiGate-VM BYOL模式；按需模式下只有OS V6.2.2支持FortiToken。
3.如需AWS带宽的最新信息，请访问https://aws.amazon.com/ec2/insttypes/。
4.IPS性能测量基于企业的混合流量与1 Mbyte HTTP。
5.应用控制性能基于64 Kbyte HTTP流量。
6.NGFW的性能基于企业混合流量，并在启用IPS与应用控制的情况测量。
7.威胁防护性能基于企业混合流量，并在启用IPS、应用控制及恶意软件防护的情况。
** 不适用于FG-VMxxV系列，因为默认情况下不支持VDOM。可以使用单独购买的VDOM许可证添加VDOM。参阅订单信息获取VDOM SKU。

规格

所有地区都可以购买FortiGate-VM，包括AWS GovCloud和AWS中国。

以下是BYOL许可的系统要求：

	VM-08/08V	VM-16/16V	VM-32/32V	VM-UL/ULV
系统要求				
vCPU（最少/最多）	1 / 8	1 / 16	1 / 32	1 / Unlimited
技术规格				
支持网络接口（最少/最多）[1]	1 / 18	1 / 18	1 / 18	1 / 18
虚拟域（默认/最大）**	10 / 500	10 / 500	10 / 500	10 / 500
防火墙策略	200,000	200,000	200,000	200,000
FortiToken最大数量[2]	5,000	5,000	5,000	5,000
系统性能	ENA驱动程序 – 是			
实例机型	C5n.2xlarge			
AWS带宽[3]	最高25Gbps			
防火墙吞吐速率（UDP数据包），以Mbps为单位	21,000			
新会话/秒（TCP）	225,000			
IPS吞吐速率，以Mbps为单位[4]	13,150			
IPS HTTP 1M，以Mbps为单位[4]	13,200			
应用程序控制吞吐速率，以Mbps为单位[5]	13,300			
NGFW吞吐速率[6]	4,000			
威胁防护吞吐速率[7]	3,750			
IPsec VPN吞吐速率（SHA2-256），采用UDP1518 bytes	3,300			

实际性能可能因网络和系统配置而异。
使用FortiGate-VM BYOL实例（使用AWS上运行的FOS v6.2.1和FortiTester-VM）观察性能指标。
1.可用网络接口数量取决于AWS实例类型/大小。
2.所有的OS版本均支持FortiGate-VM BYOL模式；按需模式下只有OS V6.2.2支持FortiToken。
3.如需AWS带宽的最新信息，请访问https://aws.amazon.com/ec2/insttypes/。
4.IPS性能测量基于企业的混合流量与1 Mbyte HTTP。
5.应用控制性能基于64 Kbyte HTTP流量。
6.NGFW的性能基于企业混合流量，并在启用IPS与应用控制的情况测量。
7.威胁防护性能基于企业混合流量，并在启用IPS、应用控制及恶意软件防护的情况。

** 不适用于FG-VMxxV系列，因为默认情况下不支持VDOM。可以使用单独购买的VDOM许可证添加VDOM。参阅订单信息获取VDOM SKU。

有关分类指南，请参阅www.fortinet.com上提供的分类文件

订单信息

以下是BYOL许可证模式下的订单SKU。如果是PAYG/按需付费，可在Marketplace上获取不同实例/VM类型BYOL是永久许可（与之对应的是PAYG/按需付费），即面向Marketplace列出的产品以按小时付费。

产品	SKU	描述
FortiGate-VM00	FG-VM00	FFortiGate-VM虚拟设备1x vCPU核心。不支持Extreme DB。
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM虚拟设备1x vCPU核心。FG-VM01V型号默认没有VDOM
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM虚拟设备2x vCPU核心。FG-VM02V型号默认没有VDOM。
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM虚拟设备4x vCPU核心。FG-VM04V型号默认没有VDOM。
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM虚拟设备8x vCPU核心。FG-VM08V型号默认没有VDOM。
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM虚拟设备16x vCPU核心。FG-VM16V型号默认没有VDOM。
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM虚拟设备32x vCPU核心。FG-VM32V型号默认没有VDOM。
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM虚拟设备无限个vCPU核心。FG-VMULV型号默认没有VDOM。
选配附件		
虚拟域许可添加5	FG-VDOM-5-UG	在FortiOS 5.4及以后版本中增加5个VDOM的升级许可，受到平台最大VDOM容量的限制。
虚拟域许可添加15	FG-VDOM-15-UG	在FortiOS 5.4及以后版本中增加15个VDOM的升级许可，受到平台最大VDOM容量的限制。
虚拟域许可添加25	FG-VDOM-25-UG	在FortiOS 5.4及以后版本中增加25个VDOM的升级许可，受到平台最大VDOM容量的限制。
虚拟域许可添加50	FG-VDOM-50-UG	在FortiOS 5.4及以后版本中增加50个VDOM的升级许可，受到平台最大VDOM容量的限制。
虚拟域许可添加240	FG-VDOM-240-UG	在FortiOS 5.4及以后版本中增加240个VDOM的升级许可，受到平台最大VDOM容量的限制。

FG-VMxx”V” 6.0.0通过添加单个VDOM许可的方式支持VDOM。可配置的VDOM数量可以累积到每个vCPU型号支持的最大VDOM数量。请参照性能规范中的虚拟域（最多）。

服务列表

FortiGuard 服务包

FortiGuard Labs提供大量安全情报服务以增强FortiGate防火墙平台性能。您可以使用这些FortiGuard服务包之一轻松优化您FortiGate设备的防护功能。

服务包	360 防护	企业防护	统一威胁管理（UTM）	威胁防护
FortiCare	ASE 1	24x7	24x7	24x7
FortiGuard应用程序控制服务	•	•	•	•
FortiGuard IPS服务	•	•	•	•
FortiGuard高级恶意软件防护（AMP）– 杀毒软件、移动恶意软件、僵尸网络、CDR、病毒爆发防护和FortiSandbox云服务	•	•	•	•
FortiGuard网页过滤服务	•	•	•	
FortiGuard反垃圾邮件服务	•	•	•	
FortiGuard安全评级服务	•	•		
FortiGuard工业服务	•	•		
FortiCASB SaaS-only服务	•	•		
FortiConverter服务	•			
SD-WAN云辅助监控[2]	•			
SD-WAN Overlay控制器VPN服务[2]	•			
FortiAnalyzer 云 [2]	•			
FortiManager 云 [2]	•			

1. 24*7 小时服务及高级Ticket服务处理支持。