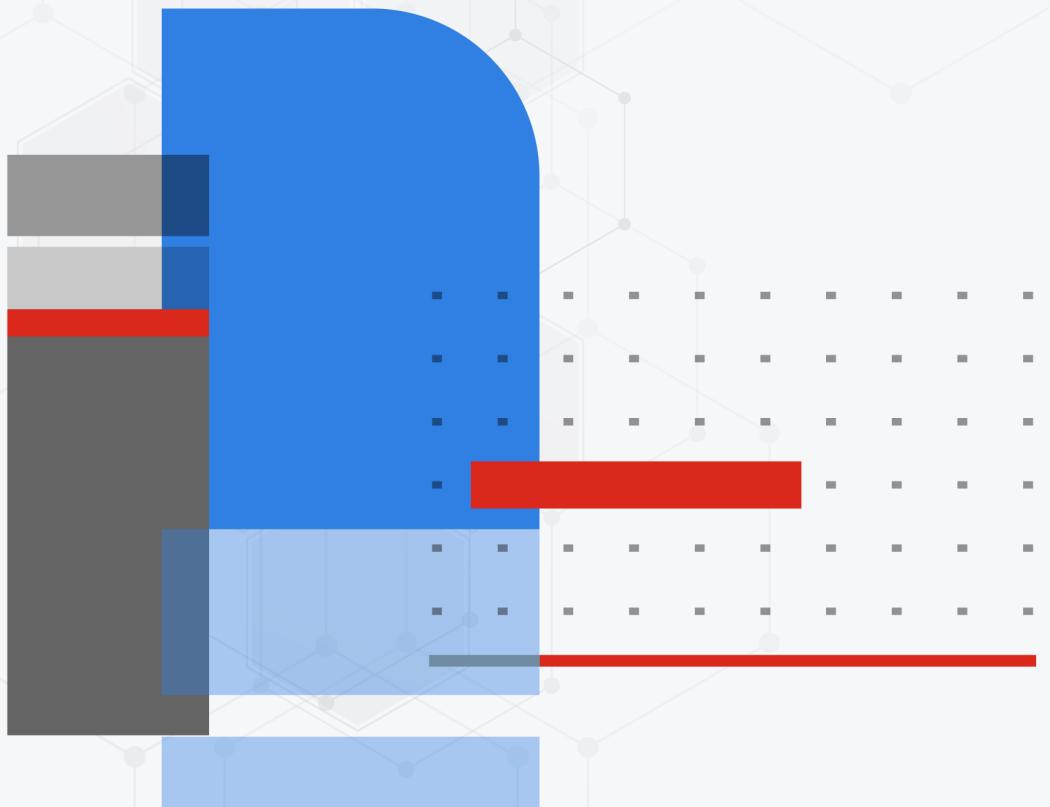




阿里云管理指南

FortiOS 7.4



FORTINET 文档库

<https://docs.fortinet.com>

FORTINET视频指南

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

客户服务与支持

<https://support.fortinet.com>

FORTINET 培训和认证计划

<https://www.fortinet.com/training-certification>

NSE 培训学院

<https://training.fortinet.com>

FORTIGUARD 威胁情报中心

<https://www.fortiguard.com>

最终用户许可协议

<https://www.fortinet.com/doc/legal/EULA.pdf>

意见与反馈

Email: techdoc@fortinet.com



2023年5月11日

FortiOS 7.4 阿里云平台管理指南

01-740-911137-20230511

目录

阿里云 FortiGate 简介	8
实例类型支持	8
地域支持	9
其他地域	10
型号	10
许可证	12
订购类型	12
创建支持帐户	12
在不同许可证类型之间迁移 FortiGate-VM 实例	14
保护阿里云实例	9
配置虚拟私有云	9
在阿里云市场订阅 FortiGate-VM	11
阿里云上 FortiGate-VM 路由配置	13
FortiGate-VM 初始防火墙策略配置	14
配置 ECS worker VM 以访问 VNC	15
测试出站流量的恶意软件扫描	16
测试出站流量的应用程序控制	17
在 FortiOS 中启用 NAT 入站流量保护	18
阿里云 FortiGate-VM 高可用性配置	20
HAVIP 在阿里云上部署和配置 FortiGate-VM	20
设置 VPC	21
阿里云市场 FortiGate-VM 订阅	24
在阿里云网页控制面板配置 HAVIP	32
连接测试	40
使用路由表和 EIP 在阿里云上部署 FortiGate-VM HA	40
在阿里云可用区之间部署 FortiGate-VM HA	51
FortiGate-VM 主动-主动 HA 配置	64
阿里云弹性伸缩部署	64
规划	65
要求	65
部署信息	67
部署	68
Terraform 变量	70
验证部署	72
删除集群	65
故障排除	66
调试 cloud-init	66
TableStore 删除时长	66
资源可用性	67
超时	67
如何重置选定的主 FortiGate	67
附录	68
阿里云 FortiGate 弹性伸缩功能	68

架构图	70
使用 RAM 角色配置阿里云 SDN 连接器	76
使用阿里云函数计算实现流水线自动化	76
将本地 FortiGate 连接至阿里云 VPC VPN.	80
通过站点至站点 VPN 将本地 FortiGate 连接至阿里云 FortiGate	86
配置本地 FortiGate	87
配置阿里云 FortiGate	93
更新日志	90

阿里云 FortiGate 简介

FortiGate下一代防火墙全面融合状态检测技术与一整套强大的安全功能，支持阿里云等各大主流公有云环境部署，为用户提供全面的内容和网络保护。

除了具备海量威胁数据库、漏洞管理和基于流量的安全检查等高级功能外，全面集成的应用过程控制、防火墙、防病毒、IPS、Web 过滤和 VPN 等功能，还可实现协同运行，全方位识别和缓解各类新兴和复杂安全威胁。

阿里云 FortiGate支持采用高可用性虚拟 IP 地址（HAVIP）实现主动/被动高可用性配置，在主备节点之间实现 FortiGate配置和会话同步，当 FortiGate 检测到故障时，被动防火墙实例将自动切换为主动状态。

FortiGate-VM 支持沙特云计算公司（SCCC）和阿里云等共同组建的独立云平台alibababaloud.sa。

阿里云 FortiGate 亮点与优势包括：

- 全面集成一系列关键安全功能和状态检测技术，提供全面的内容和网络保护。
- IPS技术可有效防御当前及新兴网络威胁，支持基于签名的威胁检测和异常威胁检测，并向用户发送警报，报告与攻击行为配置文件匹配的所有流量。
- Docker 应用过程控制签名可保护容器环境免受各类新兴威胁侵扰。
- 请参阅 [Docker 环境中的 FortiGate-VM](#)。

实例类型支持

FortiGate-VM支持阿里云部署，并可作为自带许可证（BYOL）设备部署在阿里云市场中FortiGate-VM列表支持的所有可用实例上。对于新部署设备，阿里云支持的实例可能更改，恕不另行通知。

有关实例规格族（instance type family）的最新信息，请参阅以下内容：

- 实例族
- [Fortinet FortiGate（BYOL）下一代防火墙](#)

区域支持

可在阿里云全球市场涵盖的所有区域/数据中心选购FortiGate-VM。可用区域连接点包括：

- 中国香港
- 亚太东南 1（新加坡）
- 美国东部 1（弗吉尼亚州）

- 亚太东北 1 (东京)
- 美国西部 1 (硅谷)
- 欧洲中部 1 (法兰克福)
- 中东 1 区 (迪拜)
- 亚太东南 2 (悉尼)
- 亚太东南 3 (吉隆坡)
- 亚太南部 1 (孟买)
- 亚太东南 5 (雅加达)
- 华北 1
- 华北 2
- 华北 3 (张家口)
- 华北 5 (呼和浩特)
- 华东 1
- 华东 2
- 华南 1

其他区域

- 沙特阿拉伯用户可通过沙特云计算公司（SCCC）选购FortiGate-VM。请参阅[阿里云 SCCC沙特运营区域](#)。

设备型号

FortiGate-VM 涵盖多种规格和型号，用户可根据所需CPU核数和 RAM容量灵活选购，各主流私有云和公有云平台均支持 FortiGate-VM部署。下表为常用订购型号，也称为自带许可证（BYOL）型号。请参阅[第 7 页订购类型](#)。

设备型号	vCPU支持数量	
	最小	最大
FG-VM01/01v/01s	1	1
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16
FG-VM32/32v/32s	1	32
FG-VMUL/ULv/ULs	1	无限



默认情况下，V 系列和 S 系列不支持虚拟域（VDOM）。如需添加 VDOM，应单独购买永久 VDOM 添加许可证。您可在初次部署后继续添加和堆叠 VDOM至最大数量上限。

通常，FortiGate BYOL许可证均有RAM容量限制，但阿里云环境不设限。阿里云支持任意容量 RAM和任意核数 CPU 型号部署。许可证仅基于 CPU 核数进行区分。

有关每个型号的订购信息、容量限制和 VDOM 添加数量，请参阅 [FortiGate-VM 技术参数表](#)。

许可证

持有许可证即可在AliCloud中部署 FortiGate。

订购类型

目前，阿里云仅支持一种订购类型：自带许可证（BYOL）。

BYOL 提供永久许可（通用系列和 V 系列）和年度订阅许可（S 系列）两种订阅模式。订阅模式按月计费，即用即付模式按小时计费。BYOL 许可证可从经销商或分销商处选购，具体价格请参阅Fortinet 每季度更新的公开价目表。无论私有云或公有云平台，BYOL 许可证均提供相同的订购模式。首次购买时，必须从 GUI（云控制台/图形用户界面）或 CLI（命令行工具/命令行界面）访问某一实例以激活许可证，即可开始使用各种功能。

对于所有订购类型，云提供商将单独收取计算实例、存储等资源消耗费用，而不对其上运行的软件收费（本示例为 FortiGate-VM）。

对于 BYOL模式，通常可以SKU形式订阅产品+技术支持服务捆绑包。S 系列 SKU 包含虚拟机产品和技术支持服务包，以简化订购流程。BYOL 许可模式的部署流程，请参阅[第 7 页创建支持帐户](#)。

创建支持帐户

阿里云 FortiGate 支持自带许可证（BYOL）许可模式。请参阅[第 7 页订购类型](#)。

为了确保 Fortinet 技术支持的正常使用并确保产品正常运行，必须完成激活步骤才能进行产品授权。成功激活后，Fortinet支持团队可在系统中识别您的注册信息。

首先，若无 Fortinet 帐号，请先自行创建[一个新账号](#)。

您必须事先购买许可证才能激活 FortiGate-VM。如果您尚未激活许可证，登录 FortiGate-VM 后，将弹出许可证上传界面，此时无法继续配置 FortiGate-VM。

您可通过Fortinet 任意合作伙伴购买 BYOL 许可证。如需合作伙伴联系方式，请发送邮件至 jerrywang@fortinet.com，我们将协助您选购许可证。

购买许可证或获取评估许可证后，您将收到带有激活码的 PDF文件。

FortiOS 7.2.1 发布了全新永久试用许可证，开通 FortiCare 帐户便可免费试用该许可证。请注意，此试用许可证的功能和容量有限。有关详细信息，请参阅 [VM 许可证](#)。

FortiOS 7.2.0 支持旧版评估许可证，有效期为 15 天。

要注册并下载 BYOL 许可证，请执行以下操作：

1. 点击[Fortinet Service & Support](#)（Fortinet 服务与支持）页面，创建新账户或使用现有账户登录。
2. 进入[Asset > Register/Activate](#)（资产>注册/激活）页面，完成注册步骤。
3. 在[Register](#)（注册）页面中，输入电子邮件中收到的安全码，选择[Register](#)（注册）选项以访问注册表。
4. 注册 S 系列订阅型号时，将提示您选择以下选项之一：
 - a. 单击[Register](#)（注册），输入安全码，以获取新许可证文件中的新序列号。
 - b. 单击[Renew](#)（续订）按钮，延长现有序列号项下的许可证有效期，完成许可证续订，确保 VM 节点上的所有功能持续正常运行。
5. 注册完毕后，将许可证 (.lic) 文件下载至计算机。稍后上传该许可证，激活 FortiGate-VM。
完成许可证注册后，等待最多30分钟，Fortinet 服务器完全识别新许可证。上传许可证 (.lic) 文件激活 FortiGate-VM 时，如果收到许可证无效的错误提示，请等待 30 分钟后重试。

在不同许可证类型之间迁移 FortiGate-VM 实例

在公有云上部署 FortiGate-VM 时，您可在部署期间选定许可证类型，如按需使用按量付费许可或自带许可（BYOL）。
许可证类型在虚拟机有效期内固定不变。用于在公有云市场上部署 FortiGate-VM 的镜像可预先确定许可证类型。

将 FortiGate-VM 实例从一种许可证类型迁移至另一种许可证类型时，需重新进行部署。暂不支持在同一虚拟机实例上简单切换许可证类型。但是，您可在以不同许可证类型运行的两个虚拟机之间迁移配置。在 FortiOS 功能方面，按量付费和 BYOL 两种许可证类型之间也存在一些差异。例如，FortiGate-VM 按量付费许可实例支持统一威胁管理（UTM）保护功能，但不支持虚拟域（VDOM），而 FortiGate-VM BYOL 实例基于具体采购合同支持更高级威胁防护和其他功能。

将 FortiOS 配置迁移至 FortiGate-VM 其他许可证类型时，请执行以下操作步骤：

1. 连接至 FortiOS GUI 或 CLI 并备份配置。请参阅[配置备份](#)。
2. 部署支持所需许可证类型的新 FortiGate-VM 实例。部署 BYOL 实例时，您必须从 Fortinet 经销商处购买新许可证。您可在部署后通过 FortiOS GUI 应用该许可证。
3. 重新启用步骤 2 中部署的 FortiGate-VM 实例上的配置，操作步骤参阅[配置备份](#)。



阿里云市场中的即用即付许可模式，目前暂不适用于 FortiGate-VM。

保护阿里云实例

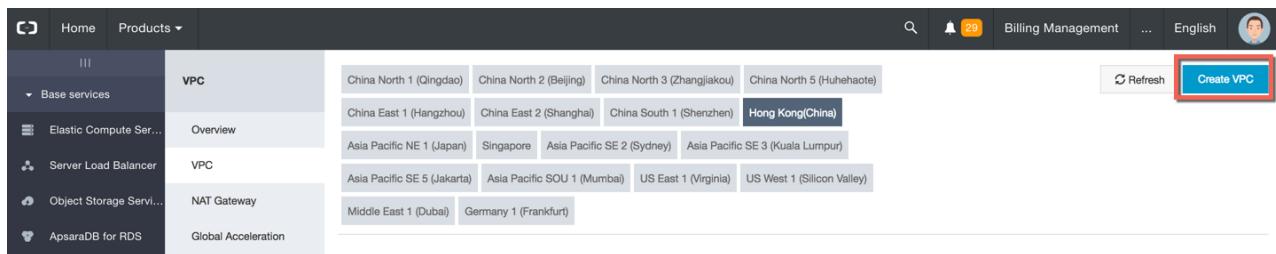
本指南介绍在阿里云上进行FortiGate-VM单一部署。此部署包括以下步骤：

1. 第 9 页 配置虚拟私有云
2. 第 11 页 在阿里云市场订阅 FortiGate-VM
3. 第 13 页 阿里云上 FortiGate-VM 路由配置
4. 第 14 页 连接测试

配置虚拟私有云

若要配置虚拟私有云，请执行以下操作：

1. 对于新部署环境，第一步应创建虚拟私有云（VPC）。在阿里云web控制台中，单击 *Create VPC*（*创建VPC*）。



2. 输入VPC名称。单击 *Create VPC*（*创建VPC*）。
3. 单击 *Next Step*（*下一步*）。
4. 您至少需创建两台虚拟交换机：分别用于ECS（云服务器）和 FortiGate-VM。首先创建用于ECS的虚拟交换机，如下图所示。

保护阿里云实例

Create VPC

Create VPC Create VSwitch

*VPC: - /vpc-j6cnfb11kn1hx4ghg0se

VPC CIDR Block: 192 . 168 . 0 . 0 / 16 Show Binary

*Name: Forti_VSwitchECS

The name can be 2-128 characters in length, including letters, digits, hyphens (-), and underscores (_), and must begin with either English letters or Chinese characters.

*Zone: Hong Kong Zone B

① It cannot be modified after creation.

*CIDR: 192 . 168 . 1 . 0 / 24 Show Binary

① It cannot be modified after creation.

The specified CIDR must be the same as, or belong to, that of the VPC. The allowed block size is between a /29 netmask and /16 netmask.

For example: 192.168.115.0/24

Learn more.

Number of Available Private IPs: 252 IPs

Description: VSswitch for ECS

The description can be 2-256 characters in length, and cannot begin with "http://" or "https://".

Create VSwitch

5. 点击 *Create More* (创建更多)。

6. 如图所示，为 FortiGate-VM 配置虚拟交换机，然后单击 *Create VSwitch* (创建虚拟交换机)。

Create VPC

Create VPC Create VSwitch

*VPC: - /vpc-j6cnfb11kn1hx4ghg0se

VPC CIDR Block: 192 . 168 . 0 . 0 / 16 Show Binary

*Name: Forti_VSwitchFW

The name can be 2-128 characters in length, including letters, digits, hyphens (-), and underscores (_), and must begin with either English letters or Chinese characters.

*Zone: Hong Kong Zone B

① It cannot be modified after creation.

*CIDR: 192 . 168 . 2 . 0 / 24 Show Binary

① It cannot be modified after creation.

The specified CIDR must be the same as, or belong to, that of the VPC. The allowed block size is between a /29 netmask and /16 netmask.

For example: 192.168.3.0/24

Learn more.

Number of Available Private IPs: 252 IPs

Description: VSswitch for the FW instance

The description can be 2-256 characters in length, and cannot begin with "http://" or "https://".

Create VSwitch

7. 单击 *Done* (完成)。VPC和虚拟交换机即创建完成。

在阿里云市场订阅FortiGate-VM

要在阿里云市场中订阅 FortiGate-VM，请执行以下操作：

1. 登录 [AliCloud Marketplace \(阿里云云市场\)](#) 并搜索Fortinet。
2. 创建 FortiGate-VM 实例。如果您已有 FortiGate-VM 许可证，请选择 BYOL 镜像。否则，请选择按需使用按量付费 (on-demand) 镜像。
 - a. 单击 *Choose Your Plan* (选择购买方案)。
 - b. 此示例中定价方案、区域和可用区分别选择：即用即付（PAYG）、中国香港和可用区 B。可用区 B 是 VPC 和虚拟交换机的位置。单击 *ECS Advance Purchase page* (ECS高级购买页面)，自定义数据盘和VPC信息。

The screenshot shows the AliCloud Marketplace product page for Fortinet FortiGate-VM On-Demand. The 'Pay-as-you-go' plan is selected. The 'Region' is set to Hong Kong and 'Zone' is set to Zone B. The 'Image' section shows the Fortinet FortiGate-VM On-Demand (2 vCore CPU) version v5.6.3. The 'Pricing Details' section shows the software fee as \$0.73 /Hour, ECS instance usage fee as \$0.072 /Hour, and data transfer fee as \$0.153 /GB. A red box highlights the 'ECS Advance Purchase page' link at the bottom left of the page.

- c. 为日志添加数据盘。建议选择SSD云盘以获得更佳性能。

The screenshot shows the 'Add Data Disk' configuration screen. It lists a 'System Disk' (SSD Cloud Disk, 40GB) and a 'Data Disk' (1/16). Under 'Data Disk', it shows 'You have selected 1 Disks, you can still add 15 Disk'. A new disk entry is being configured with 'SSD Cloud Disk', '50 GB', '2700 IOPS', 'Quantity: 1', and checked options for 'Release with Instance', 'Encrypted', and 'Create from snapshot'. A red box highlights the 'Data Disk' configuration area.

保护阿里云实例

d. 在 Network (网络) 页面, 请选择 “TP_FortiVPC和Forti_VSwitchFW” 。为镜像分配公网 IP 地址。

The screenshot shows the Network configuration step of the ECS instance creation wizard. It includes:

- Network selection: TP_FortiVPC and Forti_VSwitchFW are selected and highlighted with red boxes.
- Network Billing Method: PayByTraffic is selected at 50Mbps, also highlighted with a red box.
- Other settings: VPC: TP_FortiVPC, VSwitch Zone: Hong Kong Zone B (17), VSwitch CIDR Block: 192.168.2.0/24.
- Cost summary: Instance Cost: \$ 0.072 USD per Hour.
- Action buttons: Prev: Basic Configurations, Next: System Configurations, Preview.

e. 继续创建实例。

The screenshot shows the System Configurations step of the ECS instance creation wizard. It includes:

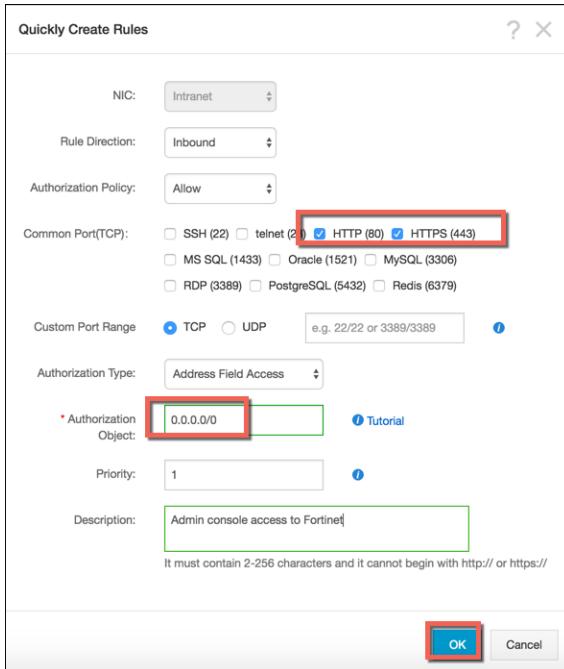
- Compute Type: n1 / ecs.n1.medium (2vCPU 4GB)
- Network: VPC
- Data Disk: 1 Unit(s) ... (highlighted with a red box)
- Networking: VPC: TP_FortiVPC / vpc-j6cnfb011kn1hx4ghg0se, VSwitch: Forti_VSwitchFW / vsw-j6coiofvmnisqvlwfyk / 192.1...
- Terms of Service: ECS Service Terms and Product Terms of Service | Image Product Terms of Use (highlighted with a red box)
- Cost summary: Instance Cost: \$ 0.087 USD per Hour.
- Action buttons: Prev: Grouping, Create Instance (highlighted with a red box).

3. 单击 Console (控制台) , 返回ECS实例列表。

4. 现在可看到 VM 已成功创建。记录公网 IP 地址和实例 ID 供后续使用。实例 ID 是FortiGate的默认密码。

Instance ID/Name	Monitor	Zone	IP Address	Status	Network Type	Configuration	Tags	Billing Method	Action
i-j6caixbrs90kkz09juwf		Hong Kong	47.75.161.235 (Internet IP Address)	Running	VPC	CPU: 2 Core(s) Memory: 4 GB (I/O Optimized) 50Mbps (peak value)		Pay-As-You-Go	Manage Connect
TP-Fortinet-5.6.3-SE		Zone B	192.168.2.8 (Private IP Address)	Running	VPC			18-03-28 10:51 created	Change Instance Type More

5. 现在，您必须配置默认安全组。进入*Security Groups*（安全组），然后单击*Configure Rules*（配置规则）。
- 单击*Quickly Create Rules*（快速创建规则）。
 - 勾选端口 80 和 443，然后单击*OK*（确定）。

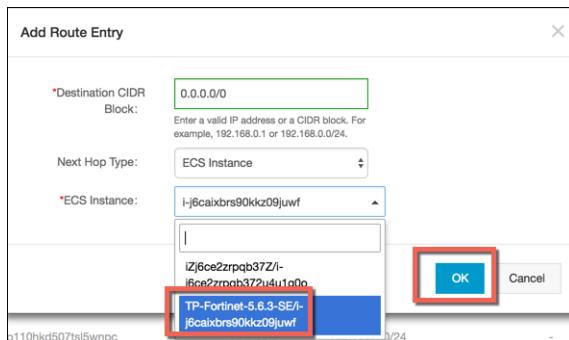


6. 现在，您可使用用户名“admin”在网页浏览器中访问FortiGate-VM。密码为您所记录的实例 ID。
7. 初次登录后，请更改密码。

阿里云上 FortiGate-VM 路由配置

阿里云上 FortiGate-VM 路由配置，请执行以下操作：

- 在 VPC 条目上，单击*Manage*（管理）。
- 单击*Add Route Entry*（添加路由条目）。
- 添加 0.0.0.0/0 并将其指向 FortiGate-VM。



上述操作确保 ECS 出站流量流经 FortiGate。

连接测试

以下内容将帮助您测试 FortiGate-VM 和 VPC 是否已正确配置。请按顺序完成以下步骤：

- 第 14 页 FortiGate-VM 初始防火墙策略配置
- 第 14 页 配置 ECS worker VM 以访问 VNC
- 第 16 页 测试出站流量的恶意软件扫描
- 第 16 页 测试出站流量的应用程序控制
- 第 17 页 在 FortiOS 中启用 NAT 入站保护

FortiGate-VM 初始防火墙策略配置

要在 FortiGate-VM 上配置初始防火墙策略，请执行以下操作：

- 在 FortiOS 中，为出站流量添加 IPv4 策略。
- 指定以下“ToInternet”策略，为所有会话开启防病毒、应用过程控制和日志记录功能。点击 *OK*（确定）。

配置 ECS worker VM 以访问 VNC

配置 ECS worker VM 以访问 VNC，请执行以下操作：

- 在阿里云网页控制台，单击 *Create Instance*（创建实例）。

- 配置 ECS 实例，使其与 FortiGate-VM 接在不同的虚拟交换机上。本示例选择 ECS 虚拟交换机。无需分配公网 IP 地址，因为绑定了公网 IP 地址的 ECS 不通过 FortiGate-VM 进行路由。

保护阿里云实例

The screenshot shows the 'Networking' step of the ECS instance creation wizard. It displays a dropdown menu for selecting a VPC, with 'TP_FortiVPC' and 'Forti_VSwitchECS' options. The 'Forti_VSwitchECS' option is highlighted with a red box. Below the dropdown, it shows the VPC selected: TP_FortiVPC, VSwitch Zone: Hong Kong Zone B (18), and VSwitch CIDR Block: 192.168.1.0/24. There is also a note about private IP addresses available: 252.

3. 确认配置，然后创建实例。

4. 重置 VNC 密码和登录密码，之后重启实例。

The screenshot shows a list of four ECS instances. The first instance, 'TP-ECS-worker-SE', has its network configuration set to 'VPC' and its billing method to 'Pay-As-You-Go'. The second instance, 'TP-Fortinet-5.6.3-SE', has its network configuration set to 'VPC' and its billing method to 'Pay-As-You-Go'. The third instance, 'TP-Windows-TestFW', has its network configuration set to 'VPC' and its billing method to 'Pay-As-You-Go'. The fourth instance, 'TP-Fortinet-5.6.3', has its network configuration set to 'VPC' and its billing method to 'Pay-As-You-Go'. On the right side of the interface, there is a 'More' button which is highlighted with a red box. Below it, there are several actions: 'Start', 'Stop', 'Restart', 'Release Setting', 'Reset Password' (highlighted with a red box), 'Buy the Same Configuration', 'Reset VNC Password' (highlighted with a red box), and 'Modify Information'.

5. 连接VNC 并登录 Windows。

The screenshot shows the same list of instances as the previous screenshot. The 'Connect' button for the first instance, 'TP-ECS-worker-SE', is highlighted with a red box. This button is located in the 'Actions' column next to the 'Manage' button.

虚拟机应能通过 FortiGate-VM 连接互联网。

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>ping hk.yahoo.com

Pinging 106.10.250.11: 32 bytes of data:
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55

Ping statistics for 106.10.250.11:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
Control-C
C:\>
```

FortiOS 还应能提供详细的日志信息。

测试出站流量的恶意软件扫描

要测试出站流量的恶意软件扫描功能，请执行以下操作：

1. 在 ECS worker 节点上，访问[测试网站](#)。
2. 单击Run Tests（运行测试）。如果应用程序防火墙或防病毒保护未正确配置，该测试将失败。

The screenshot shows a 'Test Cases & Results' section. At the top, it says '0/18 Tests Passed' and has buttons for 'Expand All', 'Collapse All', and 'Print All'. Below this, there are two test cases:

- Plain - Plain test file**: Status: Clean file, Generated a minute ago. Description: This is a screenshot from fortinet.com, taken in the last few minutes to show sample freshness.
- EICAR Infected file**: Status: Infected file, Generated a minute ago. Description: This is EICAR test file as well as a screenshot from fortinet.com, taken in the last few minutes to show sample freshness.

At the bottom right of the interface, it says 'Please run this test'.

FortiGate 阻止下载该文件。



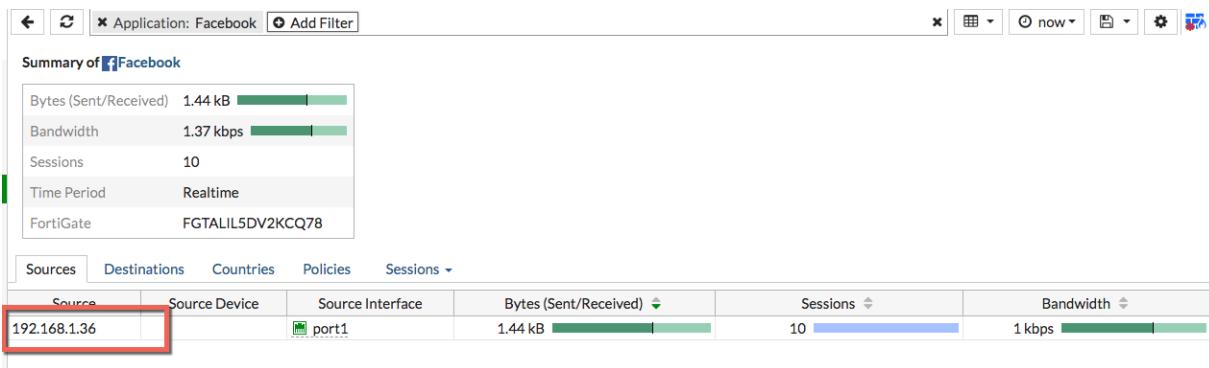
为获得最佳防病毒扫描功能，请确保 FortiOS 中的防病毒定义文件始终保持最新状态。

3. 在 FortiOS 中，请点击 FortiView > Threat。您可查看尝试下载的文件。

测试出站流量的应用程序控制

要测试出站流量的应用程序控制功能，请执行以下操作：

1. 在 FortiOS 中，点击 *Security Profiles > Application Control*（安全配置文件 > 应用过程控制）。在 *Categories*（类别）项下，点击拦截Video/Audio and Social Media（视频/音频和社交媒体），并单击 *OK*（确定）。
2. 在 ECS 上，尝试访问 Facebook 和 YouTube 时，应提示无法连接。FortiOS 显示客户端尝试连接至 Facebook 和 YouTube。



在 FortiOS 中启用 NAT 入站流量保护

在本示例中，启用 FortiGate-VM 来保护入站 RDP 流量。相同的概念可应用于HTTP / HTTPS和其他服务。本节为您介绍如何配置 FortiGate-VM 以监控入站和出站流量。

要在 FortiOS 中启用 NAT 入站流量保护，请执行以下操作：

1. 创建虚拟 IP 地址：

- 在 FortiOS 中，点击 *Policy & Objects > Virtual IP* (策略&对象 > 虚拟IP)。
- 单击 *Create New* (新建)。
- 从 *Interface* (接口) 下拉列表中，选择 *port1*。
- 在 *Mapped IP address/range* (镜像IP地址/范围) 字段中，输入 ECS IP地址：192.168.1.36。
- 启用 *Port Forwarding* (端口转发)。
- 在 *External service port* (外部服务端口) 和 *Map to port* (映射至端口) 字段中，输入 3389。
- 单击 *OK* (确定)。

2. 配置 RDP 重定向入站策略。点击 *Policy & Objects > Firewall Policy* (策略和对象 > 防火墙策略)，然后单击 *Create New* (新建)。

3. 在 *Destination* (目的地) 字段中，选择步骤 1 中创建的虚拟 IP 地址。

4. 启用所需的安全配置文件，然后记录所有会话以备后续演示。

5. 单击 *OK* (确定)。

现在，可使用 FortiGate 公网地址通过 RDP 接入ECS。

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping hk.yahoo.com

Pinging oob-media-router-fp1.prod.media.wg1.b.yahoo.com [106.10.250.11] with 32
bytes of data:
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55
Reply from 106.10.250.11: bytes=32 time=35ms TTL=55

Ping statistics for 106.10.250.11:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
Control-C
^C
C:\Users\Administrator>

```

此外，还可在 FortiOS 中查看日志和会话信息。

阿里云 FortiGate-VM 高可用性配置

可采用多种方法在阿里云上为 FortiGate-VM 配置主动-被动高可用性（HA）。

第一种部署方案，[如第18页所述，使用HAVIP在阿里云上部署和配置FortiGate-VM](#)，具体取决于阿里云提供的 HA 虚拟 IP 地址功能。该方案中，必须在 port 1 上配置内外部接口。主备 FortiGates 之间共享同一 IP 地址。因为无需更新弹性 IP（EIP）地址或路由表，故障转移时间可能比第二种方案更快。此方案原生支持 *session pickup*（会话同步）功能。

第二种部署方案，[如第40页所述，使用路由表和EIP在阿里云上配置FortiGate-VM HA](#)，通过引入 EIP 切换和路由表更新功能来实现 HA。在此方案中，可在不同接口配置内外部接口。此外，您还可选择将高可用性虚拟 IP 地址（HAVIP）用于 port1 上的外部流量和 port2 上的内部流量，以提高效率和灵活性。此方案支持会话同步，但故障转移时不如第一种方案更高效。

选择部署 HA 方案时，请考虑以下事项：

- 如需会话同步功能，且无法为入站防火墙策略禁用 NAT，则必须选用第一种方案。
- 如需会话同步功能，且可为入站防火墙策略禁用 NAT，可选择第二种方案，在 port1 上使用 HAVIP，并将 EIP 绑定至 HAVIP。此方案无需切换 EIP，但需为内部流量更新路由表。此方案可实现灵活性和效率的最佳平衡。
- 若不能将 port1 用于外部流量，则必须使用第二种方案，切换 EIP 并更新路由表。这可能使故障转移时间更长。

使用 HAVIP 在阿里云上部署和配置 FortiGate-VM

阿里云平台支持使用高可用性虚拟 IP 地址（HAVIP）配置两个 FortiGate-VM 实例，以实现主动-被动高可用性（HA）配置。FortiGate-VM 配置将在两个实例之间同步。当主 FortiGate-VM 出现故障时，处于备份状态的 FortiGate-VM 立即切换为主设备，同时确保会话不中断。HAVIP 将流量转发至新的主 FortiGate-VM，同时确保最短的切换时间。

在此方案中，阿里云 VPC 无法创建多个路由表，VPC 仅支持单臂部署模式。HAVIP 涵盖 VPC 间（inter-VPC）服务，VPC 默认路由指向 HAVIP。VPC 出站流量首先路由至 HAVIP，然后转发至主 FortiGate-VM。您必须将 HAVIP 绑定至弹性 IP 地址，以便转发 VPC 入站流量。

设置VPC

要设置 VPC，请执行以下操作：

- 对于新部署环境，第一步是创建虚拟私有云（VPC），单击 *Create VPC*（创建VPC）。

The screenshot shows the 'VPCs' section of the AliCloud Management Console. On the left, there's a sidebar with 'Route Tables', 'VSwitches', and 'Shared Bandwidth P...'. The main area has tabs for 'VPCs' (selected) and 'VPCs'. Below is a table with columns: Instance ID/Name, Destination CIDR Block, Status, Default VPC, Route Table, VSwitch, and Actions. A single row is shown with values: '192.168.0.0/16', 'Available', 'No', '1', '3', and 'Manage Delete'.

- 将 VPC 命名为TP_FortiVPC。

VPC

Region

China East 1 (Hangzhou)

Name ?

TP_FortiVPC

11/128 ✓

Destination CIDR Block ?

192.168.0.0/16

▼

! The CIDR cannot be changed once the VPC is created.

Description ?

VPC For demo Fortinet

21/256

- 这一方案中，至少需创建三个虚拟交换机：分别用于ECS、FortiGate-虚拟机出/入站接口和FortiGate-VM高可用性接口。还可创建第四个虚拟交换机，为FortiGate 预留管理接口。

首先创建ECS虚拟交换机，如下图所示。

● Name ?

ECS_SW 6/128 ✓

● Zone ?

East China 1 Zone F ▾

Zone Resource ?

ECS ✓ RDS ✓ SLB ✓

● Destination CIDR Block

192 · 168 · 4 · 0 / 24 ▾

① The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs
252

Description ?

0/256

Contact Us

(You can only create three instances once.)

Add

Delete

4. 为 FortiGate-VM 出/入站接口创建虚拟交换机，如下图所示。

VSwitch

● Name ?

FortiGate_Internet_SW

21/128 ✓

● Zone ?

East China 1 Zone F

∨

Zone Resource ?

ECS ✓RDS ✓SLB ✓

● Destination CIDR Block

192

·

168

·

0

·

0

/

24

∨

! The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs

252

Description ?

0/256

Contact Us

⊕ Add

>Delete

5. 为 FortiGate-VM HA 接口创建虚拟交换机，如下图所示。

● Name ?

15/128 ✓

● Zone ?

▾

Zone Resource ?

ECS ✓ RDS ✓ SLB ✓

● Destination CIDR Block

. . . / ▾

(!) The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs

252

Description ?

0/256

Contact Us

Add Delete

6. (可选项) 创建第四个虚拟交换机, 为 FortiGate 预留管理接口。

Create VSwitch

(?) X

● VPC

TP_FortiVPC/vpc-bp1ue3buvqego4vkha4wl



Destination CIDR Block

192.168.0.0/16

● Name (?)

FortiGate_Reserved_MGMT_SW

26/128

● Zone (?)

East China 1 Zone F



Zone Resource (?)

ECS

RDS

SLB

● Destination CIDR Block

192

· 168

· 3

· 0

/ 24



The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs

252

Contact Us

Description (?)

0/256

OK

Cancel

VPC 现已准备就绪。

Create VPC

Details

VPC Name	TP_FortiVPC
VPC ID	vpc-bp1ue3buvqego4vkha4wl
Status	Success Create NAT Gateway

VSwitch name	FortiGate_Internet_SW
VSwitch ID	vsw-bp18zyff1ou2azweoun6r
Status	Success Purchase▼

VSwitch name	FortiGate_HA_SW
VSwitch ID	vsw-bp1q5b9yoxinv9syb0jgc
Status	Success Purchase▼

VSwitch name	ECS_SW
VSwitch ID	vsw-bp1gejklo1u0j8brt4ioz
Status	Success Purchase▼

Contact Us

Complete

阿里云市场FortiGate-VM订阅

要在阿里云市场中订阅 FortiGate-VM，请执行以下操作：

1. 登录[阿里云市场](#)并搜索Fortinet。
2. 创建 FortiGate-VM 实例。如您已有 FortiGate-VM 许可证，请选择 BYOL 镜像。否则，请选择按量付费镜像。

阿里云 FortiGate-VM 高可用性配置

- a. 单击 *Choose Your Plan* (选择购买方案)。
- b. 本示例中定价方案、区域 (region) 和可用区 (zone) 分别选择：即用即付 (PAYG)、华东 1 区 (杭州) 和可用区 F。可用区 F 是 VPC 和虚拟交换机的位置。单击 *ECS Advance Purchase* (ECS高级购买) 页面，自定义数据盘和VPC信息。

Choose Your Plan

Pricing Plan
 Subscription Pay-as-you-go

Region
China East 1 (Hangzhou) Zone G Zone B Zone F Zone E

Image
Fortinet FortiGate-VM On-Demand (2 vCore CPU)
Version v5.6.3 Release Note: 5.6.3

ECS Instance
 I/O Optimized
Default Type: ecs.sn1ne.large Select another instance type

You can choose more specific instance configurations on [ECS Advance Purchase page](#).

Overview
Image: Fortinet FortiGate-VM On-Demand (2 vCore)
ECS Instance Type: ecs.sn1ne.large (2 Core 4 GB)
System Disk: 40GB (default)
Bandwidth: 2M (pay by traffic)

Pricing Details
Software fee: \$ 0.73 /Hour
ECS Instance usage fee: \$ 0.143 /Hour
Data Transfer: \$ 0.123 /GB

Agree Terms and Buy Now

By subscribing to this product you agree to [End User License Agreement \(EULA\)](#), and all applicable terms and conditions contained in the Alibaba Cloud International Website.

- c. 单击选择 4 核 vCPU ECS 规格，启动 FortiGate 实例。4 核 vCPU ECS 规格最多支持 3 个NIC，2核 vCPU ECS 规格最多支持 2 个NIC。如需预留 FortiGate 管理接口，请选择4核 vCPU ECS 规格。

Region
Select a region
Cloud services available in different regions do not have intranet communication with one another. Select a region close to your visitors to achieve the best download experience and lowest latency.

Instance Type
IO-Optimized Instance
vCPU: Select vCPU Memory: Select memory Instance type: e.g. ecs.sn1ne.large

Current Generation All Generations

Architecture: x86-Architecture Heterogeneous Computing

Category: General Purpose Compute Optimized Memory Optimized Big Data Local SSD High Clock Speed Entry-Level (Shared)

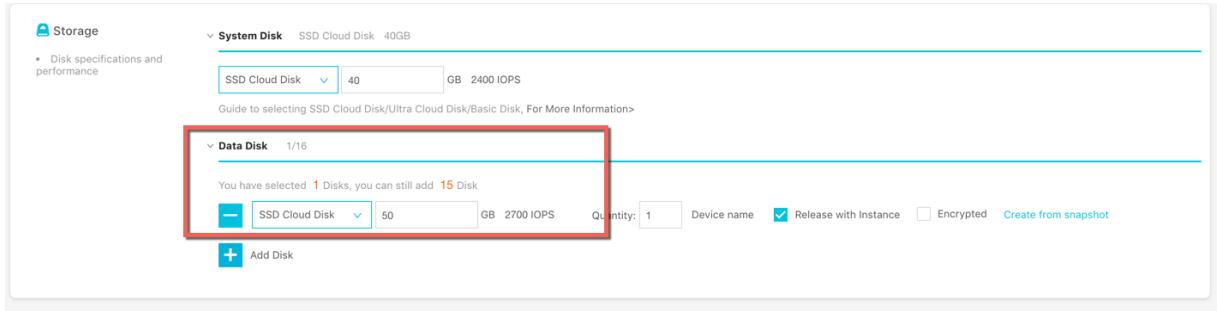
Family	Instance type	vCPU	Memory	Physical processor	Clock speed	Intranet bandwidth	Packet forwarding rate
Compute Optimized Type sn1	ecs.sn1.medium	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.5 Gbps	PPS(Packets Per Second) 100,000
Compute Optimized Type sn1	ecs.sn1.large	4 vCPU	8 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	0.8 Gbps	PPS(Packets Per Second) 200,000
Network Enhanced sn1ne	ecs.sn1ne.large	2 vCPU	4 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	PPS(Packets Per Second) 300,000

Bandwidth: 2Mbps PayByTraffic
Instance Cost: \$ 0.262 USD per Hour + Marketplace image fee: \$ 0.730 USD per Hour + Public traffic fee: \$ 0.123 USD per GB
Save \$ 0.013 USD per Hour save 5% for ECS

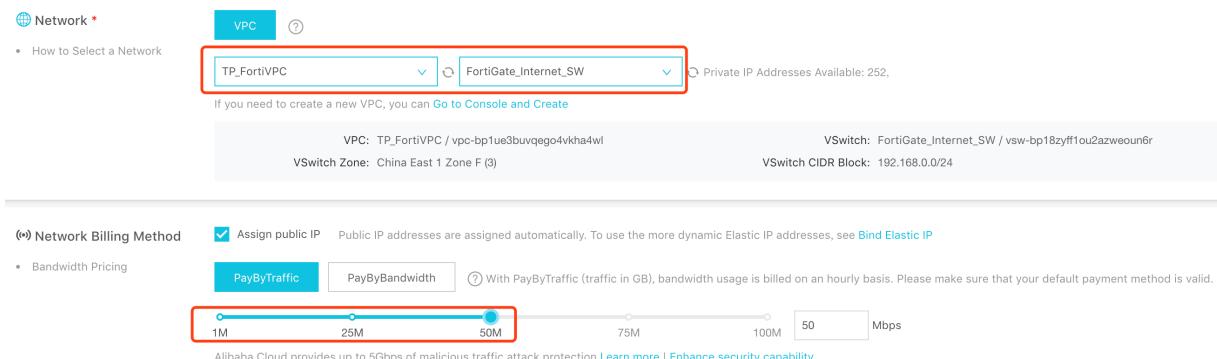
Next: Networking Preview

阿里云 FortiGate-VM 高可用性配置

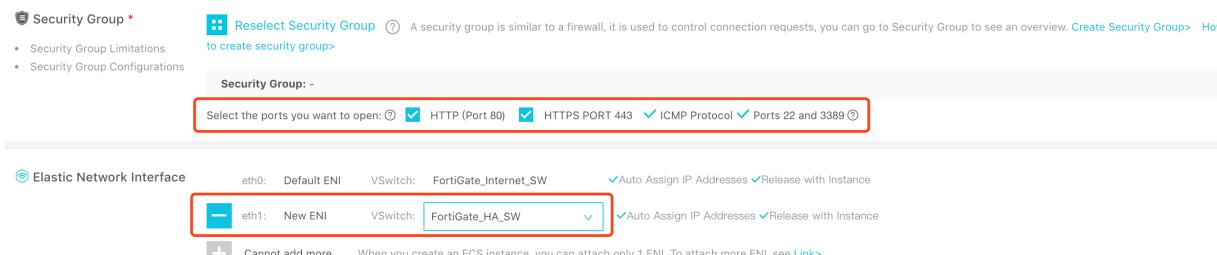
- d. 为日志添加数据盘。建议使用 SSD 云盘以获得更佳性能。



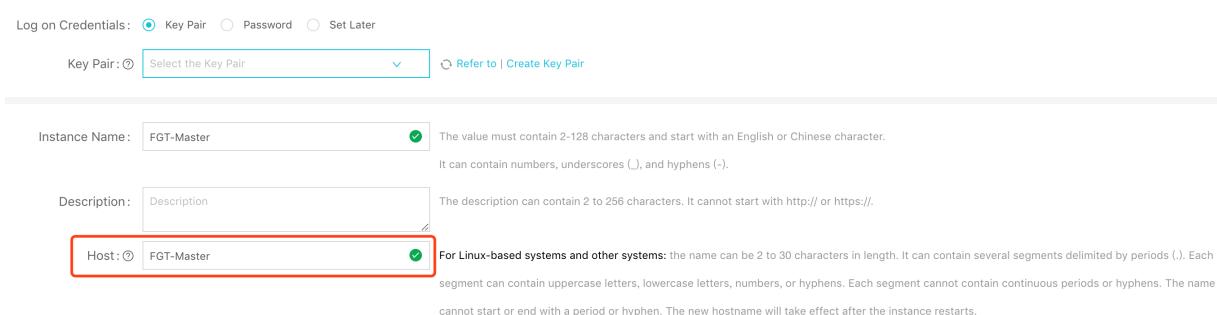
- e. 在 Network (网络) 界面, 请选择 “TP_FortiVPC” 和 “Forti_internet_SW” 。为镜像分配公网 IP 地址。该NIC为 FortiGate-VM上的port1 (默认 ENI) 。



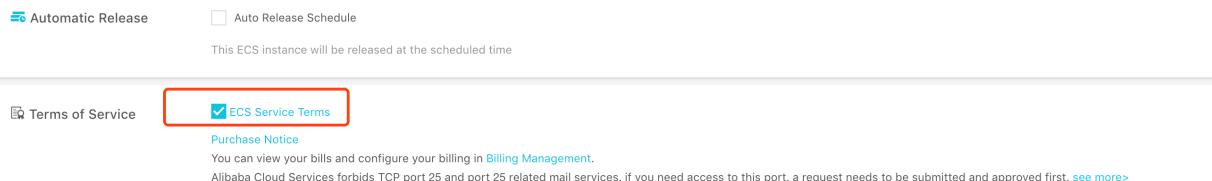
- f. 将HTTPS、ICMP 和 SSH 端口和协议保持开放状态以允许连接。在FortiGate_HA_SW上添加另一个ENI。该 ENI为FortiGate 上的port2。



- g. 在 Host (主机) 框中输入 FortiGate 主机名。



h. 单击勾选ECS Service Terms (ECS服务条款)。



3. 单击Console (控制台)，返回ECS实例列表。

4. 现在，VM 已创建成功。记录公网 IP 地址和实例 ID 供后续使用。实例 ID 是 FortiGate的默认密码。

Instance List									Create Instance	Bulk Action
<input type="text"/> Select the instance attribute, or directly enter the keyword Tag									Advanced Search	
Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions	
i-bp1cj6it8c8hndkxom7j FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	 Manage Connect Change Instance Type More	

5. 重复步骤 1 和 2，创建另一名为 FGT-Slave 的 FortiGate 实例。

Instance List									Create Instance	Bulk Action
<input type="text"/> Select the instance attribute, or directly enter the keyword Tag									Advanced Search	
Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions	
i-bp1cj6it8c8hndkxom7j FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	 Manage Connect Change Instance Type More	
i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247 (Internet IP Address) 192.168.0.151 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	 Manage Connect Change Instance Type More	
i-bp1cj6it8c8hndkxom7j FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	 Manage Connect Change Instance Type More	
i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	192.168.5.144 (Private IP Address)	Stopped	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-04-04 07:50 created	 Manage Change Instance Type More	
i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	 Manage Connect Change Instance Type More	

6. 您可创建两个ENI，并与FortiGate 实例绑定。该步骤为可选项。

- a. 勾选并点击停止 (stop) 使用两个 FortiGate 实例。

The screenshot shows the AliCloud Instance List interface. Two instances are selected: 'bp167uui7rqzmp8ta0kw FGT-Slave' and 'i-bp1cj6it8c8hndkxom7 FGT-Master'. Both instances are in the 'Running' state. A red box highlights the 'Stop' button at the bottom of the instance list table.

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247 (Internet IP Address) 192.168.0.151 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage Connect Change Instance Type More
i-bp1cj6it8c8hndkxom7 FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage Connect Change Instance Type More
bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	47.98.103.62 (Internet IP Address) 192.168.5.144 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large 5Mbps (peak value)	Pay-As-You-Go 18-04-04 07:50 created	Manage Connect Change Instance Type More
bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage Connect Change Instance Type More

Bottom buttons: Start, Stop, Restart, Reset Password, Renew, Switch to Subscription, Release Setting, More. Total: 4 item(s), Per Page: 20 item(s). Page: 1 of 1.

- b. 点击 *Networks & Security > Network Interfaces* (网络和安全 > 网络接口) 并创建两个 ENI。

The screenshot shows the AliCloud Network Interfaces page under the Networks & Security category. The 'Network Interfaces' tab is selected. The main area displays four network interfaces, each with details like Name, VSwitch/VPC, Zone, Security Group ID, and Actions (Modify, Detach, Delete). A red box highlights the 'Network Interfaces' link in the left sidebar.

Create

Network Interface

Name:

FGT-Master-Port3

2-128 characters, not http:// or https:// at the beginning, must be based on the size of letters beginning, may contain numbers, - or _

*VPC:

vpc-bp1ue3buvqego4vkha4wl / TP_FortiG...

*VSwitch:

vsw-bp1n4o8m36029aq05akvk / FortiG...

CIDR: 192.168.3.0/24

IP:

Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.

*Security Group

sg-bp153m2jlzs6qlvntqt5

Description:

It must contain 2-256 characters and it cannot begin with http:// or https://

OK

Cancel

Create

X

Network Interface
Name:

FGT-Slave-Port3

2-128 characters, not http:// or https:// at the beginning,
must be based on the size of letters beginning, may
contain numbers, - or _

*VPC:

vpc-bp1ue3buvqego4vkha4wl / TP_Forti...

*VSwitch:

vsw-bp1n4o8m36029aq05akvk / FortiG...

CIDR: 192.168.3.0/24

IP:

Must be the free address in the address section
of the VSwitch to which it belongs. By default,
the free address in the switch is allocated
randomly.

*Security Group

sg-bp153m2jlzs6qlvntqt5

Description:

It must contain 2-256 characters and it cannot begin with http:// or https://

OK

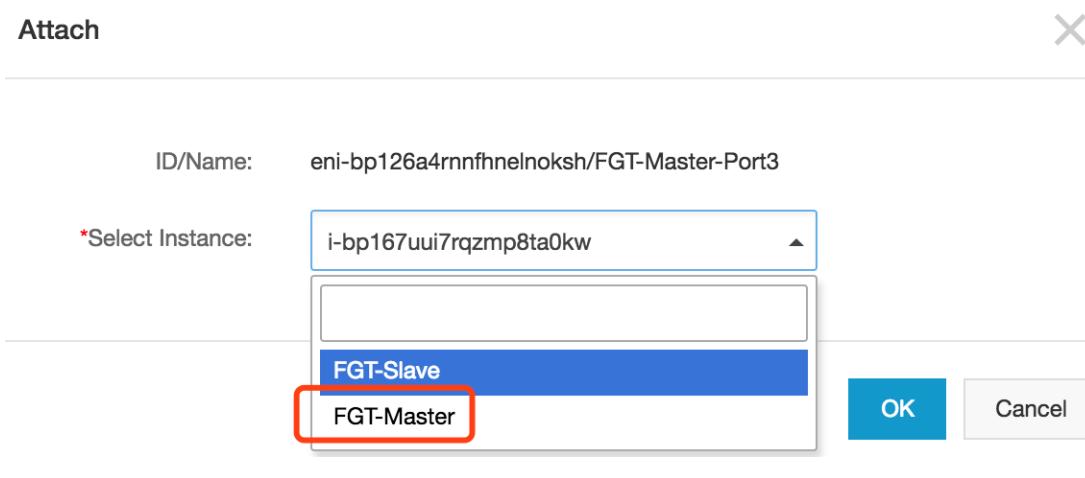
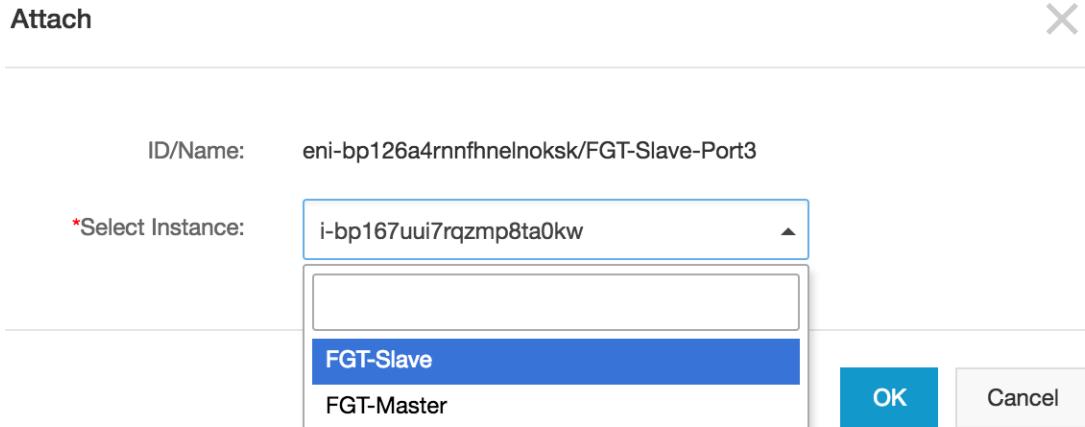
Cancel

c. 将两个新的 ENI 分别与两个 FortiGate 实例绑定。

Network Interfaces

Create

Name	Enter name	Search	ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksh FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...					192.168.3.250	Secondary 00:16:3e:12:2b:bf	Available 2018-05-02		Modify Attach Delete
eni-bp126a4rnnfhnelnoksh FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...					192.168.3.249	Secondary 00:16:3e:10:13:3e	Available 2018-05-02		Modify Attach Delete



Network Interfaces									
Name	Enter name		Search		Update success				
ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	Status/Created At	Actions
eni-bp126a4rnnfhnelnoksk FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp167uui7r...	192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use 2018-05-02		Modify Detach Delete
eni-bp126a4rnnfhnelnoksh FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp1cj6it8c...	192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use 2018-05-02		Modify Detach Delete

d. 点击 *Restart* (重新启动) 两个 FortiGate 实例。

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Actions
i-bp167uui7rqzmp8ta0kw FGT-Slave			East China 1 Zone F	47.98.242.247 (Internet IP Address) 192.168.0.151 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:29 created	Manage Connect Change Instance Type More
i-bp1c6it8c8hndkxom7 FGT-Master			East China 1 Zone F	116.62.190.109 (Internet IP Address) 192.168.0.150 (Private IP Address)	Running	VPC	4 vCPU 16 GB (I/O Optimized) ecs.sn2.large 50Mbps (peak value)	Pay-As-You-Go 18-05-02 14:21 created	Manage Connect Change Instance Type More
i-bp1i12dakoen7nchepx8 SSL_VPN_Server			East China 1 Zone F	47.98.103.62 (Internet IP Address) 192.168.5.144 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large 5Mbps (peak value)	Pay-As-You-Go 18-04-04 07:50 created	Manage Connect Change Instance Type More
i-bp1ionhm5ibeb1hyra65 client			China East 1 Zone G	192.168.3.84 (Private IP Address)	Running	VPC	2 vCPU 8 GB (I/O Optimized) ecs.sn2ne.large	Pay-As-You-Go 18-03-19 20:55 created	Manage Connect Change Instance Type More

Buttons at the bottom: Start, Stop, **Restart**, Reset Password, Renew, Switch to Subscription, Release Setting, More.

Total: 4 item(s), Per Page: 20 item(s) | Page: 1 / 1

7. 使用用户名“admin”在网页浏览器中访问 FortiGate-VM。密码是前面记录的实例 ID。

8. 首次登录后，请更改密码。

9. 为 FortiGate 上的三个接口设置 IP 地址。

Name	Enter name	Search							
ID/Name	VSwitch/VPC	Zone	Security Group ID	Binded Instance	Public IP Address	Private IP Address	Type/MAC(All)	At	Actions
eni-bp167uui7rqzmp8ta0kw FGT-Slave-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp167uui7r...	192.168.3.250	Secondary 00:16:3e:12:2b:bf	In Use	2018-05-02	Modify Detach Delete
eni-bp1c6it8c8hndkxom7 FGT-Master-Port3	vsw-bp1n4o8m... vpc-bp1ue3bu...	East China 1 Zone F	sg-bp153m2jl...	i-bp1c6it8c...	192.168.3.249	Secondary 00:16:3e:10:13:3e	In Use	2018-05-02	Modify Detach Delete

在阿里云网页控制面板配置HAVIP

在阿里云网页控制面板上配置HAVIP，请执行以下操作：

- 创建新的高可用性虚拟 IP (HAVIP) 地址。选择虚拟私有云 (VPC) 和 FortiGate-VM port1 虚拟交换机，并设置 HAVIP 地址。

The screenshot shows the AliCloud VPC management interface. On the left sidebar, under the 'VPC' category, the 'HAVIP Addresses' option is selected and highlighted with a red box. At the top center, there is a 'Create HAVIP Address' button, also highlighted with a red box. Below the header, there is a search bar with 'Instance ID' and 'Enter a name or ID' fields, and a magnifying glass icon.

Instance ID	IP Address	Status	Bind Instance	VPC	VSwitch	Actions
... (redacted)						
... (redacted)						
... (redacted)						

Create HAVIP Address

Region

China East 1 (Hangzhou)

● VPC

vpc-bp1ue3buvqego4vkha4wl

● VSwitch

vsw-bp18zyff1ou2azweoun6r

VSwitch CIDR Block

192.168.0.0/24

Private IP Address

192 - 168 - 0 - 252

2. 通过阿里云网页GUI上的VNC控制台或通过SSH在FortiGate上设置HA配置。

- a. 主 FortiGate 配置如下。在此示例中，192.168.3.253 是虚拟交换机上的网关，而 192.168.1.250 是备用 FortiGate port2 的 IP 地址。具有较高优先级值的 FortiGate 为主 FortiGate。

```
config system ha
    set group-name "ha"
    set mode a-p
    set hbdev "port2" 0
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interface
        edit 1
            set interface "port3"
            set gateway 192.168.3.253
        next
    end
    set priority 200
    set monitor "port1"
    set unicast-hb enable
    set unicast-hb-peerip 192.168.1.250
end
```

- b. 备用 FortiGate 配置如下。此示例中，192.168.1.249是主FortiGate port2的IP地址。

```
config system ha
    set group-name "ha"
    set mode a-p
    set hbdev "port2" 0
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interface
        edit 1
            set interface "port3"
            set gateway 192.168.3.253
        next
    end
    set priority 100
    set monitor "port1"
    set unicast-hb enable
    set unicast-hb-peerip 192.168.1.249
end
```

3. 重新启动两个 FortiGate。

4. 在 CLI 中运行命令 `diagnose sys ha status` 以检查 HA 状态。应显示以下内容：

```

FGT-Master # diagnose sys ha status
HA information
Statistics
    traffic.local = s:0 p:20456 b:7590378
    traffic.total = s:0 p:20467 b:7591052
    activity.fdb = c:0 q:0

Mode=90019, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_master=1.
FGTALIG8XFM4RR79: Master, serialno_prio=1, usr_priority=200, hostname=FGT-Master
FGTALIZT2A540C07: Slave, serialno_prio=0, usr_priority=100, hostname=FGT-Slave

[Kernel HA information]
vcluster 1, state=work, master_ip=192.168.1.249, master_id=0:
FGTALIG8XFM4RR79: Master ha_prio/o_ha_prio=0/0
FGTALIZT2A540C07: Slave ha_prio/o_ha_prio=1/1

```

5. 将 HAVIP 地址设置为两个 FortiGate 上的 port1 备用 IP 地址。在两个 FortiGate 上，配置以下内容。配置的备用 IP 地址应与 HAVIP 地址相同。

```

config system interface
    edit "port1"
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip 192.168.0.252 255.255.255.0
                set allowaccess ping https ssh
            next
        end
    next
end

```

6. 将弹性 IP 地址和两台 FortiGate 弹性云服务器绑定至 HAVIP。

a. 创建新的EIP。

The screenshot shows the 'Elastic IP Address' management page. At the top, there's a navigation bar with tabs for 'Elastic IP Address' and 'Elastic IP Addresses'. Below the navigation bar is a search bar with placeholder text 'Enter the Elastic IP address for an exact search' and a 'Search' button. To the right of the search bar are 'Refresh' and 'Create EIP' buttons.

The main area displays a grid of regions where EIPs can be allocated. Regions shown include China North 1 (Qingdao), China North 2 (Beijing), China North 3 (Zhangjiakou), China North 5 (Huhehaote), China East 1 (Hangzhou), China East 2 (Shanghai), China South 1 (Shenzhen), Hong Kong (China), Asia Pacific NE 1 (Tokyo), Asia Pacific SE 1 (Singapore), Asia Pacific SE 2 (Sydney), Asia Pacific SE 3 (Kuala Lumpur), Asia Pacific SE 5 (Jakarta), Asia Pacific SOU 1 (Mumbai), US East 1 (Virginia), US West 1 (Silicon Valley), Middle East 1 (Dubai), and EU Central 1 (Frankfurt).

At the bottom of the page, there's a table with columns: Instance ID, IP Address, Monitoring, Bandwidth, Billing Method (All), Status (All), Shared Bandwidth, Instance Bound, Instance Type, and Actions. A specific row is highlighted with a red box, showing an EIP entry with the instance ID 'eip-bp1fkuoatanoco05jgk2', IP address '47.97.186.150', pay-as-you-go billing, and an available status.

阿里云 FortiGate-VM 高可用性配置

VPC

HAVIP Addresses

Instance ID	IP Address	Status	Bind Instance	VPC	Vswitch	Actions
havip-bp1bwya8f7lppbl0qq6l5	192.168.0.252(Intranet IP)	Available	No ECS Bound	vpc-bp1ue3buvqego4vkha4wl	vsw-bp18zyff1ou2azweoun6r	Manage More

HAVIP Addresses

HAVIP Details

Information		Resources	
ID	havip-bp1bwya8f7lppbl0qq6l5	Status	Available
Region	China East 1 (Hangzhou)	Intranet IP	192.168.0.252
VPC ID	vpc-bp1ue3buvqego4vkha4wl	Created At	05/02/2018, 15:12:42
VSwitch	vsw-bp18zyff1ou2azweoun6r	Description	- Edit

Resources

```
graph TD; HAVIP["HAVIP Address: 192.168.0.252 (Intranet IP)"] --- ECS1["No ECS Bound"]; HAVIP --- ECS2["No ECS Bound"];
```

- b. 将弹性公网IP（EIP）与HAVIP绑定。

Bind Elastic IP Address

HAVIP Address

havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

192.168.0.252

● Elastic IP Address

Select

47.97.186.150

116.62.161.94

- c. 将2个FortiGate分别与HAVIP绑定。

Bind an ECS Instance

HAVIP Address

havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

192.168.0.252

● ECS Instance

i-bp167uuui7rqzmp8ta0kw

Bind an ECS Instance

HAVIP Address

havip-bp1bwya8f7lppbl0qq6l5

Intranet IPIP

192.168.0.252

ECS Instance

Select

i-bp167uumi7rqzmp8ta0kw
i-bp1cj6it8c8hndkxom7j

HAVIP Details

Refresh Delete

Information	
ID	havip-bp1bwya8f7lppbl0qq6l5
Region	China East 1 (Hangzhou)
VPC ID	vpc-bp1ue3buvqego4vkha4wl
VSwitch	vsw-bp18zyff1ou2azweounr
Status	Allocated
Intranet IPIP	192.168.0.252
Created At	05/02/2018, 15:12:42
Description	- Edit

Resources

```

graph TD
    H[HAVIP Address: 192.168.0.252] --- S[ECS Instance(Slave)]
    H --- M[ECS Instance(Master)]
    S --- U1[Unbind]
    M --- U2[Unbind]
  
```

7. 将路由条目添加至 FortiGate，确保来自 ECS 的所有出站流量均流经 FortiGate。

Route Table

Route Table Details

Route Table ID	vtb-bp17850mvus5wpyvwiogn	VPC ID	vpc-bp1ue3buvqego4vkha4wl
Name	- Edit	Route Table Type	System
Created At	05/02/2018, 13:48:20	Description	- Edit

Route Entry List

Destination CIDR Block	Status	Next Hop	Type	Actions
192.168.0.0/24	● Available	-	System	
192.168.1.0/24	● Available	-	System	
192.168.3.0/24	● Available	-	System	
192.168.4.0/24	● Available	-	System	
100.64.0.0/10	● Available	-	System	

Add Route Entry

● Destination CIDR Block

● Next Hop Type

● HAVIP Address

Route Table

Route Table Details

Route Table ID	vtb-bp17850mvus5wpyvwiogn	VPC ID	vpc-bp1ue3buvqego4vkha4wl
Name	- Edit	Route Table Type	System
Created At	05/02/2018, 13:48:20	Description	- Edit

Route Entry List

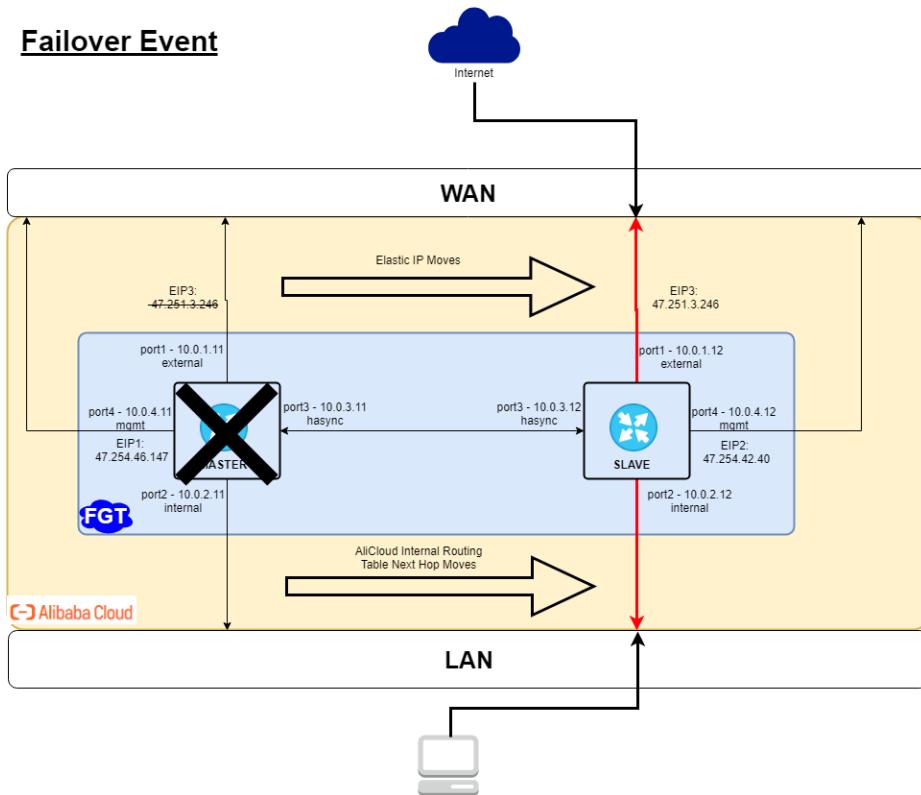
Add Route Entry	Refresh	Route Entry List			
Destination CIDR Block	Status	Next Hop	Type	Actions	
0.0.0.0/0	● Creating	Instance ID:havip-bp1bwya8f7lppbl0qq6l 5 Instance Type:HAVIP	Custom	Delete	
192.168.0.0/24	● Available	-	System		
192.168.1.0/24	● Available	-	System		
192.168.3.0/24	● Available	-	System		
192.168.4.0/24	● Available	-	System		
100.64.0.0/10	● Available	-	System		

连接测试

如需测试FortiGate-VM 实例和 VPC（虚拟专有网络）是否正确配置，请参阅第 14 页连接测试。

使用路由表和EIP在阿里云上部署FortiGate-VM HA

本指南为您提供阿里云可用区主动-被动 FortiGate-VM HA 配置示例。下图为该部署示例的网络拓扑：



下表为此部署示例中 FortiGate-A 的 IP 地址分配列表：

Port	AliCloud primary address	Subnet
port1	10.0.1.11	10.0.1.0/24 EIP3
port2	10.0.2.11	10.0.2.0/24
port3	10.0.3.11	10.0.3.0/24
port4	10.0.4.11	10.0.4.0/24 EIP1

下表为此部署示例中 FortiGate-B 的 IP 地址分配列表：

Port	AliCloud primary address	Subnet
port1	10.0.1.12	10.0.1.0/24
port2	10.0.2.12	10.0.2.0/24
port3	10.0.3.12	10.0.3.0/24
port4	10.0.4.12	10.0.4.0/24

请检查是否满足以下必要条件：

此部署必须满足以下条件：

- 创建1个VPC以及分别用于管理接口、内网流量接口、外部流量接口及心跳接口的子网
- 3个公网 IP 地址：
 - EIP1 和 EIP2 分别用于绑定FortiGate-A 和 FortiGate-B 管理接口
 - EIP3用于绑定HA 外部流量 IP 地址
- 以BYOL或PAYG模式订阅和部署的2个 FortiGate-VM 实例
- 以下为此部署示例中RAM 角色所需的最低管理权限：

 - AliyunECSFullAccess
 - AliyunEIPFullAccess
 - AliyunVPCFullAccess



实际角色配置可能因环境而异。更多详情，请咨询贵公司的公有云管理员。

在阿里云中配置 FortiGate-VM HA，请执行以下操作：

- 在阿里云管理控制台中创建1个包含4个虚拟交换机的VPC：

虚拟交换机名称	用途
net1-external	面向公网端的外部数据流量。
net2-internal	面向专网端的外部数据流量
net3-heartbeat	2个FortiGate 节点间的心跳。通信方式为单播通信。
net4-mgmt	专用管理界面。

Instance ID/Name	VPC	Status	IPv4 CIDR Block	Default VSwitch	Zone	Route Table	Route Table Type	Actions
vsw-rj96khrfvl5gmnj3rk0x net4-mgmt	vpc-rj95m14eo5l u97hjaptw flua-vpc-ha	Available	10.0.4.0/24	No	Silicon Valley Zone A	vib-rj9599919c2uoq oetzra	System	Manage Delete Purchase
vsw-rj9973znqxcsh9fhloqj net3-heartbeat	vpc-rj95m14eo5l u97hjaptw flua-vpc-ha	Available	10.0.3.0/24	No	Silicon Valley Zone A	vib-rj9599919c2uoq oetzra	System	Manage Delete Purchase
vsw-rj9e6tqgp9v12xo0h1jr net2-internal	vpc-rj95m14eo5l u97hjaptw flua-vpc-ha	Available	10.0.2.0/24	No	Silicon Valley Zone A	vib-rj95q1tguwfqqe5ps 3q60i	Custom	Manage Delete Purchase
vsw-rj9tglt2vla806u969hrt net1-external	vpc-rj95m14eo5l u97hjaptw flua-vpc-ha	Available	10.0.1.0/24	No	Silicon Valley Zone A	vib-rj9599919c2uoq oetzra	System	Manage Delete Purchase

2. 添加6个ENI (弹性网络接口)

Elastic Compute Serv...	eni- rj9dimvg0hykei8bl8o fhuu-net4-12	vsw- rj9khmf... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj95x...	47.254.42.40 10.0.4.12	Secondary/ 00:16:3e:00:c0:a5	Bound May 31, 2019, 14:42	Modify Unbind Manage Secondary Private IP Address Delete
Overview	eni- rj9ga16wvcti7anp0at7m fhuu-net3-12	vsw- rj9973fz... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj95x...	10.0.3.12	Secondary/ 00:16:3e:00:14:b9	Bound May 31, 2019, 14:42	Modify Unbind Manage Secondary Private IP Address Delete
Tags	eni- rj9y4eztzg3bv65yqd6x fhuu-net2-12	vsw- rj9e6tag... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj95x...	10.0.2.12	Secondary/ 00:16:3e:00:1d:8d	Bound May 31, 2019, 14:42	Modify Unbind Manage Secondary Private IP Address Delete
Instances	eni- rj911uoh9t3qd5doe3 fhuu-net4-11	vsw- rj9khmf... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj91t...	47.254.46.147 10.0.4.11	Secondary/ 00:16:3e:00:2ba7	Bound May 31, 2019, 14:41	Modify Unbind Manage Secondary Private IP Address Delete
Elastic Container In...	eni- rj91wj13vwjs7y1n25ow fhuu-net3-11	vsw- rj9973fz... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj91t...	10.0.3.11	Secondary/ 00:16:3e:00:45:3e	Bound May 31, 2019, 14:41	Modify Unbind Manage Secondary Private IP Address Delete
HPC Clusters	eni- rj94jig06lag0v1jnevy fhuu-net2-11	vsw- rj9e6tag... vpc- rj9h5m14...	Silicon Valley Zone A	sg-rj99v... i-rj91t...	10.0.2.11	Secondary/ 00:16:3e:00:c0:1a	Bound May 31, 2019, 14:39	Modify Unbind Manage Secondary Private IP Address Delete
Reserved Instances	eni- rj95mchbk2uqxq0y6t8	vsw- rj9mwzsu... vpc- rj9h23d9...	Silicon Valley Zone A	sg-rj99v... i-rj94e...	192.168.0.184	Primary 00:16:3e:00:c1:47	Bound May 31, 2019, 09:21	Modify Unbind Manage Secondary Private IP Address Delete
Custom Images								
Deployment & Elastic								
Storage & Snapshots								
Network & Security								
Security Groups								
ENI								
SSH Key Pair								

3. 创建2个路由表:

- a. 为虚拟交换机“net2-internal”创建一个名为“rtb-internal”的路由表。将NIC2的IP地址(10.0.2.11)设置为“rtb-internal”的默认网关。您可在FortiGate-A上配置NIC2后创建此路由表。确保默认网关为FortiGate-A port2的ENI。

The screenshot shows the 'Route Table Details' page. The 'Route Entry List' tab is selected. A new route entry is being added with the following details:

- Destination CIDR Block: 0.0.0.0/0
- Status: Available
- Next Hop: eni-rj94jig06lag0v1jnevy
- Type: Custom
- Action: Delete

The table also lists other existing route entries:

Destination CIDR Block	Status	Next Hop	Type	Actions
10.0.1.0/24	Available	-	System	
10.0.2.0/24	Available	-	System	
10.0.3.0/24	Available	-	System	
10.0.4.0/24	Available	-	System	
100.64.0.0/10	Available	-	System	

- b. 为其余虚拟交换机创建一个名为“rtb-external”的路由表。将此VPC的互联网网关设置为其默认网关。确保该路由表可访问互联网。

Route Table Details

Route Table ID	vtb-rj9g999919c2uoqetzra	VPC ID	vpc-rj9h5m14eo5lu97hjaptw
Name	rtb-external	Route Table Type	System
Created At	05/30/2019, 16:26:01	Description	- Edit

Route Entry List Associated VSwitches

Destination CIDR Block	Status	Next Hop	Type	Actions
10.0.1.0/24	Available	-	System	Edit
10.0.2.0/24	Available	-	System	Edit
10.0.3.0/24	Available	-	System	Edit
10.0.4.0/24	Available	-	System	Edit
100.64.0.0/10	Available	-	System	Edit

在阿里云中部署 FortiGate-VM，请执行以下操作：

如需利用 A-P (热备式) HA模式，您需为组成 A-P HA 集群的每个 FortiGate-VM 配置四个 vNIC (port1 至 port4)。配置支持 A-P HA 模式需要的所有网络接口（参见阿里云ENI和FortiGate-VM 网络接口配置）。您必须选择至少支持4个NIC的阿里云实例规格。

请确保已完成以下操作：

- 已为每个子网的出入接口配置适当安全组。请特别注意，管理接口应具备互联网出口访问权限，用于API接口调用以接入阿里云元数据服务器。
- 已分别为每个 FortiGate-VM 配置4个NIC，并已分配静态专用 IP 地址。
- 已将EIP1与管理接口FortiGate-A port4绑定。
- 已将EIP3与外部接口FortiGate-A port1绑定。
- 已将EIP2与管理接口FortiGate-B port4绑定。



您可通过在VPC中创建一个HAVIP地址，然后将该 HAVIP 地址与2个 FortiGate 外部接口绑定，从而在主FortiGate-VM的外部接口上附加绑定一个公共IP地址，而非EIP。

FGT-A

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(All)	Status/Created At	Actions
eni-rj9h5m14eo5lu97hjaptw	vsw-rj9g999919c2uoqetzra	vpc-rj9h5m14eo5lu97hjaptw	Silicon Valley Zone A	sg-rj99v...	47.251.3.246	10.0.1.11	Primary 00:16:3e:00:02:4d	Bound May 31, 2019, 15:02	Modify Unbind Manage Secondary Private IP Address Delete
eni-rj9h11uoh9t3qd5doe3	vsw-rj99khfr...	vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...	47.254.46.147	10.0.4.11	Secondary 00:16:3e:00:2ba7	Bound May 31, 2019, 14:41	Modify Unbind Manage Secondary Private IP Address Delete
eni-rj91wvj3vvjs7y1n25ow	vsw-rj997fz...	vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.3.11	Secondary 00:16:3e:00:45:3e	Bound May 31, 2019, 14:41	Modify Unbind Manage Secondary Private IP Address Delete
eni-rj94jig06fag01jnely	vsw-rj96ftaq...	vpc-rj9h5m14...	Silicon Valley Zone A	sg-rj99v...		10.0.2.11	Secondary 00:16:3e:00:c0:1a	Bound May 31, 2019, 14:39	Modify Unbind Manage Secondary Private IP Address Delete

如需使用 CLI 配置 FortiGate-A, 请执行以下操作:

以下命令向您展示了如何在GUI上使用CLI命令或通过SSH配置 A-P HA 设置。若使用 SSH进行设置, FortiGate 可能因路由表更改而切断连接, 因此建议通过 GUI 配置 HA。

```

config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.11 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.2.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.3.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.4.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.1.253
        set device "port1"
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable

```

```

        next
    end

config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.253
        next
    end
    set priority 128
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.12
end

```

如需使用 CLI 配置 FortiGate-B，请执行以下操作：

以下命令向您展示了如何在GUI上使用CLI命令或通过SSH配置 A-P HA 设置。若使用 SSH进行设置，FortiGate 可能因路由表更改而切断连接，因此建议通过 GUI 配置 HA。

```

config system interface
    edit "port1"
        set mode static
        set ip 10.0.1.12 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.2.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.3.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.4.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.1.253
        set device "port1"
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept

```

```

        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.4.253
        next
    end
    set priority 64
    set unicast-hb enable
    set unicast-hb-peerip 10.0.3.11
end

```



设置防火墙优先级时，FortiGate-B HA 的数值必须低于 FortiGate-A。具有较低优先级的节点将被确定为备用节点。

如需检查 HA 状态和功能，请执行以下操作：

1. 在主 FortiGate 的 FortiOS 中，点击进入System > HA。检查 HA 状态是否已同步。
2. 登录位于内部子网的 PC。验证当 FortiGate-A 为主节点时，该PC 是否可通过 FortiGate-A 访问互联网。
3. 关闭 FortiGate-A。验证 FortiGate-B 是否自动切换为主节点。使用 API 调用验证备用专用IP地址是否自动切换至FortiGate-B。
4. 登录PC。验证当 FortiGate-B 为主节点时，该PC 是否可通过 FortiGate-B 访问互联网。
5. 您可使用以下诊断命令，检查故障转移期间，备用专用 IP地址是否从 FortiGate-A 自动切换至 FortiGate-B：

```
FGT-B # diagnose debug application alicloud-ha -1
Debug messages will be on for 30 minutes.
```

```
FGT-B # Become HA master mode 2
===== start acs ha failover =====
send_vip_arp: vd root master 1 intf port1 ip 10.0.1.12
send_vip_arp: vd root master 1 intf port2 ip 10.0.2.12
acs meta info [instance id]: i-rj9f5xs9cp9xsweedlcs
acs meta info [ram role]: fhua-ecs-role
acs meta info [region]: us-west-1
acs meta info [vpc id]: vpc-rj9h5m14eo5lu97hjaptw
acs ecs endpoint is resolved at ecs.us-west-1.aliyuncs.com:47.88.73.18
acs vpc endpoint is resolved at vpc.aliyuncs.com:106.11.61.112
acs is parsing page 1 of total 3(1 page) instances
```

```

acs is checking tags on instance FGT-A
Tag.FGT_port1: eni-rj9dirnvg0hykodvv7z
Tag.FGT_port2: eni-rj94jig06fag0v1jneyv
Tag.FGT_port3: eni-rj91wj13vwjs7y1n25ow
Tag.FGT_port4: eni-rj9illiuoh9t3qd5doe3
acs is checking tags on instance FGT-B
Tag.FGT_port1: eni-rj9f5xs9cp9xswekw6zh
Tag.FGT_port2: eni-rj9j4eztzg3bv65yqd6x
Tag.FGT_port3: eni-rj9ga16wcti7anp0ot7m
Tag.FGT_port4: eni-rj9dirnvg0hykei8bl8o
acs is parsing page 1 of total 13(1 page) EIPs
acs local instance: FGT-B(i-rj9f5xs9cp9xsweedlcs)
eni: 0, 10.0.1.12(eni-rj9f5xs9cp9xswekw6zh, port1)
eni: 1, 10.0.2.12(eni-rj9j4eztzg3bv65yqd6x, port2)
eni: 2, 10.0.3.12(eni-rj9ga16wcti7anp0ot7m, port3)
eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9illiuoh9t408i1a60)
eni: 0, 10.0.1.11(eni-rj9dirnvg0hykodvv7z, port1) <--- eip(47.251.3.246)
eni: 1, 10.0.2.11(eni-rj94jig06fag0v1jneyv, port2)
eni: 2, 10.0.3.11(eni-rj91wj13vwjs7y1n25ow, port3)
eni: 3, 10.0.4.11(eni-rj9illiuoh9t3qd5doe3, port4) <--- eip(47.254.46.147)
acs is moving eip(47.251.3.246) from eni0(10.0.1.11) to eni0(10.0.1.12)
acs eip(47.251.3.246) status: Unassociating
acs eip(47.251.3.246) status: Unassociating
acs eip(47.251.3.246) status: Available
acs unassociated eip(47.251.3.246) from instance FGT-A successfully
acs eip(47.251.3.246) status: Associating
acs eip(47.251.3.246) status: Associating
acs eip(47.251.3.246) status: InUse
acs associated eip(47.251.3.246) to instance FGT-B successfully
acs local instance: FGT-B(i-rj9f5xs9cp9xsweedlcs)
eni: 0, 10.0.1.12(eni-rj9f5xs9cp9xswekw6zh, port1) <--- eip(47.251.3.246)
eni: 1, 10.0.2.12(eni-rj9j4eztzg3bv65yqd6x, port2)
eni: 2, 10.0.3.12(eni-rj9ga16wcti7anp0ot7m, port3)
eni: 3, 10.0.4.12(eni-rj9dirnvg0hykei8bl8o, port4) <--- eip(47.254.42.40)
acs peer instance: FGT-A(i-rj9illiuoh9t408i1a60)
eni: 0, 10.0.1.11(eni-rj9dirnvg0hykodvv7z, port1)
eni: 1, 10.0.2.11(eni-rj94jig06fag0v1jneyv, port2)
eni: 2, 10.0.3.11(eni-rj91wj13vwjs7y1n25ow, port3)
eni: 3, 10.0.4.11(eni-rj9illiuoh9t3qd5doe3, port4) <--- eip(47.254.46.147)
acs route table: vtb-rj9qltgufwqqe5ps3q60i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.11(eni-rj94jig06fag0v1jneyv)
acs is deleting route table entry: 0.0.0.0/0 via 10.0.2.11
acs route table entry deleting
acs route table entry deleted
acs deleted route table entry: 0.0.0.0/0 via 10.0.2.11 successfully
acs is creating route table entry: 0.0.0.0/0 via 10.0.2.12
acs route table entry created

```

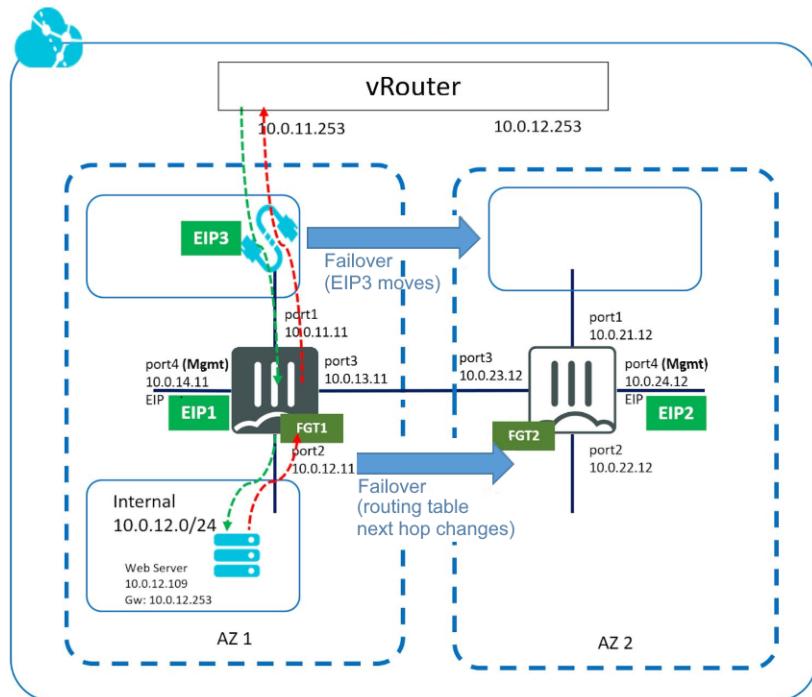
```

acs created route table entry: 0.0.0.0/0 via 10.0.2.12 successfully
acs route table: vtb-rj9q1tgufwqqe5ps3q60i
rule: cidr: 0.0.0.0/0, nexthop: 10.0.2.12 (eni-rj9j4eztzg3bv65yqd6x)
===== exit acs ha failover =====

```

在阿里云可用区之间部署 FortiGate-VM HA

本指南提供了在阿里云单一区域（region）不同可用区（AZ）之间手动配置主动-被动 FortiGate-VM HA 的示例。以下为此部署示例的网络拓扑：



下表为此部署示例中 FortiGate-A 的 IP 地址分配列表：

接口	阿里云主地址	子网
port1	10.0.11.11	10.0.11.0/24 EIP3
port2	10.0.12.11	10.0.12.0/24
port3	10.0.13.11	10.0.13.0/24
port4	10.0.14.11	10.0.14.0/24 EIP1

下表为该部署示例中 FortiGate-B 的 IP 地址分配列表：

接口	阿里云主地址	子网
port1	10.0.21.12	10.0.21.0/24
port2	10.0.22.12	10.0.22.0/24
port3	10.0.23.12	10.0.23.0/24
port4	10.0.24.12	10.0.24.0/24 EIP2



IPsec VPN 的阶段1配置不可跨可用区在主备 FortiGate 之间实现同步。阶段 2 配置可实现同步。

请检查是否满足以下先决条件：

该部署需满足以下条件：

- 创建1个VPC以及分别用于管理接口、内网流量接口、外部流量接口及心跳接口的子网
- 3个公网 IP 地址：
 - EIP1 和 EIP2 分别用于绑定FortiGate-A 和 FortiGate-B 管理接口
 - EIP3用于绑定HA 外部流量 IP 地址
- 部署2个拥有相同实例类型的 FortiGate-VM 实例。请选择至少支持四个网络接口的实例类型。
- 以下为该部署示例中[RAM 角色](#)所需的最低管理权限：
 - AliyunECSFullAccess
 - AliyunEIPFullAccess
 - AliyunVPCFullAccess



实际角色配置可能因环境而异。更多详情，请咨询贵公司的公有云管理员。

如需在阿里云中配置 FortiGate-VM HA，请执行以下操作：：

- 在阿里云管理控制台中创建一个包含8个虚拟交换机的VPC（每个可用区4个）：

虚拟交换机名称	用途
net1-external-za	面向公网端的外部数据流量。
net2-internal-za	面向受保护/受信任网络端的内网数据流量接口。
net3-heartbeat-za	2个 FortiGate 节点间的心跳。通信方式为单播通信。
net4-mgmt-za	专用管理接口。
net1-external-zb	面向公网端的外部数据流量。
net2-internal-zb	面向受保护/受信任网络端的内部数据流量接口。
net3-heartbeat-zb	2个 FortiGate 节点间的心跳。通信方式为单播通信。
net4-mgmt-zb	专用管理接口。

The screenshot shows the Alibaba Cloud VSwitches management interface. On the left, there's a sidebar with navigation links like VPCs, Route Tables, and VSwitches. The main area is titled 'VSswitches' and shows a table of 8 virtual switches. Each row includes columns for 'Instance Name', 'VPC', 'Status', 'IPv4 CIDR Block', 'Number of Available Private IPs', 'Default VSwitch', 'Zone', 'Route Table', 'Route Table Type', and 'Actions'. The switches are distributed across two zones: Silicon Valley Zone A and Zone B.

- 添加6个ENI：每个可用区3个：

The screenshot shows the Alibaba Cloud Network Interfaces management interface. On the left, there's a sidebar with navigation links like Overview, Instances & Images, Basic Container Images, Reserved Instances, Deployment & Elastic..., Storage & Snapshots, Network & Security, and Security Groups. The main area is titled 'Network Interfaces' and shows a table of 6 elastic network interfaces. Each row includes columns for 'Name', 'Search by ENI name...', 'Tags', 'VSwitch/VPC', 'Zone', 'Security Group ID', 'Bound Instance', 'Public IP Address', 'Primary Private IP Address', 'Type/MAC Address/All', 'Status/Created At', and 'Actions'. The ENIs are bound to various instances and security groups across two zones.

- 创建2个路由表：

- 为 net2-internal 虚拟交换机创建一个名为“rtb-internal”的路由表。将 NIC2 IP 地址（10.0.12.11）设置为“rtb-internal”的默认网关。您可在 FortiGate-A 上配置 NIC2 后创建该路由表。确保默认网关为 FortiGate-A port2 的 ENI。

The screenshot shows the Route Table Details page for the 'rtb-internal' route table. It includes fields for Route Table ID (vrt-008bae3c050d04c), VPC ID (vpc-09c0e16252877vpdv), Name (rtb-internal), and Description. The table lists route entries with columns for Destination CIDR Block, Status, Next Hop, Type, and Actions. The table has 10 entries, all marked as Available and System type.

Destination CIDR Block	Status	Next Hop	Type	Actions
0.0.0.0/0	Available	eni-00200e031919190d	Custom	Delete
10.0.11.0/24	Available	-	System	
10.0.12.0/24	Available	-	System	
10.0.13.0/24	Available	-	System	
10.0.14.0/24	Available	-	System	
10.0.21.0/24	Available	-	System	
10.0.22.0/24	Available	-	System	
10.0.23.0/24	Available	-	System	
10.0.24.0/24	Available	-	System	
100.64.0.0/10	Available	-	System	

- b. 为其余虚拟交换机创建名为“rtb-external”的路由表。将此VCN的互联网网关设置为其默认网关。确保该路由表可访问互联网。

The screenshot shows the Route Table Details page for the 'rtb-external' route table. It includes fields for Route Table ID (vrt-008bae3c050d04c), VPC ID (vpc-09c0e16252877vpdv), Name (rtb-external), and Description. The table lists route entries with columns for Destination CIDR Block, Status, Next Hop, Type, and Actions. The table has 10 entries, all marked as Available and System type.

Destination CIDR Block	Status	Next Hop	Type	Actions
10.0.11.0/24	Available	-	System	
10.0.12.0/24	Available	-	System	
10.0.13.0/24	Available	-	System	
10.0.14.0/24	Available	-	System	
10.0.21.0/24	Available	-	System	
10.0.22.0/24	Available	-	System	
10.0.23.0/24	Available	-	System	
10.0.24.0/24	Available	-	System	
100.64.0.0/10	Available	-	System	

如需在阿里云中部署 FortiGate-VM，请执行以下操作：

如需利用A-P（热备式）HA模式，您需为组成A-P HA集群的每个FortiGate-VM配置四个vNIC（port1至port4）。配置支持A-P HA所需的所有网络接口（参见阿里云ENI和FortiGate-VM网络接口配置）。您必须选择至少支持4个NIC的阿里云实例规格。

确保已完成以下操作：

- 已为每个子网的出入接口配置适当的安全组。请特别注意，管理接口应具备互联网出口访问权限，用于API接口调用以访问阿里云元数据服务器。
- 已为每个FortiGate-VM配置4个NIC，并分配了静态专用IP地址。
- 已将EIP1与管理接口FortiGate-A port4绑定。
- 已将EIP3与外部接口FortiGate-A port1绑定。
- 已将EIP2与管理接口FortiGate-B port4绑定。

阿里云 FortiGate-VM 高可用性配置

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(AII)	Status/Created At	Actions
eni-0906dec2busbbsrv4	vsw-095552...	vpc-0f9cke...	Silicon Valley Zone A	sg-0f9ab...	47.254.46.147	10.0.14.11	Secondary 00:16:3e:00:a3:6b	Bound June 25, 2019, 14:05	Modify Unbind Manage Secondary Private IP Address Delete
eni-096cd5pk3d0scnpli	vsw-09v39j...	vpc-0f9cke...	Silicon Valley Zone A	sg-0f9ab...		10.0.13.11	Secondary 00:16:3e:00:00:29	Bound June 25, 2019, 14:05	Modify Unbind Manage Secondary Private IP Address Delete
eni-0920sged01g1qfod	vsw-09wy91...	vpc-0f9cke...	Silicon Valley Zone A	sg-0f9ab...		10.0.12.11	Secondary 00:16:3e:00:42:56	Bound June 25, 2019, 14:04	Modify Unbind Manage Secondary Private IP Address Delete
eni-09fc057y0db1m0un2a	vsw-09fb05...	vpc-0f9cke...	Silicon Valley Zone A	sg-0f9ab...	47.251.3.246	10.0.11.11	Primary 00:16:3e:00:00:2c	Bound June 25, 2019, 12:10	Modify Unbind Manage Secondary Private IP Address Delete

ID/Name	Tags	VSwitch/VPC	Zone	Security Group ID	Public IP Address	Primary Private IP Address	Type/MAC Address(AII)	Status/Created At	Actions
eni-091550b2cep1ay3na	vsw-09520...	vpc-0f9cke...	Silicon Valley Zone B	sg-0f9ab...		10.0.21.12	Primary 00:16:3e:00:bcae	Bound June 25, 2019, 14:13	Modify Unbind Manage Secondary Private IP Address Delete
eni-091550b2cep1ay3na	vsw-09520...	vpc-0f9cke...	Silicon Valley Zone B	sg-0f9ab...	47.254.42.40	10.0.24.12	Secondary 00:16:3e:00:81:ee	Bound June 25, 2019, 14:06	Modify Unbind Manage Secondary Private IP Address Delete
eni-09050084hp6k	vsw-09mm8...	vpc-0f9cke...	Silicon Valley Zone B	sg-0f9ab...		10.0.23.12	Secondary 00:16:3e:00:6eff:a	Bound June 25, 2019, 14:06	Modify Unbind Manage Secondary Private IP Address Delete
eni-091550b2cep1ay3na	vsw-094045...	vpc-0f9cke...	Silicon Valley Zone B	sg-0f9ab...		10.0.22.12	Secondary 00:16:3e:00:48:7e	Bound June 25, 2019, 14:06	Modify Unbind Manage Secondary Private IP Address Delete

如需使用 CLI 配置 FortiGate-A，请执行以下步骤：

下一步将向您展示如何在GUI上使用CLI命令或通过SSH配置 A-P HA 设置。若使用 SSH进行配置，FortiGate 可能因路由表更改而切断连接，因此建议通过 GUI 配置 HA。

```
config system interface
    edit "port1"
        set mode static
        set ip 10.0.11.11 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.12.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.13.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.14.11 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.11.253
        set device "port1"
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
```

```
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set nat enable
next
end

config system ha
    set group-name "FGT-HA"
    set mode a-p
    set hbdev "port3" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.14.253
        next
    end
    set priority 192
    set unicast-hb enable
    set unicast-hb-peerip 10.0.23.12
end
```

如需使用 CLI 配置 FortiGate-B，请执行以下操作：

下一步将向您展示如何在 GUI 上使用 CLI 命令或通过 SSH 配置 A-P HA 设置。若使用 SSH 进行配置，FortiGate 可能因路由表更改而切断连接，因此建议通过 GUI 配置 HA。

```
config system interface
    edit "port1"
        set mode static
        set ip 10.0.21.12 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
    next
    edit "port2"
        set ip 10.0.22.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port3"
        set ip 10.0.23.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
    edit "port4"
        set ip 10.0.24.12 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
    next
end

config router static
    edit 1
        set gateway 10.0.21.253
        set device "port1"
    next
end
```

```

config firewall policy
edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
next
end

config system ha
set group-name "FGT-HA"
set mode a-p
set hbdev "port3" 50
set ha-mgmt-status enable
config ha-mgmt-interfaces
edit 1
    set interface "port4"
    set gateway 10.0.24.253
next
end
set priority 64
set unicast-hb enable
set unicast-hb-peerip 10.0.13.11
end

```



设置防火墙优先级时，FortiGate-B HA 的数值必须低于 FortiGate-A。具有较低优先级的节点将被确定为备用节点。

检查 HA 状态和功能，请执行以下操作：

- 在主 FortiGate 的 FortiOS 中，点击进入 *System > HA*。检查 HA 状态是否已同步。

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
Yes	64	FGT-A	FGTALIURNL7L4OS9B	Master	00:00:37:36	11	29.00 kbps
Yes	192	FGT-B	FGTALIAFPJABDCE	Slave	00:00:37:46	12	24.00 kbps

- 登录位于内部子网的 PC。验证当 FortiGate-A 为主节点时，该PC 是否可通过 FortiGate-A 访问互联网。
- 关闭 FortiGate-A。验证 FortiGate-B 是否自动切换为主节点。
- 登录PC。验证当 FortiGate-B 为主节点时，该PC 是否可通过 FortiGate-B 访问互联网。
- 可使用命令“diagnose debug application alicloud-ha -1”，查看故障转移期间，备用专用 IP 地址是否从 FortiGate-A 自动切换至 FortiGate-B。

FortiGate-VM 主动-主动 HA 配置

请参阅阿里云主动-主动出口路由故障切换。

阿里云弹性伸缩部署

您可部署 FortiGate-VM 以支持阿里云弹性伸缩（Auto Scaling）。

多个 FortiGate-VM 实例可组成一个弹性伸缩组，以便在工作负载过高时提供高性能集群。FortiGate-VM 实例可根据预定义的工作负载等级自动横向扩展。凭借 FortiGate 原生高可用性（HA）功能（如 config-sync）可实现弹性伸缩，该功能可在发生横向扩展（scale-out）事件时跨多个 FortiGate-VM 实例实现操作系统（OS）配置同步。

FortiGate Autoscale for AliCloud 适用于 FortiOS 6.2 及更高版本按需使用（PAYG）实例。标准部署包含以下内容：

- 跨2个可用区（AZ）的高可用性架构。
- 已配置公有子网和专用子网的虚拟专用云（VPC）。
- 允许从受保护服务器传出流量的 NAT 网关。
- 在部署过程中创建面向外网的负载均衡器。面向内网的负载均衡器为可选项。
- 运行由 Fortinet 提供脚本的阿里云函数计算（AliCloud Function Compute），以实现弹性伸缩。该函数用于处理弹性伸缩和故障转移管理。
- 开放结构化数据服务（OTS）或表格存储（TableStore）以及一个存储弹性伸缩配置信息（如主/备IP地址）的 NoSQL 数据库。

规划

部署 FortiGate Autoscale for AliCloud 的最简单方法是使用 Terraform。

此部署已经以下方法进行测试：

- Terraform 0.11
- Terraform provider for AliCloud 1.48.0

要求

安装和配置 FortiGate AutoScale for AliCloud 需要了解以下内容：

- 使用 CLI 配置 FortiGate
- 阿里云服务
- Terraform

建议由熟悉上述内容的 DevOps 工程师或高级系统管理员部署 FortiGate Autoscale for AliCloud。

RAM账号权限

可使用管理员帐号部署该解决方案。由于管理员账号对阿里云账号下的所有资源拥有完全控制权，因此您需自行创建一个单独的 RAM（资源访问管理）账号，并确保至少拥有以下管理权限：

- AliyunVPCFullAccess
- AliyunEIPFullAccess
- AliyunOSSFullAccess
- AliyunECSFullAccess
- AliyunSLBFullAccess
- AliyunOTSFulAccess
- AliyunESSFullAccess
- AliyunFCFullAccess
- AliyunRAMFullAccess
- AliyunBSSOrderAccess

区域要求

如需在阿里云中部署 FortiGate 弹性伸缩集群，该区域必须支持以下服务：

- TableStore
- OSS
- 函数计算
- 弹性伸缩
- NAT 网关

支持区域

以下区域包含运行 FortiGate AutoScale for AliCloud 所需的所有服务

可用区域	扩展
亚太东北部1（东京）	m-6weakry8j13jxmjlmi4o
亚太东南部 2（悉尼）	m-p0wb4dw13d6qc1sndaj6
亚太南部 1（孟买）	m-a2dbkrpr8wsobn9ygddc
欧洲中部 1（法兰克福）	m-gw8cizn7dguyeikpgozb
美国东部 1（弗吉尼亚）	m-0xif6xxwhjlqhoaqjrr6
美国西部 1（硅谷）	m-rj91iqplyxdp7crb0gvj

部署信息

Terraform 将部署以下资源：

- 跨2个可用区配置2个子网的VPC
- 2个虚拟交换机
- 1个NAT网关
- 1个弹性伸缩集群
- 1种弹性伸缩配置
- 2种弹性伸缩规则：横向缩减（Scale in）和横向扩展（Scale out）
- 1个对象存储服务（OSS）存储桶（bucket）
- 函数计算服务、函数和HTTP触发器
- 2个安全组规则：Allow all（全部允许）和Allow only internal connections（仅允许内部连接）
- 1个表格存储（TableStore）实例和5个表
- 3个弹性IP（EIP）地址
- 1个拥有描述和创建弹性网络接口（ENI）权限的RAM角色
- 1个面向外网的负载均衡器

部署

1. 登录阿里云账号。若无阿里云账号，请按照阿里云[创建RAM用户](#)章节中的说明自行创建账号。RAM 帐号必须拥有[第 58 页 RAM 帐户权限](#)小节中列出的最低管理权限。
2. 创建阿里云AccessKey密钥。有关[创建访问密钥](#)的详细信息，请参阅阿里云[创建AccessKey密钥](#)章节，创建AccessKeyId和AccessKey密钥。
3. 安装Terraform。有关安装的详细信息，请参阅 HashiCorp 安装 Terraform章节。
4. 获取 FortiGate AutoScale for AliCloud 部署包。访问 [GitHub 项目发布页面](#)，下载需使用的相应版本压缩包 `fortigate-autoscale-alicloud.zip`。
5. 在本地电脑上解压缩文件。将提取以下文件和文件夹：

```
|── alicloud_function_compute  
|── alicloud_terraform  
|── core  
|── dist  
|── LICENSE  
|── node_modules  
|── package.json  
|── scripts  
└── test
```

6. 在您的终端中，将其更改为`alicloud_terraform`文件夹：

```
cd alicloud_terraform
```

`alicloud_terraform`文件夹包含以下文件：

```
|── assets  
|   └── configset  
|       ├── baseconfig  
|       ├── httproutingpolicy  
|       ├── httpsroutingpolicy  
|       ├── internalelbweb  
|       └── storelogtofaz  
|── main.tf  
└── vars.tf
```

- `baseconfig`包含 FortiGate-VM 的 `cloud-init`配置，可适当进行调整以支持更高级设置。
- `main.tf`包含大部分部署代码。作为部署的一部分，可将`baseconfig`上传至 OSS 存储桶，供 FortiGate-VM 实例使用。
- `vars.tf`包含部署所需变量。例如：镜像 ID (`instance_ami`)、集群名称、实例、区域等。有关所包含变量的详细说明，请参阅[第 61 页Terraform变量](#)。

7. 编辑 `vars.tf`文件并自定义部署变量。



OSS存储桶的名称必须为小写字母。

函数计算 URL 不得超过 127 个字符。变量`cluster_name`用于创建该 URL。

8. 使用命令 `terraform init` 初始化 provider 插件和模块：

```
terraform init
```

9. 使用以下命令提交 Terraform 计划：

```
terraform plan -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region=<region>"
```

10. 确认并应用计划：

```
terraform apply -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region=<region>"
```

输出命令类似下图所示。随机生成的三个字母后缀将添加至所有资源中，并可用于帮助识别集群资源。

```
Apply complete! Resources: 48 added, 0 changed, 0 destroyed.

Outputs:

Auto Scaling Group ID = asg-0xi1g2hk9z048yn6cuu1
AutoScale External Load Balancer IP = 47.89.136.18
PSK Secret = !_YfA7FQ@b_aYuei
Scale In Threshold = 35
Scale Out Threshold = 70
VPC name = FortigateAutoScale-rrr
```

Terraform 变量

以下为 `vars.tf` 文件中的变量列表。可自行更改以满足您的集群需求。

资源	默认	描述
access_key	要求输入	AliCloud AccessKey。 有关创建 AccessKey 密钥的详细信息，请参阅阿里云创建 AccessKey 密钥章节 。
secret_key	要求输入	使用 AccessKey 创建的阿里云密钥，用于访问 API。
region	us-east-1	阿里云区域。
scale_in_threshold	35	用于横向缩减（移除）1 个实例的默认聚合 CPU 阈值（百分比）。
scale_out_threshold	70	用于横向扩展（添加）1 个实例的默认聚合 CPU 阈值（百分比）。
alicloud_account	阿里云账号	(数据类型)
cluster_name	FortigateAutoScale	跨对象使用的集群名称。
bucket_name	fortigateautoscale	OSS 存储桶名称，必须为小写字母。

资源	默认	描述
instance_ami	要求输入	若为指定状态，将成为build命令使用的镜像。否则，脚本将获取最新的 FortiGate AMI。
instance	ecs.sn1ne	弹性伸缩配置需选择的实例系列规格。
vpc_cidr	172.16.0.0/16	VPC无类别域间路由（CIDR）块，分为2个/21子网。
vswitch_cidr_1	172.16.0.0/21	第1个 Vswitch 位于该区域的可用区A。
vswitch_cidr_2	172.16.8.0/21	第2个Vswitch位于该区域的可用区B。
table_store_instance_type	容量	默认值为 <i>HighPerformance</i> (高性能) 或 <i>Capacity</i> (容量)。

可使用以下方法从命令行引用变量：

```
terraform plan -var "<var name>=<value>"
```

验证部署

1. 登录阿里云控制台，进入TableStore（表格存储）。
2. 点击进入表FortiGateMasterElection。
3. 记录主 FortiGate-VM IP 地址，并确保voteState（投票状态）已完成。有关示例，请参阅以下内容：

 FortiGateMasterElection

Table Data Insert Search Update Delete

Data Source:FortiGateMasterElection Table can display up to 50 rows.

	Row Detail	asgName(Primary Key)	instanceId	ip	subnetId	voteEndTime	voteState	vpcId
■	Row Detail	Master	i-0xi2pts0vr46rxhht3...	172.16.14.111	candidateInstanceId...	1.561416933046E12	done	candidateInstanc...
Total: 1 item(s), Per Page: 10 item(s) « < 1 > »								

4. 点击表FortiGateAutoscale并确认已添加至集群中的实例。以下为健康状态的集群示例：

Table Data Insert Search Update Delete

Data Source:FortiGateAutoscale Table can display up to 50 rows.

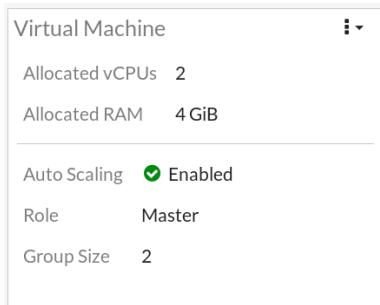
	Row Detail	instanceId(Primary K...)	HeartBeatLossCount	MasterIp	NextHeartBeatTime	SyncState	autoScalingGroupName	heartBeatInterval
■	Row Detail	i-0xi2pts0vr46rxhht3...	0.0	172.16.14.111	1.561418453349E12	in-sync	FortigateAutoScale-g...	10.0
■	Row Detail	i-0xial3fyiqsf3tgbiz...	0.0	172.16.14.111	1.561418451745E12	in-sync	FortigateAutoScale-g...	10.0
Total: 2 item(s), Per Page: 10 item(s) « < 1 > »								



MasterIp 列显示主 FortiGate-VM IP 地址。
从集群中删除实例时，该实例在此表中的记录不会被删除。

5. 使用步骤 3 中的公网 IP 地址登录至主 FortiGate-VM 实例。默认管理端口为 8443，默认用户名/密码为：admin/<instance-id>。

6. 从 Web 界面中，您可查看实例角色和当前集群大小：



7. 从 CLI 中键入以下命令，获取角色状态和当前*callback-url*：

```
get system auto-scale
```

输出命令类似下图所示：

```
status          : enable
role           : master
sync-interface : port1
callback-url   : https://*****.ap-southeast-5-internal.fc.aliyuncs.com/2016-
08-15/proxy/FortigateAutoScale-smc/FortiGateASG-rrr/
hb-interval    : 10
psksecret      : *
```

删除集群

如需删除群集，请首先输入并验证以下代码：

```
terraform destroy -var "access_key=<access_key>" -var "secret_key=<secret_key>" -var "region=<region>"
```

当表中存有数据时，对表的删除操作将受限。因此，必须从控制台手动删除TableStore。

如需删除TableStore，请执行以下操作：

1. 点击进入表格，然后点击Delete删除选中的表格：

The screenshot shows the FortiGate Table Store management interface. At the top, there is a navigation bar with icons for Home, Cluster, Firewall, Network, Application, System, and Help. Below the navigation bar, there is a search bar and a filter section with dropdowns for Region, Type, and Status.

The main content area displays a table of tables. The columns include Table Name, Time To Live, Max Versions, Max Version Offset, Stream Status, Monitor, Table Size, Actions, and a Delete button. The table lists several tables, including FortiAnalyzer, FortiGateAutoscale, FortiGateLifecycleItem, FortiGateMasterElection, and Settings. The Delete button for the Settings table is highlighted with a red border.

At the bottom of the page, there is a footer with links for Help, Support, and Contact Us, along with the Fortinet logo.

2. 删除表后，返回`Instance`（实例）页面，单击`Release`（释放）：

Instance Name	Instance Type	Instance Description	Status	Created At	Monitor	Actions
FortiGateASG-rrr	Capacity	TableStore Instance Terraform...	Running	2019-06-20 12:45:51	Link	Manage Release

故障排除

调试cloud-init

启动时若出现问题，请先检索`cloud-init`（云初始化）日志。检索日志，请登录 FortiGate-VM 并在 CLI 中输入以下命令：

```
diag debug cloudinit show
```

输出命令类似下图所示：

```
>> Checking metadata source ali
>> ALI user data obtained
>> Fos-instance-id: i-p0w3dr3bf9rck4jub4vb
>> Cloudinit trying to get config script from https://*****.ap-southeast-2-
internal.fc.aliyuncs.com/2016-08-15/proxy/FortigateAutoScale-wke/FortigateAutoScale-rrr/
>> Cloudinit download config script successfully
>> Found metadata source: ali
>> Run config script
>> Finish running script
>> FortiGate-VM64-ALI $ config system dns
>> FortiGate-VM64-ALI (dns) $ unset primary
>> FortiGate-VM64-ALI (dns) $ unset secondary
>> FortiGate-VM64-ALI (dns) $ end
>> FortiGate-VM64-ALI $ config system auto-scale
>> FortiGate-VM64-ALI (auto-scale) $ set status enable
>> FortiGate-VM64-ALI (auto-scale) $ set sync-interface port 1
>> FortiGate-VM64-ALI (auto-scale) $ set role master
>> FortiGate-VM64-ALI (auto-scale) $ set callback-url
https://*****.ap-southeast-2-internal.fc.aliyuncs.com/2016-08-
15/proxy/FortigateAutoScale-wke/FortigateAutoScale-rrr/
```

TableStore删除时长

删除TableStore最多可能需要 10 分钟，可能显示如下内容：

```
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m0s elapsed)
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m10s elapsed)
alicloud_ots_instance.tablestore: Still destroying... (ID: FortiGateASG-rrr, 7m20s elapsed)
```

如果 10 分钟后仍显示该消息，则可能是TableStore中包含数据。您需手动删除TableStore，然后重新运行`terraformd destroy`命令。有关手动删除TableStore的详细内容，请参见第65页删除集群。

资源可用性

如果某个区域指定资源已用尽，则会显示如下错误消息。若出现此类情况，需将群集另外部署至其他区域。

```
1 error occurred:
  * alicloud_slb.default: 1 error occurred:
    * alicloud_slb.default: [ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_
slb.go:324: Resource alicloud_slb CreateLoadBalancer Failed!!! [SDK alibaba-cloud-sdk-go
ERROR]:
SDK.ServerError
ErrorCode: OperationFailed.ZoneResourceLimit
Recommend:
RequestId: 83972A94-0640-49DA-8586-DCF535D14886
Message: The operation failed because of resource limit of the specified zone.
```

超时

如出现如下所示的超时错误提示，请重新运行该命令。

```
Error: Error applying plan:

1 error occurred:
  * alicloud_vswitch.vsw2: 1 error occurred:
    * alicloud_vswitch.vsw2: [ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_
vswitch.go:58:
[ERROR] terraform-provider-alicloud/alicloud/resource_alicloud_vswitch.go:170:
[ERROR] terraform-provider-alicloud/alicloud/service_alicloud_ecs.go:51: Resource us-east-1b
DescribeZones Failed!!! [SDK alibaba-cloud-sdk-go ERROR]:
net/http: request canceled (Client.Timeout exceeded while reading body)
```

如何重置选定的主 FortiGate

重置选定的主 FortiGate，请进入 *TableStore >FortiGateMasterElection* 并删除唯一项目，将选择一个新的主FortiGate，并创建一条新记录。

有关如何进入*TableStore >FortiGateMasterElection*的详细信息，请参阅第63页验证部署。

附录

阿里云FortiGate 弹性伸缩功能

主要组件

- 弹性伸缩组。Auto Scaling (弹性伸缩) 组包含1至多个 FortiGate-VM (PAYG 许可模型)。该组将根据伸缩规则中的具体伸缩指标进行动态扩容或缩容。
- Configset (配置集) 文件夹包含作为新 FortiGate-VM 实例初始配置加载的文件。
 - baseconfig 为基本配置文件，可按需修改此文件以满足您的网络要求。有关 {SYNC_INTERFACE} 等占位符的详细说明，请参阅第 68 页配置集占位符表。
- TableStore 中的表格。这些表将存储健康状况检查监控、主备选择、状态切换等信息。除非需进行故障排除，否则不应修改这些记录。

配置集占位符

当 FortiGate-VM 为支持弹性伸缩功能请求相关配置时，表中的占位符将替换为存储在函数计算中的关联环境变量。

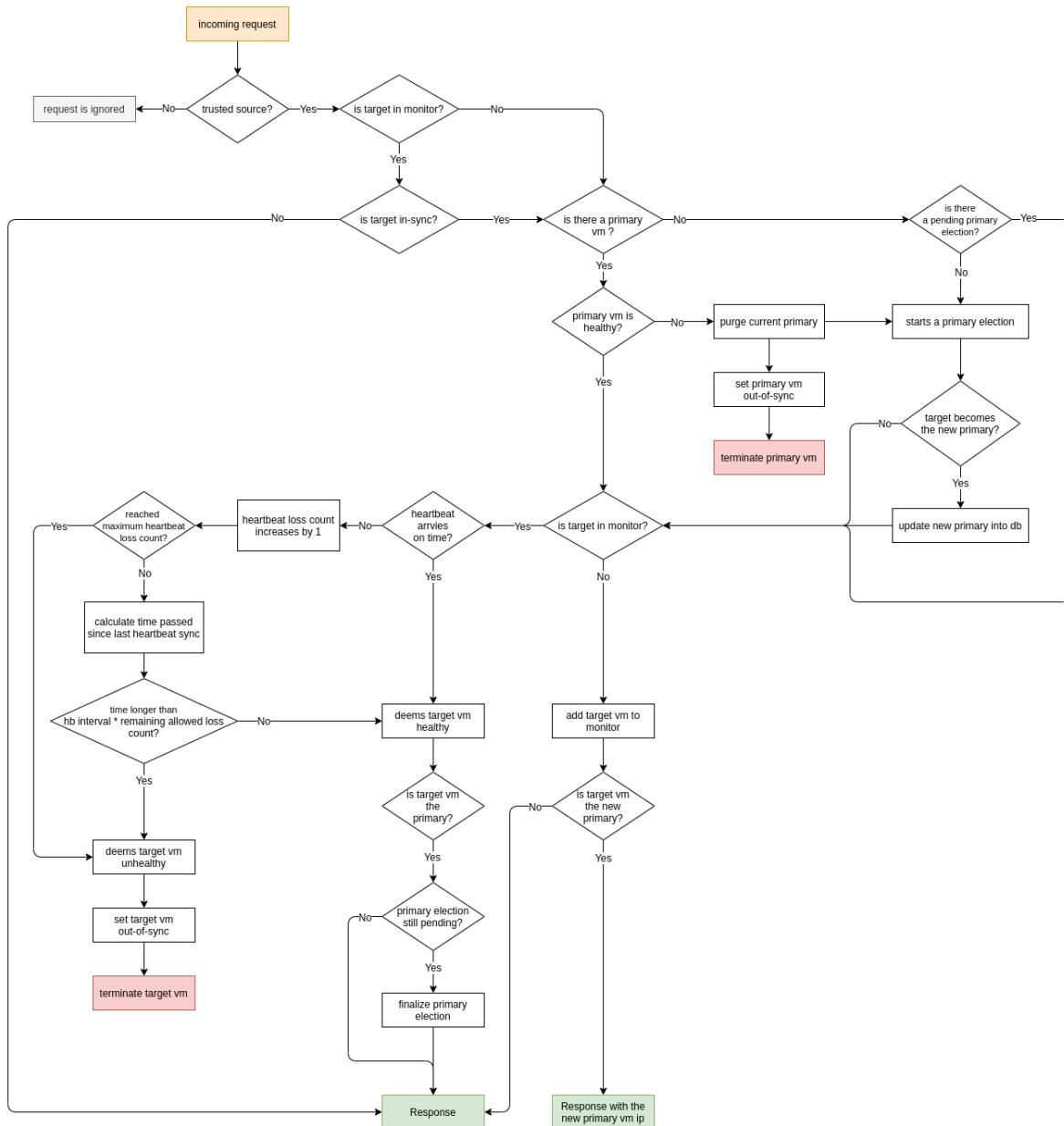
占位符	类型	描述
{SYNC_INTERFACE}	文本	FortiGate-VM 同步信息的接口。 所有字符必须为小写。
{CALLBACK_URL}	URL	与弹性伸缩处理程序脚本交互的终端 URL。 在 Terraform 部署期间自动生成。
{PSK_SECRET}	文本	FortiOS 中使用的预共享密钥。 在 Terraform 部署期间随机生成。
<hr/>		
 部署 FortiGate Autoscale for AliCloud 后，针对 PSK 密钥所做的更改不在此显示。对于使用已更改 PSK 密钥生成的新实例，必须手动更新此环境变量。		
<hr/>		
{ADMIN_PORT}	数字	管理员登录指定端口号。 正整数，如 443 等。 默认值：8443。
 部署后对管理员端口的更改不在此处显示。对于使用已更改管理员端口生成的新实例，必须更新此环境变量。		

架构图

主实例的选择

FortiGate Autoscale

with heartbeat response & failover management



在阿里云上手动部署弹性伸缩

以下是在阿里云上部署弹性伸缩配置示例的操作步骤：

-
1. 在阿里云控制台创建伸缩组。
 2. 在阿里云控制台创建伸缩配置。
 3. 在阿里云控制台创建伸缩规则。
 4. 将弹性伸缩组中的1个 FortiGate-VM 配置为主成员。
 5. 横向扩展1个新的 FortiGate-VM，并将其配置为备用成员，按照主FortiGate-VM配置同步备用 FortiGate-VM 配置。
 6. 运行诊断命令，确认弹性伸缩是否正常运行。

如需在阿里云控制台创建伸缩组，请执行以下操作：

1. 登录阿里云控制台。
2. 进入*Auto Scaling > Scaling Groups > Create Scaling Group* (弹性伸缩>伸缩组>创建伸缩组)。
3. 为弹性伸缩组设置以下参数：
 - a. *Scaling Group Name* (伸缩组名称)：输入伸缩组名称。本配置示例中为：*FGT-ASG*。
 - b. *Maximum Instances* (最大实例数)：输入可组成组的最大实例数。在本配置示例中，四 (4) 为最大数值。
 - c. *Minimum Instances* (最小实例数)：输入可组成组的最小实例数。在本配置示例中，一 (1) 为最小数值。
 - d. *Instance Configuration Source* (实例配置源)：保留默认值。
 - e. *Network Type* (网络类型)：保留默认值，即 VPC。
 - f. 按需选择VPC和虚拟交换机。

Create Scaling Group

*Scaling Group Name: FGT-ASG
The name can be 2 to 40 characters in length. It must start with a letter, number or Chinese character. It can also contain periods (.), underscores (_), and hyphens (-).

*Maximum Instances (): 4
Valid range: 0 to 1000

*Minimum Instances (): 1
Valid range: 0 to 1000

*Default Cooldown Time (Seconds) (): 300
The value must be an integer no less than 0.

Removal Policy (): First Pick Earliest Instance Created Using : Then Pick Earliest Created Instance To Remove
[How can I ensure that a manually added ECS instance will not be removed from the scaling group?](#)

* Instance Configuration Source (): Custom Scaling Configuration Launch Template

* Network Type: VPC VPC (A scaling group can support multiple VSswitches.)
 * VPC: VPC ID: vpc-rj9kk7ico621z27p1fv4y [Create VPC network](#)
 VSswitch: fgtvswitch (US West 1 Zone A)
 sw2 (US West 1 Zone A)

Multi-Zone Scaling Policy (): Priority Distribution Balancing Cost Optimization

Reclaim Mode (): Release Mode Shutdown and Reclaim Mode

SLB Instances (): -- Select an SLB instance -- [Manage SLB instances](#)

Only SLB instances that have been configured with listeners can be used by scaling groups.

RDS Instances (): -- Select an RDS instance -- [Manage RDS databases](#)

Databases in the scaling group: configured=0, maximum=10

OK **Cancel**

4. 单击 **OK** (确定)。

如需在阿里云控制台创建伸缩配置，请执行以下操作：

1. 创建弹性伸缩组后，在激活弹性伸缩服务前，阿里云将弹出一个窗口，用于创建新的伸缩配置。请在弹出窗口中，单击 *Create Now* (立即创建)。
2. 选择实例类型。
3. 选择所需的 FortiGate-VM 镜像。
4. 确保已选定 *Assign Public IP* (分配公网 IP 地址)。
5. 选择所需的安全组。

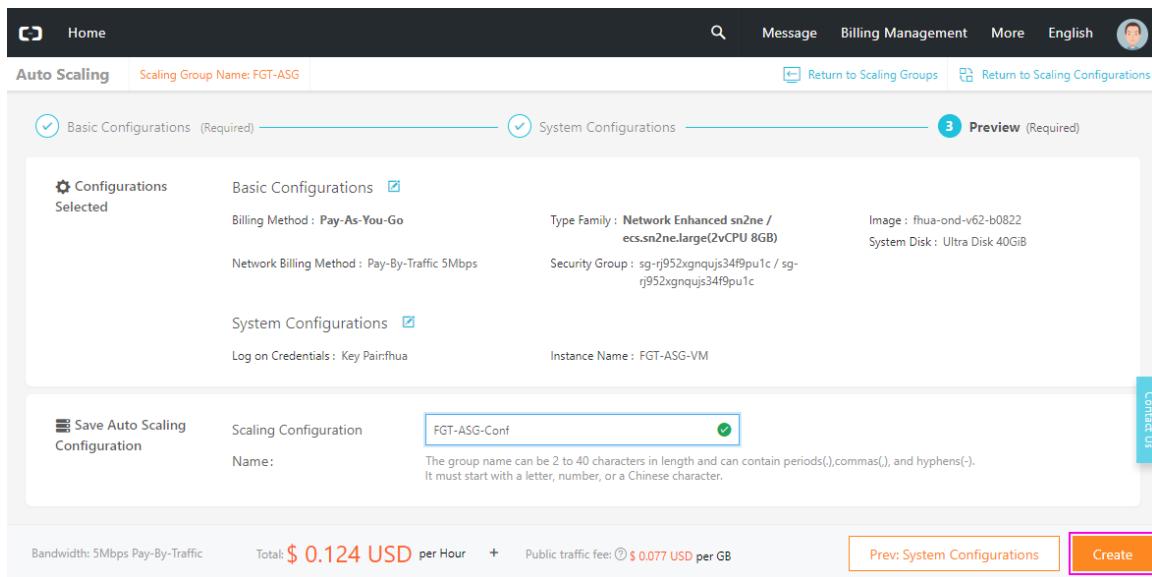
6. 单击 *Next: System Configurations* (下一步：系统配置)。

The screenshot shows the 'Basic Configurations' step of the Auto Scaling wizard. The instance type selected is 'ecs.sn2ne.large'. The 'Next: System Configurations' button is highlighted with a red box.

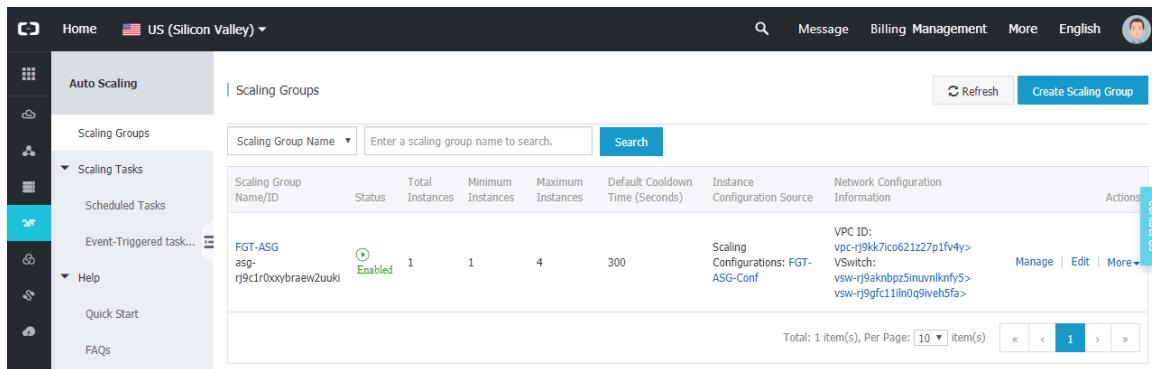
7. (可选) 设置密钥对。

The screenshot shows the 'System Configurations' step of the Auto Scaling wizard. A key pair 'fhua' is selected. The 'Next: Preview' button is highlighted with a red box.

8. 预览伸缩配置，然后点击 *Create and Enable Configuration* (创建和启用配置)



9. 进入 *Auto Scaling > Scaling Groups* (弹性伸缩>伸缩组)，确保阿里云已创建弹性伸缩组，且该组下的第一个 FortiGate-VM 已自动启动。



如需在阿里云控制台创建伸缩规则，请执行以下操作：

1. 在 *Auto Scaling > Scaling Groups* (弹性伸缩>伸缩组) 中，单击伸缩组名称。
2. 单击右侧菜单中的 *Scaling Rules* (伸缩规则)。
3. 在 *Create Scaling Rule* (创建伸缩规则) 对话框中，输入伸缩规则名称。
4. 配置操作。在本配置示例中，伸缩规则配置为添加一 (1) 个FortiGate- VM 实例。
5. 输入冷却时间，然后单击 *Create Scaling Rule* (创建伸缩规则)。您还可配置另一个伸缩规则，通过该规则执行删除一 (1) 个 FortiGate-VM 实例的操作。

The screenshot shows the 'Create Scaling Rule' dialog box. The 'Name' field is set to 'FGT-ASG-ADD1'. The 'Action' dropdown is set to 'Add' with a value of '1'. The 'Cooldown Time (Seconds)' field is set to '300'. At the bottom, there are 'Create Scaling Rule' and 'Cancel' buttons.

如需将弹性伸缩组中的 FortiGate-VM 配置为主成员，请执行以下操作：

1. 登录至 FortiGate-VM。
2. 在 CLI 中运行以下命令以启用弹性伸缩功能，并将此 FortiGate-VM 配置为弹性伸缩组的主成员：

```
config system auto-scale
    set status enable
    set role master
    set sync-interface
    "port1" set psksecret
    xxxxxxxx
end
```

横向扩展1个新的 FortiGate-VM，将其配置为备用成员并同步主成员配置，请执行以下操作：

1. 在 *Auto Scaling > Scaling Groups* (弹性伸缩>伸缩组) 中，单击伸缩组名称并执行之前已创建的伸缩规则。在阿里云上创建一个新的FortiGate-VM实例。
2. 登录至新的 FortiGate-VM 实例。
3. 在 CLI 中运行以下命令以启用弹性伸缩功能，并将此 FortiGate-VM 配置为弹性伸缩组的备用成员。`master-ip` 应为主 FortiGate-VM 的专用 IP 地址：

```
config system auto-scale
    set status enable
    set role slave
    set sync-interface
    "port1" set master-ip
    192.168.1.204 set
    psksecret xxxxxxxx
end
```

将备用 FortiGate-VM 配置与主 FortiGate-VM 配置进行同步。备用 FortiGate-VM 可从主 FortiGate-VM 接收配置。

如需运行诊断命令，请执行以下操作：

您可运行以下诊断命令，以确定主备 FortiGate-VM 是否完成配置同步：

```
FortiGate-VM64-ALION~AND # diag deb app hasync -1
```

```
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
```

SDN 连接器与阿里云集成

使用 RAM 角色配置阿里云 SDN 连接器

有关阿里云 SDN 连接器的详细信息，请参阅 [《FortiOS 管理指南》](#)。

以下为SDN连接器与阿里云集成所需的RAM角色最低管理权限：

- AliyunECSReadOnlyAccess
- AliyunEIPReadOnlyAccess
- AliyunVPCReadOnlyAccess



实际角色配置可能因环境而异。更多详情，请咨询贵公司的公有云管理员。

使用阿里云函数计算实现流水线自动化

请参阅[GitHub](#)。

适用于阿里云FortiGate-VM 的VPN

将本地 FortiGate 连接至阿里云 VPC VPN

本指南提供了通过支持静态路由的 IPsec VPN，从本地 FortiGate 至阿里云 VPC VPN 创建站点到站点 VPN 连接的配置示例。

您在阿里云 VPC 中启动的实例，可通过本地 FortiGate 和阿里云 VPC VPN 之间的站点至站点 VPN，与您的远程网络进行通信。您可通过配置连接至VPC的VPN网关和客户网关，然后配置站点至站点 VPC VPN 连接，从 VPC 访问远程网络。

此配置要求满足以下先决条件：

- 已创建阿里云VPC并完成子网、路由表、安全组规则等相关配置
- 已将本地 FortiGate与外网 IP 地址绑定

本指南包括以下步骤：

- 创建 VPN 网关。
- 创建客户网关。
- 在阿里云上创建站点至站点 VPN 连接。
- 配置本地 FortiGate。
- 运行诊断命令。

如需创建 VPN 网关，请执行以下操作：

- 登录阿里云管理控制台，进入VPN >VPN Gateway (VPN >VPN网关)。
- 单击Create VPN Gateway (创建 VPN 网关)。
- 创建虚拟专用网关，并将其绑定至需创建站点至站点 VPN 连接的 VPC。

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Gateway Status	Concurrent SSL Connections	Description	Actions
vpn-rj94kb7n3aqed9wdl1ns my-ali-vpn-gw	47.88.4.89		vpc-rj9h5m14eo5u97h japtw fhua-vpc-ha	Normal	10Mbps	Upgrade	Billing by Traffic Usage 06/04/2019, 11:31:15 Created	IPsec: Enabled SSL: Enable SSL		

如需创建客户网关，请执行以下操作：

此示例是以VPC VPN连接的本地 FortiGate作为客户网关。

1. 点击进入 *VPN > Customer Gateways* (*VPN > 客户网关*)。
2. 单击 *Create Customer Gateway* (*创建客户网关*)。
3. 配置客户网关，如下图所示：

Instance ID/Name	IP Address	Description	Created At	Actions
cgw-rj9xvkm2z21vz19sex0t5 my-all-customer-gw	208.91.114.1	-	06/04/2019, 11:36:32	Delete

如需在阿里云上创建站点至站点 VPN 连接，请执行以下操作：

1. 点击进入 *VPN > IPsec Connections* (*VPN > IPsec 连接*)。
2. 单击 *Create IPsec Connection* (*创建 IPsec 连接*)。
3. 在 VPN 和客户网关之间创建 IPsec 连接。
4. 在 *Actions* (*操作*) 菜单下，单击 *Download Configuration* (*下载配置*)。

Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status	Health Check Status	Created At	Actions
vco-j912mnz0h688wsqtlrvk my-all-ipsec-conn...	vpn-rj94kb7n3aqed9wd1sns my-all-vpn-gw	cgw-rj9xvkm2z21vz19sex0t5 my-all-customer-gw	Phase 2 of IKE Tunnel Negotiation Succeeded	-	06/04/2019, 11:38:36	Edit Delete Download Configuration View Logs

5. 记录与 IPsec 相关的参数。在下一步骤中，您可使用该参数配置本地 FortiGate：

```
{
    "LocalSubnet": "0.0.0.0/0",
    "RemoteSubnet": "0.0.0.0/0",
    "IpsecConfig": {
        "IpsecPfs": "group2",
        "IpsecEncAlg": "aes",
        "IpsecAuthAlg": "sha1",
        "IpsecLifetime": 86400
    },
    "Local": "x.x.x.x",
    "Remote": "47.88.4.89",
    "IkeConfig": {
        "IkeAuthAlg": "sha1",
        "LocalId": "x.x.x.x",
        "IkeEncAlg": "aes",
        "IkeVersion": "ikev1",
        "IkeMode": "main",
        "IkeLifetime": 86400,
        "RemoteId": "47.88.4.89",
        "Psk": "xxxxxxxxxxxxxxxxxxxx",
        "IkePfs": "group2"
}
```

```
    }  
}
```

如需配置本地 FortiGate，请执行以下操作：

1. 在 FortiOS CLI 中，使用所记录的 IPsec 相关参数配置本地 FortiGate。设置 remote-gw 和 psksecret 时，请分别使用上文Remoteld 和 Psk 命令中的值。该示例中，本地FortiGate使用port9作为其外部接口：

```
config vpn ipsec phase1-interface  
    edit "AliCloudVPN"  
        set interface "port9"  
        set keylife 86400  
        set peertype any  
        set net-device enable  
        set proposal aes128-sha1  
        set dhgrp 14 2  
        set remote-gw 47.88.4.89  
        set psksecret xxxxxxxxxxxxxxxx  
    next  
end  
config vpn ipsec phase2-interface  
    edit "AliCloudVPN"  
        set phase1name "AliCloudVPN"  
        set proposal aes128-sha1  
        set dhgrp 14 2  
        set keepalive enable  
        set keylifeseconds 3600  
    next  
end  
config firewall address  
    edit "AliCloudVPN-local-subnet-1"  
        set allow-routing enable  
        set subnet 10.6.30.0 255.255.255.0  
    next  
end  
config firewall address  
    edit "AliCloudVPN-remote-subnet-1"  
        set allow-routing enable  
        set subnet 10.0.1.0 255.255.255.0  
    next  
end  
config router static  
    edit 2  
        set device "AliCloudVPN"  
        set dstaddr "AliCloudVPN-remote-subnet-1"  
    next  
end  
config firewall policy  
    edit 10
```

```
        set name "AliCloudVPN-local-ali"
        set srcintf "mgmt1"
        set dstintf "AliCloudVPN"
        set srcaddr "AliCloudVPN-local-subnet-1"
        set dstaddr "AliCloudVPN-remote-subnet-1"
        set action accept
        set schedule "always"
        set service "ALL"

    next
edit 20
    set name "AliCloudVPN-ali-local"
    set srcintf "AliCloudVPN"
    set dstintf "mgmt1"
    set srcaddr "AliCloudVPN-remote-subnet-1"
    set dstaddr "AliCloudVPN-local-subnet-1"
    set action accept
    set schedule "always"
    set service "ALL"

next
end
```

2. 如果IPsec隧道未自动连接，请运行诊断命令：diagnose vpn tunnel up AliCloudVPN。
3. 登录FortiOS GUI，点击进入 *VPN > IPsec Tunnels* (*VPN > IPsec 隧道*)。验证隧道是否已成功创建。现在，本地 FortiGate 可使用其专用IP地址访问AliCloud VM。阿里云虚拟机还可通过其专用IP地址访问本地FortiGate。

运行诊断命令：

```
FGT600D_B # diagnose vpn ike gateway list
vd: root/0
name: AliCloudVPN
version: 1
interface: port9 10
addr: 172.16.200.212:4500 -> 47.88.4.89:4500
created: 1087s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 9110/9110/9110 ms
IPsec SA: created 1/2 established 1/1 time 30/30/30 ms

id/spi: 0 d9d4ae9111a51b0b/de39f4ac9deffc18
direction: initiator
status: established 1087-1078s ago = 9110ms
proposal: aes128-sha1
key: 9bf9b58431949e77-a0c21ded48368db1
lifetime/rekey: 28800/27421
DPD sent/recv: 00000000/00000000

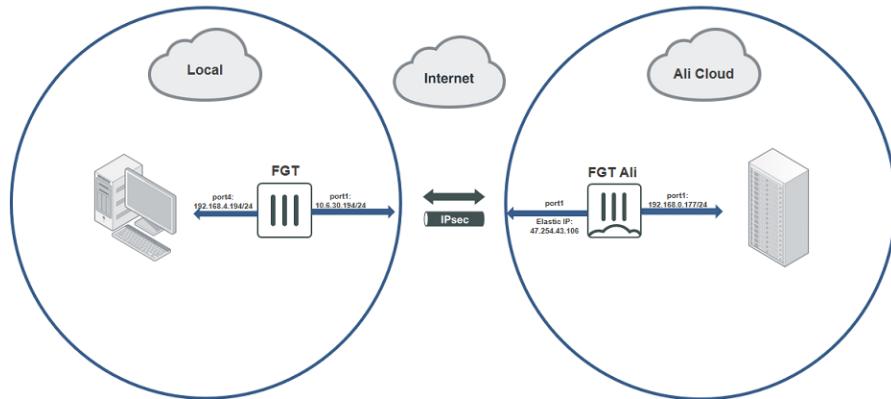
FGT600D_B # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=AliCloudVPN ver=1 serial=1 172.16.200.212:4500->47.88.4.89:4500 dst_mtu=1500
bound_if=10 lgwy=static/1 tun=intf/0 mode=auto/1 encapsulation=none/536 options[0218]=npu create_dev
```

```
frag-rfc accept traffic=1

proxyid_num=1 child_num=0 refcnt=14 ilast=1084 olast=270 ad=/0
stat: rxp=1 txp=43 rxb=16452 txb=4389
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=AliCloudVPN proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=10227 type=0 soft=0 mtu=1422 expire=2399/0B replaywin=2048
    seqno=2c esn=0 replaywin_lastseq=00000001 itn=0 qat=0
life: type=01 bytes=0/0 timeout=3298/3600
dec: spi=ac5426a9 esp=aes key=16 417b83810bf1f17b30e8b0974716d37d
    ah=sha1 key=20 a3e1d5ca5d85907a35c7720e9c640d0fafbb0ee3
enc: spi=c999e156 esp=aes key=16 837b20f727c957f700f6c89acbb9e9a9
    ah=sha1 key=20 7f4634601d6962575c00761f7270d36a683c3d65
dec:pkts/bytes=1/16376, enc:pkts/bytes=43/7648
npu_flag=03 npu_rgwy=47.88.4.89 npu_lgwy=172.16.200.212 npu_selid=0 dec_npuid=1 enc_
npuid=1
```

通过站点至站点 VPN 将本地 FortiGate 连接至阿里云 FortiGate

本指南提供了通过支持静态路由的站点至站点 IPsec VPN，从本地 FortiGate 至阿里云 FortiGate 创建站点至站点 VPN 连接的配置示例。下图为该部署示例的网络拓扑：



此配置必须满足以下先决条件：

- 位于阿里云上的FortiGateport1已连接至本地局域网，公网IP地址已映射至port1。
- 本地环境中已配置1个本地FortiGate。确定您的 FortiGate 是否拥有可公开访问的 IP 地址，或其是否隐藏于 NAT 背后。在此示例中，本地 FortiGate 隐藏于 NAT 背后。

本指南包括以下步骤：

- 配置本地 FortiGate。
- 配置阿里云 FortiGate。
- 在本地和阿里云 FortiGates 之间创建 VPN 连接。
- 运行诊断命令。

配置本地 FortiGate

如需使用 GUI 配置本地 FortiGate，请执行以下操作：

1. 配置接口：
 - a. 在 FortiOS 中，点击进入 *Network > Interfaces* (网络>接口)。
 - b. 编辑 port1。从 *Role* (角色) 下拉列表中，选择“WAN”。在 *IP/Network Mask* (IP/网络掩码) 字段中，为连接至互联网的接口输入：10.6.30.194/255.255.255.0。
 - c. 编辑 port4。从 *Role* (角色) 下拉列表中，选择“LAN”。在 *IP/Network Mask* (IP/网络掩码) 字段中，为连接至本地子网的接口输入：192.168.4.194/255.255.255.0。
2. 配置静态路由以连接至互联网：
 - a. 点击进入 *Network > Static Routes* (网络>静态路由)。
 - b. 单击 *Create New* (新建)。
 - c. 在 *Destination* (目的地) 字段中，输入：0.0.0.0/0.0.0.0。
 - d. 从 *Interface* (接口) 下拉列表中，选择 port1。
 - e. 在 *Gateway Address* (网关地址) 字段中，输入：10.6.30.254。
3. 配置 IPsec VPN：
 - a. 点击进入 *VPN > IPsec Wizard* (VPN > IPsec 向导。)
 - b. 配置 VPN 设置：
 - i. 在 *Name* (名称) 字段中，输入所需名称。
 - ii. *Template Type* (模板类型)，请选择 *Site to Site* (站点至站点)。
 - iii. *NAT Configuration* (远程设备类型)，请选择“FortiGate”。
 - iv. *NAT Configuration (NAT 配置)*，请选择 *This site is behind NAT* (此站点隐藏于 NAT 背后)。单击 *Next* (下一步)。针对本地 FortiGate 具有外网 IP 地址的非拨号情况，请选择 *No NAT between sites* (站点之间无 NAT)。
 - c. 配置 *Authentication* (身份验证)：
 - i. *Remote Device* (远程设备)，请选择 *IP Address* (IP 地址)。
 - ii. 在 *IP Address* (IP 地址) 字段中，输入 47.254.43.106，此为阿里云 FortiGate 接 port1 的公网 IP 地址。
 - iii. 从 *Outgoing Interface* (出站接口) 下拉列表中，选择 port1。
 - iv. *Authentication Method* (身份验证方法)，请选择 *Pre-shared Key* (预共享密钥)。
 - v. 在 *Pre-shared Key* (预共享密钥) 字段中，输入 123456。单击 *Next* (下一步)。
 - d. 配置 *Policy & Routing* (策略和路由)：
 - i. 从 *Local Interface* (本地接口) 下拉列表中，选择 port4，以使用 192.168.4.0/24 自动填充 *Local Subnets* (本地子网) 字段。
 - ii. 在 *Remote Subnets* (远程子网) 字段中，输入 192.168.4.0/24，此为阿里云 FortiGate port1 子网。
 - iii. *Internet Access* (互联网访问)，请选择 *None* (无)。单击 *Create* (创建)。

使用 CLI 配置本地 FortiGate，请执行以下操作：

1. 配置接口：

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.6.30.194 255.255.255.0
    set allowaccess ping https ssh http fgfm
    set type physical
    set role wan
```

```
    set snmp-index 1
next
edit "port4"
    set vdom "root"
    set ip 192.168.4.194 255.255.255.0
    set allowaccess ping https ssh snmp fgfm ftm
    set type physical
    set device-identification enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
next
end
```

2. 配置连接至互联网的静态路由：

```
config router static
    edit 1
        set gateway 10.6.30.254
        set device "port1"
    next
end
```

3. 配置 IPsec VPN：

```
config vpn ipsec phasel-interface
    edit "to_ali"
        set interface "port1"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: to_ali (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 47.254.43.106
        set psksecret xxxxxxx
    next
end
config vpn ipsec phase2-interface
    edit "to_ali"
        set phasename "to_ali"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set comments "VPN: to_ali (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to_ali_local"
        set dst-name "to_ali_remote"
    next
end
config router static
    edit 2
```

```

    set device "to_ali"
    set comment "VPN: to_ali (Created by VPN wizard)"
    set dstaddr "to_ali_remote"
next
edit 3
    set distance 254
    set comment "VPN: to_ali (Created by VPN wizard)"
    set blackhole enable
    set dstaddr "to_ali_remote"
next
end
config firewall policy
edit 1
    set name "vpn_to_ali_local"
    set uuid c6b2d36e-6c65-51e9-5a78-9a0881a0b07c
    set srcintf "port4"
    set dstintf "to_ali"
    set srcaddr "to_ali_local"
    set dstaddr "to_ali_remote"
    set action accept
    set schedule "always"
    set service "ALL"
    set comments "VPN: to_ali (Created by VPN wizard)"
next
edit 2
    set name "vpn_to_ali_remote"
    set uuid c6bf126e-6c65-51e9-8652-cb88546929b4
    set srcintf "to_ali"
    set dstintf "port4"
    set srcaddr "to_ali_remote"
    set dstaddr "to_ali_local"
    set action accept
    set schedule "always"
    set service "ALL"
    set comments "VPN: to_ali (Created by VPN wizard)"
next
end

```

配置阿里云 FortiGate

如需使用 GUI 配置 AliCloud FortiGate，请执行以下操作：

1. 配置接口：
 - a. 在 FortiOS 中，点击进入 *Network > Interfaces*（网络>接口）。
 - b. 编辑 port1。
 - c. 从 *Role*（角色）下拉列表中，选择“*LAN*”。
 - d. 确保 *Addressing mode*（寻址模式）设置为 DHCP，且 FortiGate 可列出已分配的 IP 地址。

2. 配置 IPsec VPN:

- a. 点击进入 *VPN >IPsec Wizard (VPN >IPsec 向导)*。
- b. 配置 VPN 设置:
 - i. 在 *Name (名称)* 字段中，输入所需名称。
 - ii. *Template Type (模板类型)*，请选择“*站点至站点 (Site to Site)*”。
 - iii. *Remote Device Type (远程设备类型)*，请选择“*FortiGate*”。
 - iv. *NAT Configuration (NAT配置)*，请选择 *The remote site is behind NAT (远程站点位于 NAT 之后)*。单击 *Next (下一步)*。
- c. 配置 *Authentication (身份验证)* 策略:
 - i. 从 *Incoming Interface (入站接口)* 下拉列表中，选择 *port1*。
 - ii. *Authentication Method (身份验证方法)*，请选择 *Pre-shared Key (预共享密钥)*。
 - iii. 在 *Pre-shared Key (预共享密钥)* 字段中，输入 123456。单击 *Next (下一步)*。
- d. 配置 *Policy & Routing (策略和路由)*:
 - i. 从 *Local Interface (本地接口)* 下拉列表中，选择 *port1*，以使用 192.168.4.0/24 自动填充 *Local Subnets (本地子网)* 字段。
 - ii. 在 *Remote Subnets (远程子网)* 字段中，输入 192.168.4.0/24，此为本地 FortiGate port4 子网。
 - iii. “*Internet Access (互联网访问)*”，请选择 *None (无)*。单击 *Create (创建)*。

如需使用 CLI 配置阿里云 FortiGate，请执行以下操作：

1. 配置接口并确保 FortiGate 可列出已分配的 IP 地址：

```
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
        set type physical
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 1
    next
end

diagnose ip address list
IP=192.168.0.177->192.168.0.177/255.255.255.0 index=3 devname=port1
```

2. 配置 IPsec VPN:

```
config vpn ipsec phase1-interface
    edit "to_local"
        set type dynamic
        set interface "port1"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set comments "VPN: to_local (Created by VPN wizard)"
        set wizard-type dialup-fortigate
        set psksecret xxxxxxx
```

```
set dpd-retryinterval 60
next
end
config vpn ipsec phase2-interface
    edit "to_local"
        set phase1name "to_local"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set comments "VPN: to_local (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to_local_local"
        set dst-name "to_local_remote"
    next
end
config firewall policy
    edit 1
        set name "vpn_to_local_local"
        set uuid e07aaa72-833c-51e9-ad33-4c1e96b656da
        set srcintf "port1"
        set dstintf "to_local"
        set srcaddr "to_local_local"
        set dstaddr "to_local_remote"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_local (Created by VPN wizard)"
    next
    edit 2
        set name "vpn_to_local_remote"
        set uuid e086b2b8-833c-51e9-3aaf-49e3cd4c5c70
        set srcintf "to_local"
        set dstintf "port1"
        set srcaddr "to_local_remote"
        set dstaddr "to_local_local"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "VPN: to_local (Created by VPN wizard)"
    next
end
```

如需在 FortiGates 之间创建VPN 连接，请执行以下操作：

隧道将关闭，直至您从本地 FortiGate 启动连接。

1. 在本地 FortiGate 上的 FortiOS 中，点击进入 *Monitor> IPsec Monitor* (*监控> IPsec 监控*) 。
2. 单击已创建的隧道。

3. 单击 Bring Up (启动)。隧道已启动。

<input type="button" value="Refresh"/> <input type="button" value="Reset Statistics"/> <input type="button" value="Bring Up"/> <input type="button" value="Bring Down"/> <input type="button" value="Locate on VPN Map"/>							
Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
<input checked="" type="radio"/> to_all	<input type="radio"/> Site to Site - FortiGate	47.254.43.106		94.46 kB	44.52 kB	to_all	<input checked="" type="radio"/> to_all

4. 在阿里云FortiOS上的FortiOS中，点击 Monitor>IPsec Monitor (监控>IPsec 监控)，验证隧道是否已启动。

<input type="button" value="Refresh"/> <input type="button" value="Reset Statistics"/> <input type="button" value="Bring Up"/> <input type="button" value="Bring Down"/> <input type="button" value="Locate on VPN Map"/>							
Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
<input checked="" type="radio"/> to_local_0	<input type="radio"/> Dialup - FortiGate	208.91.114.1		126.59 kB	59.34 kB	to_local	<input checked="" type="radio"/> to_local

运行诊断命令，请执行以下操作：

1. 以下消息显示本地 FortiGate VPN 的状态：

```
FGT-194-Level1 # diagnose vpn ike gateway list
vd: root/0
name: to_ali
version: 1
interface: port1 3
addr: 10.6.30.194:4500 -> 47.254.43.106:4500
created: 4057s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 21180/21180/21180 ms
IPsec SA: created 1/3 established 1/3 time 20/26/30 ms
  id/spi: 2 fd018d163ea303aa/9d7a245f889ee6c4
  direction: initiator
  status: established 4057-4036s ago = 21180ms
  proposal: aes128-sha256
  key: c7bab4dd8883b727-3b249220088216f8
  lifetime/rekey: 86400/82063
  DPD sent/recv: 00000000/00000000
FGT-194-Level1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=to_ali ver=1 serial=1 10.6.30.194:4500->47.254.43.106:4500 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options
[0210]=create_dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=/0
stat: rxp=3382 txp=3404 rxb=432896 txb=204240
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=to_ali proto=0 sa=1 ref=2 serial=3
  src: 0:192.168.4.0/255.255.255.0:0
  dst: 0:192.168.0.0/255.255.255.0:0
  SA: ref=3 options=10226 type=00 soft=0 mtu=1422 expire=39471/0B replaywin=2048
    seqno=d14 esn=0 replaywin_lastseq=00000d0d itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=8427ce41 esp=aes key=16 961323608ef02c111ce4cc393cd79293
    ah=sha1 key=20 9cffabaa0163df6a92e1917efa333148b58ff9da
  enc: spi=e2723047 esp=aes key=16 f93b233906039c179924923a4f09ebae
    ah=sha1 key=20 c2c6225e26927de6381bf44c6ccd6d0a325e2e27
```

dec:pkts/bytes=3325/199500, enc:pkts/bytes=3347/428416

2. 以下信息显示阿里云FortiGate VPN状态:

```
FGT-ALIONDEMAND # diagnose vpn ike gateway list
vd: root/0
name: to_local_0
version: 1
interface: port1 3
addr: 192.168.0.177:4500 -> 208.91.114.1:64916
created: 4103s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 120/120/120 ms
IPsec SA: created 1/3 established 1/3 time 20/26/30 ms
id/spi: 0 fd018d163ea303aa/9d7a245f889ee6c4
direction: responder
status: established 4103-4103s ago = 120ms
proposal: aes128-sha256
key: c7bab4dd8883b727-3b249220088216f8
lifetime/rekey: 86400/82026
DPD sent/recv: 00000009/00000000
FGT-ALIONDEMAND # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=to_local ver=1 serial=1 192.168.0.177:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/528 options
[0210]=create_dev frag-rfc accept_traffic=1
proxyid_num=0 child_num=1 refcnt=11 ilast=4118 olast=4118 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
-----
name=to_local_0 ver=1 serial=2 192.168.0.177:4500->208.91.114.1:64916 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/976 options
[03d0]=create_dev no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1
parent=to_local index=0
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=/0
stat: rxp=3459 txp=3459 rxb=442752 txb=207540
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=9
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=to_local proto=0 sa=1 ref=2 serial=3 add-route
src: 0:192.168.0.0/255.255.255.0:0
dst: 0:192.168.4.0/255.255.255.0:0
SA: ref=3 options=282 type=0 soft=0 mtu=1422 expire=39694/0B replaywin=2048
seqno=d4b esn=0 replaywin_lastseq=00000d52 itn=0 qat=0
life: type=01 bytes=0/0 timeout=43187/43200
dec: spi=e2723047 esp=aes key=16 f93b233906039c179924923a4f09ebae
ah=sha1 key=20 c2c6225e26927de6381bf44c6cccd6d0a325e2e27
enc: spi=8427ce41 esp=aes key=16 961323608ef02c111ce4cc393cd79293
ah=sha1 key=20 9cffabaa0163df6a92e1917efa333148b58ff9da
```

dec:pkts/bytes=3402/204120, enc:pkts/bytes=3402/435456

更新日志

日期	内容更新描述
2023-05-11	首次发布



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.