

天翼云 • 态势感知系统

用户使用指南

中国电信股份有限公司云计算分公司



目 录

1 产品介绍	4
1.1 产品定义	4
1.2 术语解释	4
1.3 产品功能	
1.4 产品优势	5
协同应急	
动态评估	
风险可视	
1.5 应用场景	
2 购买指南	7
2.1 规格	7
3 快速入门	9
3.1:虚拟网关配置	9
3.2 态势感知控制台登录及内网 IP 配置	
登录	
内网 IP 配置	
3.3 负产官埕	
3.3 负产官理	
3.3 负产官理 资产收集 资产列表	



资产概览	23
3.4 脆弱性检测	23
漏洞扫描	23
漏洞列表	24
漏洞概览	25
3.5 威胁检测	26
威胁概览	
威胁列表	
警告配置	27
3.6 国家能力中心	29
国家信誉库	
威胁情报	
3.7 控制台	
3.8 系统管理	
系统设置	
用户管理	
报表管理	
4 操作指南	45
4.1 申请双网卡弹性云主机	45
开通态势感知弹性云主机	
开通态势感知虚拟网关云主机	
	11



4.2 申请虚 IP	48
4.3 订购态势感知基础版/高级版	49
4.4 虚拟网关配置	50
4.5 网络配置	51
场景 A	51
场景 B	52
场景 C	53
场景 D	56
4.6 部署完毕	59
5 常见问题	60
Q:态势感知产品有哪些规格?	60
Q:为什么检测口没有流量?	60
Q:为什么威胁检测没有数据?	60
Q:为什么信誉库没有同步?	60





1.1 产品定义

态势感知为用户提供统一的威胁检测和风险处置平台。态势感知能够帮助用户检测云上资产 遭受到的各种典型安全风险,还原攻击历史,感知攻击现状,预测攻击态势,为用户提供强大的 事前、事中、事后安全管理能力。

态势感知系统通过资产管理、脆弱性评估、威胁检测等手段完成用户网络的安全检查、风险 评估、可视化呈现。同时,通过与国家应急响应中心(CNCERT)权威监测平台的威胁情报、知识 库对接,动态实时的完成应急协同、威胁情报接入、信息流转、防护规则更新等信息交换,做到 用户安全风险的快速发现和信息闭环。

1.2 术语解释

态势感知(Situation Awareness, SA): 是一种基于环境的、动态、整体地洞悉安全风险的 能力,是以安全大数据为基础,从全局视角提升对安全威胁的发现识别、理解分析、响应处置能 力的一种方式,最终是为了决策与行动。

网络资产:网络资产主要是计算机(或通讯)网络中使用的各种 IT 设备。主要包括主机、服务器、网络设备(路由、交换等)和安全设备(防火墙等)等。

风险评估(Risk Assessment): 是对网络资产所面临的威胁、存在的弱点、造成的影响, 以及三者综合作用所带来风险的可能性的评估。

1.3 产品功能

资产发现

通过主被动两种资产探测方式,实时精准的持续监控资产变化情况,可自动识别网络设备、 机、安全设备、操作系统、数据库、web应用等。

资产管理

资产组件信息、变化趋势、端口分布、归属、操作系统分布自动化统计。可根据 IP、操作系统、应用组件/服务、归属部门、硬件信息等进行资产高级检索,快速统计资产信息、根据资产特征排查安全隐患。

脆弱性检测

通过漏洞扫描完成资产脆弱性评估,漏洞库可覆盖当前网络环境中主流的操作系统、数据 库、web 中间件、网络设备漏洞,同时,对接国家应急响应中心安全监测平台的漏洞预警、安全 事件通报及漏洞检测规则,完成检测规则的更新,有效应对突发安全事件,支持以资产存在漏洞 及漏洞影响资产两个维展示脆弱性资产。

网络威胁检测

根据网络流量可识别丰富的网络应用层协议,通过协议分析、内容萃取等报告对应的异常事件。可检测勒索软件、恶意软件、信息泄露、C&C 通信、扫描探测、暴力破解、系统提权、web 攻击等网络威胁。同步国家应急响应中心下发的恶意 URL、域名等信誉数据,完成新型威胁及高级 持续威胁的检测。

高级版功能

权威情报数据

借助国内顶尖厂家共同分析的结果,快速构建威胁信誉库,将诸如僵尸木马活动、恶意代码 传播、恶意攻击行为、恶意站点数据等网络安全事件及信誉数据同步至本系统,形成联动能力。

权威安全预警

定时同步国家应急响应中心(CNCERT)的漏洞预警、威胁情报、安全资讯数据,及时明晰最 新安全信息。

攻击源警告

当系统检测到远端 IP 地址存在恶意入侵或者探测行为时,可以配置对应的 IP 进行警告,警告 页面的内容可以自定义,当此 IP 再次连接 WEB 服务时,对其推送警告界面,以做警示。

恶意网站告警

通过国家应急响应中心信誉库自动同步恶意网站数据,在用户访问恶意网站时,给予及时告 警,协助用户识别 WEB 威胁,同时运维管理员可自定义添加恶意网站。

1.4 产品优势

协同应急

对接国内最权威的网络安全监测平台,与国家应急响应中心(CNCERT)形成联动能力,及时 发现用户单位网络安全威胁

动态评估

按照资产、威胁、脆弱性多维度的风险评估标准,动态调整风险权重,发现和分析潜在的威胁和脆弱点,进行预防、控制和修复。

风险可视

实时呈现网络攻击态势、资产威胁、资产漏洞、安全态势评分,同步展示国家应急响应中心 发布的威胁预警、安全资讯。

1.5 应用场景

态势感知适用于安全需求较高、经常遭受个人或组织网络攻击的央企、政府、医疗、教育、金融 等大型企事业单位。

重点行业信息系统

能源、金融、交通、教育、医疗、市政、电信与互联网、政府部门等支撑关键业务的信息系统;

电子政务和门户

各级党政军门户网站,教育类网站,重大活动及会议保障,重点新闻网站等;

大型互联网平台

注册用户、订单额或交易额较大,一旦发生网络安全事故,产生较严重影响,如敏感信息泄露、基础数据泄露等;

生产业务类系统

政府机关面向公众服务的业务系统,或与医疗、安防、消防、应急指挥、生产调度、交通指 挥等相关的城市管理系统。



天翼 e Cloud

2 购买指南

2.1规格

态势感知产品根据提供的功能不同分为两个版本:基础版、高级版。

功能	基础版	高级版
安全可视化	\checkmark	\checkmark
资产发现	\checkmark	\checkmark
资产管理	\checkmark	\checkmark
脆弱性检测	\checkmark	\checkmark
网络威胁检测	\checkmark	\checkmark
国家情报数据		\checkmark
国家安全预警		\checkmark
攻击源警告		\checkmark
恶意网站警告		\checkmark

云主机规则参照下表,

弹性云主机	服务器配置	设备性能	扩展性	作用	备注
(Linux)					
一台双网卡弹	4核 CPU/32G 内	此配置可处理	提高硬件配	态势感知系	其中 eth0 网卡
性云主机	存/500G 硬盘	200M以下流量	置,可提高流	统,通过资	IP 同业务一个
			量处理性能	产、脆弱性、	网段, eth1
				威胁多维度动	(扩展网卡)
	4核 CPU/64G 内	此配置可处理		态评估风险可	是态势感知网
	存/2T 硬盘	800M以下流量		视化	段。态势感知
					网段和业务、
					负载均衡、云
					下一代防火墙
					不同网段
两台双网卡弹	2核 CPU/2G内	此配置可处理	不涉及	虚拟网关系	其中 eth0 网卡
性云主机	存/50G 硬盘	1000M 以下流量		统,将访问业	IP 同业务、防



		务的所有流量	火墙、负载均
		镜像给态势感	衡器同一网
		知系统分析	段,eth1(扩展
			网卡)同态势感
			知一个网段。
			两者网段不同

收费标准:根据版本、监控云主机台数、订购周期进行收费。

产品规格	标准价格(元/月/台)
基础版	330
高级版	4200

备注:针对一次性包年付费服务,1、2、3年包年标准价格按照85折计算。



3 快速入门

3.1: 虚拟网关配置

完成虚拟网关云主机创建。将申请的虚拟 IP 绑定在 2 个虚拟网关云主机的 eth0 网口上,并 将公网 IP 绑定在此虚拟 IP 上。

	虚拟私有云,v	pc-sldtest > s	subnet-1.0					
~	子网名称 网络ID IPv4子网ID IPv6子网ID 子网IPv4网段 子网IPv6网段	subnet-1. 206f6d76 bbd14cba 192.168.1 开启IPv	申请虚排 ^{当前子网}	以IP地址 subnet-1.0 ^{当前子网IPv4网段:19} 自动分配	92.168.1.0/24 手动分配		×	常 3.118.118.9,202.98.192.67 ,《 即创建 2.168.1.1
~	已用IP地址 申请虚拟IPt	虚拟IP 也址	_	确分	2 取消			虚拟IP地址 🔻
	由th ID++++			体化合わる単体サロ	470-00-0	四夕昭(四上)		43//2

通过天翼云远程连接访问,输入用户名/密码: sens/sens,进入配置界面:

Conne	cted (encrypted) to: 2d447970-2527-490a-8bde-b1fae91c3087 Before you exit,ensure that computer is locked.	Local Curs
SENS	CPE (version: 1.19.9.25)	
You a hi	Operate Menu can use the UP/DOWN arrow keys, the first letter of the choice as ot key, or the number keys 0–9 to choose an option.	
Plea	ase choose your option: (0–9)	
	Logout system 1 Show interface 2 Show CPE base information 3 Set controller ipaddr 4 Set device plugin code 5 Reboot system 6 Halt system 7 Restore the factory configuration 8 Login system 9 Cluster config a ↓ ↓	

按 "3" 选择 "set controller ipaddr" 并按 "回车", 然后在对话框内输入控制器地址(地址会 在购买后通过邮件方式发送至邮箱), 按 "回车" 输入, 按 "ESC" 取消。



天翼云 e Cloud

按 "4" 选择 "set device plugin code"并按 "回车", 然后在对话框内输入验证码(验证码会 在购买后通过邮件方式发送至邮箱), 按 "回车" 输入, 按 "ESC" 取消。

You can use the UP/DOWN arrow keys, the first letter of the choice as a hot key, or the number keys 0-9 to choose an option. Please choose your option: (0-9) 0 Logout system 1 show interface 2 show CPE base information 3 Set controller ipaddr 5 Rebot system 6 Hall system 7 Restore the factory configuration 8 Login system 9 Cluster config a • •	Set device plugin code Please input the device plugin code(need reboot) [HJDX3D_ (JDX3D_ (Concel)

按 "9"选择 "Cluster config"并按 "回车", 然后在对话框内输入 "设备名, VIP 地址, VRRPID "中间需要用","分开, 设备名两个虚拟网关要不同(可随意取)、VIP 是 2 个虚拟网关的 虚 IP、VRRPID (范围 1-255, 两个虚拟网关保持一致就行), 按 "回车"输入, 按 "ESC"取消。



按 "5" 选择 "Reboot system" 并按 "回车" 重启系统, 然后就可以配置另外一台虚拟网关, 配置过程一样, 唯一的区别是在配置 "9" "cluster config" 中的设备名要确定不能相同



SENS CPE (version: 1.19.9.25)
Operate Menu You can use the UP/DOWN arrow keys, the first letter of the choice as a hot key, or the number keys 0–9 to choose an option. Please choose your option: (0–9)
<pre>0 Logout system 1 Show interface 2 Show CPE base information 3 Set controller ipaddr 4 Set device plugin code Reboot system 6 Halt system 7 Restore the factory configuration 8 Login system 9 Cluster config a ↓ ↓</pre>

场景一:

虚拟网关做为 NAT 网关, 直接下挂业务服务器的场景, 网络配置:

如图将 VPC 的下一跳地址指向 2 个虚拟网关的虚拟 Ip 地址(VIP)

	控制中心 服务列表 ▼ 收藏 ▼		● 贵州
\bigcirc	虚拟私有云,vpc-sldtest		
网络控制台	名称 vpc-sldtest ID 7bd993f9-f5be-46cf-be0e-585a1a07d50f ごのへ数 3 へ	状态 VPC网i 企业面	正常 段 192.168.0.0/16 🖉
虚拟私有云			
访问控制	→ 子网 路由表 拓扑图 标签		
弹性公网IP和带宽	~ 自定义路由表		
NAT网关	添加路由信息 您还可以申请99个路由信息。		
弹性负载均衡	~ 目的地址	下一跳地址	操作
对等连接	0.0.0/0	192.168.1.100	修改
虚拟专用网络	对等连接路由表		
云专线			场内
弹性云服务器		1. MONGAIL	1941 F

场景二:

虚拟网关下挂负载均衡器,网络配置:

如图将 VPC 的下一跳地址指向 2 个虚拟网关的虚拟 Ip 地址(VIP)

	控制中心 服务列表 ▼ 收藏 ▼		● 贵州
\bigcirc	虚拟私有云 > vpc-sldtest		
网络控制台	名称 vpc-sldtest 🖌	状态	正常
总览	ID 7bd993f9-f5be-46cf-be0e-585a1a07d50f	VPC网段	192.168.0.0/16 🖋
虚拟私有云	子网个数 3个	企业项目	default
访问控制	→ 子网 路由表 拓扑图 标签		
弹性公网IP和带宽	→ 自定义路由表		
NAT网关	添加路由信息 您还可以申请99个路由信息。		
弹性负载均衡	Y 目的地址 下一	跳地址	操作
对等连接	0.0.0.0/0 192.	.168.1.100	修改
虚拟专用网络	对等连接路由表		
云专线	- 目的地址 下一	跳地址	操作
弹性云服务器	0		DRIT

场景三:

翼口 Cloud

虚拟网关下挂防火墙 , 外部访问业务服务器的流量经过防火墙, 业务服务器主动访问外部流量不 经过防火墙网络配置:

如图将 VPC 的下一跳地址指向 2 个虚拟网关的虚拟 Ip 地址(VIP)

天翼云・	控	制中心 服务列表 ◆ 收藏 ◆			。 贵 州	
Ś		虚拟私有云 > vpc-sldtest				
网络控制台		名称 vpc-sldtest D 7bd993f9-f5be-46cf-be0e-585a1a07d50f		状态 VPC网段	正常 192.168.0.0/16	1
虚拟私有云		-1.67 3.1.		TETEME	delauit	
访问控制	~	子网 路由表 拓扑图 标签				
弹性公网IP和带宽	\sim	自定义路由表				
NAT网关		添加路由信息 您还可以申请99个路由信息。				
弹性负载均衡	~	目的地址	下一跳地址			操作
对等连接		0.0.0/0	192.168.1.100			修改
虚拟专用网络		对等连接路由表				
云专线	~					揭作
弹性云服务器	5	CI LI TARAT	1. 19040341			1981 F

在防火墙所在虚拟机网卡上关闭 源/目的检查

天員 Cloud		用户使用指南
	可用分区 可用区1 委托名称 ✔ ⑦ 新建委托名称	
<u>太子</u> がは全利日 意覧	企业项目 default 云主机组 查看云主机组	
弹性云主机 云主机备份 物理机服务	云硬盘 网卡 安全组 弹性IP 监控 标签 添加网卡 您还可以增加 0 块网卡	
云硬盘 云硬盘备份 镜像服务	 へ 192.168.1.8 网卡ID 6c44ad9d-10f0-4bb7-9c49-f67a1a788026 	
弹性伸缩 ~ 举 弹性负载均衡(外网)	状态 学性IP 安全组 guantong	
密钥对云主机组	源/目的检查 ⑦ ⑦	

需要通过同一内网网段的业务主机访问防火墙配置页面

首先将防火墙 IP 改为静态 Ip 地址

云下一代防火墙 _{ECFW}			^{我略} 对象 网络	备 系统			
🔗 安全域	+ 新建 ~ ∥ 编辑 - 删除						
□ 接口	□ 接口名称 状态	获取类型. IP/掩码	IPv6/前缀长度 MAC	安全域	虚拟系统 接入用户/IP数	上行速率	下行速率 功能
+ DNS	🖂 ethernet0/0 🛛 👰 👰	Ethernet 接口				× Mbps	204.94 K
+ 💮 路由	🗌 vswitchif1 🛛 👰 👰	基本配置 IPv6 配置	属性 高级			0 bps	0 bps
80 应用层网关		基本配置					
+ 羄 全局网络参数		接口名称:	ethernet0/0				
		描述:		(0 - 63)字符			
		绑定安全域:	○ 二层安全域 ● 三层安	全域 〇 TAP	○ 无绑定		
		安全域:	trust ~				
		HA同步:	□ 启用				
		IP配置					
		类型:	● 静态IP	自动获取			
		IP地址:	192.168.1.8				
		子网掩码:	255.255.255.0				
		□ 配置为Local IP					
		管理方式					
		Telnet 🖂 SS	H 🖓 Pina 🗌 HTTP	🖂 HTTPS 🛛 🖓	SNMP		

添加防火墙默认路由 0.0.0.0/0 下一跳为 虚拟网关的虚 IP



云下	一代防火墙	ECFW			首页 威胁	的监控中心	\$	监控 1	策略	对象	网络	系统	
8	> 安全域		+	新建	✔ 编辑 — 删除	Ì.							
£.	接口			状态	IP/掩码	下一跳到	地型	下一跳网关/虚拟	下一跳接口	协议	时间表	优先权	度量
+ 01	DNS				0.0.0/0	网关		192.168.1.100	ethernet0/0	静态		1	0
_ (**	路由				192.168.1.0/	接口			ethernet0/0	直连		0	0
					192.168.1.8/	接口	m 44 mb -	- W 7 892	ethernet0/0	主机		0	0
	目的路由						目的路日	日配直					×
	目的接口路由						目	的地:	0.0.0.0				
	源路由						子	网掩码:	0				
	源接口路由						下	—跳:	◎ 网关		〇 当前	系统虚拟路由器	
20	前田屋岡关								〇接口				
							20	关:	192.168.1	1.100			
+ 33	全局网络参数						时	间表:		`	<i>(</i>		
							优	先权:	1		(1 - 255), 🕯	決省值: 1	
							路	由权值:	1		(1 - 255), 🗄	決省值: 1	
							Та	g值:			(1 - 4294967	7295)	
							描	述:			(1 - 63)字符		
												确定	取消

去掉防火墙绑定的弹性 IP, 然后可以通过虚拟网关虚 Ip 绑定的弹性 IP 来访问防火墙:

<u>https://VIP</u>对应的弹性 IP: 10443

← → C ▲ 不安全	140.246.158.130:10443/#	homepage									ŕ	४ 😩 🕻
云下一代防火墙 ECFI	N 首页	威胁监控中心		策略		网络				A ect	wadmin@roo	
										个性化 刷	新间隔: 5分	钟
系统信息					G -×	许可证						c -×
序列号: 主机名称: 硬件平台: 系统时间: 系统运行时间: HA状态: 软件版本: 启动文件: 病毒过滤特征库:	01006038065965년 ECFW-6000 婚祖 ECFW-6000-VM01 2019/92년 星期回 0:-17:34 47 分钟 46 원· Version 5.5 ECFW6000-5.5R6P2.3-v6 2011 2.1.190922 2019/09/20 00.52:4	编辑 8/12/13 15:12:50 54 升级				客户 天翼云 天翼云 天翼云 武用授权 试用授权		 类型 URL DB 应用特征库 入侵防衛 病毒过滤 SCVPN IPSEC VPN QoS 云沙箱 平台 虚拟CPU 值尸网络C& 	有效时间 水久有效、升级有效限2016 水久有效、升级有效限2016 水久有效、升级有效限2016 水久有效、升级有效限2016 水久有效、升级有效限2016 水久有效、升级有效限2016 水及和数。 水极权 有效限制%50天。 未提权 有效限制%55天。 未提权	//11/26(剩余61天 //11/26(剩余61天 //11/26(剩余61天	其他信息 可购买超6 可购买超6 可购买超6	采服务延 采服务延 采服务延
展記約4288 ☆ RE約 の ア面	<u> </u>	 #	最近一天	× 	C - X	总流量 1.5k (red)) 野 ビ 500 0	09/25 12:00	0 00/25	18.00 08/26	最近一天	29/26 06:00	c -×

场景四:

虚拟网关下挂防火墙 , 业务主机内外流量均经过防火墙 网络配置:

如图将 VPC 的吓一跳地址指向 防火墙私网地址

用户使用指南

の络控制台	名称 ID 子网个数	vpc-sldtest 7bd993f9-f5be-46cf-be0e-585a1a07d50f さる个		状态 VPC网段 企业项目	正常 192.168.0.0/16 default	1	
总览	子网	路由表 拓扑图 标签					
虚拟私有云	自定义	各由表					
访问控制	~ 添加	络由信息 您还可以申请99个路由信息。					
弹性公网IP和带宽	~ 目的地	址	下一跳地址			操作	
NAT网关	0.0.0.0	/0	192.168.1.8			修改	删除
弹性负载均衡	~	****					

在防火墙所在虚拟机网卡上关闭 源/目的检查

天翼云 e Cloud

	可用分区	可用区1
C≡∋⊃	委托名称	🖉 ② 新建委托名称
云主机控制台	企业项目	default
总览	云主机组	查看云主机组
弹性云主机	云硬盘 网十	≂ 安全组 弹性IP 监控 标签
云主机备份		
物理机服务		经产业交通当10 条图下
云硬盘	192.168	1.8
云硬盘备份		
镜像服务		6C44ad9d-10T0-4DD7-9C49-T67a1a788026
弹性伸缩 ~	大念	◎ 淑古
弹性负载均衡(外网)	5甲性IP	
密钥对	安全组	quantong
云主机组	源/目的检查	

需要通过同一内网网段的 Vm 访问防火墙配置页面

首先将防火墙端口改为静态 Ip 地址

云下一代防火墙 _{ECFW}			策略 对象 🕅	网络 系统		۶
🔗 安全域	+ 新建 ~ ✔ 编辑 - 删除					
□ 接口	□ 接口名称 状态	获取类型. IP/掩码	IPv6/前缀长度 MAC	安全域	虚拟系统 接入用户/IP数	上行速率 下行速率 功
+ DNS	🖂 ethernet0/0 🛛 👰 👰	Ethernet 接口				× ! Mbps 204.94 K
+ 😳 路由	🗌 vswitchif1 🛛 🁰 🧟	基本配置 IPv6 配置	属性 高级			0 bps 0 bps
80 应用层网关		基本配置				
+ 蒜 全局网络参数		接口名称:	ethernet0/0			
		描述:		(0 - 63)字符		
		绑定安全域:	○ 二层安全域 ● 三层g	安全域 ○ TAP	○ 无绑定	
		安全域:	trust ~	·		
		HA同步:	□ 启用			
		IP配置				
		类型:	● 静态IP ()自动获取		
		IP地址:	192.168.1.8			
		子网掩码:	255.255.255.0			
		□ 配置为Local IP				
		管理方式 □ Telnet □ □ SS	iH 🖂 Pina 🗆 HTTP	HTTPS 17	SNMP	

添加防火墙默认路由 0.0.0.0/0 吓一跳为 虚拟网关的虚 IP



云下	一代防火墙	ECFW			首页 威胁)监控中心		监控	策略	对象	网络	系統	ŧ	
6	。 安全域		+	新建 🧳	🖌 编辑 — 删除	t								
6	3 接口			状态	IP/掩码	下一跳类	型	下一跳网关/虚护	5 下一跳接口	协议	时间	表	优先权	度量
+ [00	DNS				0.0.0/0	网关		192.168.1.100	ethernet0/0	静态			1	0
- @	路由			.	192.168.1.0/	接口			ethernet0/0	直连			0	0
	日約號由				192.168.1.8/	接口	日的路底	中記書	ethernet0/0	王机			0	0 X
+ 5	日前田田 目的接口路由 源接口路由 う 应用层网关 全局网络参数						目 子 下 网 时 优 路 Ta 描	的地: 网摊码: 一跳: 关: 间表: 先权: 由权值: g值: 述:	0.0.0.0 0 ● 网关 ○ 接□ 192.168. 1 1	1.100	(1 - 2: (1 - 2: (1 - 4: (1 - 6:	〕当前系统 555), 缺省位 294967295) 3)字符	虚拟路由器 直: 1 直: 1) 确定 耳	又消

去掉防火墙绑定的弹性 IP, 然后可以通过 VR 虚 Ip 绑定的弹性 IP 来访问防火墙: <u>https://VIP</u>对 应的弹性 IP: 10443

← → C ▲ 不安	全 140.246.158.130:10443/#h	iomepage									☆ 😩 🤇
云下一代防火墙	CFW 首页	威胁监控中心		策略	对象	网络				A ecfwadmi	n@root
									11	生化 刷新间隔	: 5分钟
系统信息					c –×	许可证					с – ×
序列号: 主机名称: 硬件平台: 系统如句: 系统运行时间: HA状态: 软件版本: 启动文件: 病离过滤特征库:	0010060380659654 ECFW-6000 編辑 ECFW-6000-VM01 2019/9/28 星期四 09:17:34 47 分钟 46 秒 Standalone 編辑 Version 5.5 ECFW6000-5.5R6P2.3-v6 2018, 2.1.190920 2019/09/20 00:52:54	编辑 /12/13 15:12:50 \$ 升级				客户 天翼云 天翼云 天翼云 天翼云 试用授权 试用授权		类型 URL DB 应用特征库 入役防衛 病毒过速 SCVPN IPSEC VPN OoS 云沙箱 平台 虚拟CPU 僵尸网络C&	有效时间 永久有效、升级有效期2019/11/26(0 永久有效、升级有效期2019/11/26(0 永久有效、升级有效期2019/11/26(0 永久有效、升级有效期2019/11/26(0 有效期剩余60天。 未授权 有效期剩余55天。 未授权 有效期剩余55天。 未授权 未授权	其他 利余61天 可购 利余61天 可购 利余61天 可购	信息 实延保服务延 实延保服务延 实延保服务延 实延保服务延
威胁视图			最近一天	Ŷ	c –×	总流量			最近一	- , ~	с – х
∲ 成語 	 	0 #		 任		1.5k ((a)))))) ()))))))))))	09/25 12:00	09/26	18.00 05/25	09/26 06	2:00

3. 2态势感知控制台登录及内网 IP 配置

登录

 打开浏览器(支持以下浏览器: Google Chrome、firefox、Edge),用 HTTPS 方式连接内 网系统部署的设备 IP 的地址加端口号,(https:/IP:18443)回车打开登录界面。导入授 权。(授权会在购买成功后,通过邮件的形式发送到邮箱)



	态势感知系统	
	授权导入	
	OWNmZmE5YzNmMzk2NDBjNWIzNDE5Njc5MGRkZThm MjE=	
11	授权文件	A State of the
	上 授权文件上传	

2)进入下图所示的登录页,输入默认登录名及密码(默认账号密码通过邮件进行通知,首次
 登陆后请修改默认密码),输入验证码,单击登陆进入系统。

用户登	录
登录名	
请输入你的登录名	
密码	
请输入您的密码	
验证码	
请输入验证码	The
登录	

内网 IP 配置

首次登录系统,或管理的 ip/ip 段变化时,需在系统管理→系统设置→内部 IP 管理菜单页 面,进行 ip/ip 段的增加、编辑、删除。添加内网 IP,可以明确流量流向,明确威胁检测的 异常行为阶段,明确资产扫描发现的资产的详细归属信息,方便资产扫描、漏洞扫描添加任 务时选择需要扫描的资产,明确扫描范围。

当前位置: 系	- 師位置: 系统管理 / 系统设置 / 内部P管理										
系统状态	系统状态 thinkflow管理 内部P管理 忽略规则管理 功能配置										
	· 版 · D · D · D · D · D · D · D · D · D										
序号	IP/IP段	公司	部门	省/直辖市	市/地区	责任人	联系电话	联系邮箱	更新时间	操作	
1	10.1.1.1/24,10.1.2.1/24,10.1.3.1/24,10.1.4.1-10.1.4.38	c	с	北京市	北京市				2018-12-14 15:4 0:27	◎ 編編 ◎ 删除	
2	192.168.1.135	华骞在线	研发部	北京市	北京市				2018-12-10 16:4 0:30	2 編編 0 無除	
3	192.168.1.0/24	华赛在线	研发部	北京市	北京市	XXXX	12345678	XX@XX.com	2018-12-10 16:4 0:38	2 編編 〇 删除	

ip/ip 段添加、编辑时需要填写相关信息,包括:所属公司、部门、地区、责任人、联系电话、联系邮箱,红色星号标明的字段为必填项。

添加		×
* IP/IP段:	支持标准CIDR格式,可以一次输入多个IP/IP段, 使用换行分隔	
*所属公司:	请填写公司名称	
* 部门:	示例:北京地区办公网	
*地区:	请选择地区 >	
责任人:	示例:总部安全组	
联系电话:	管理责任人联系电话	
联系邮箱:	管理责任人联系邮箱	
	取消	保存

3.3资产管理

资产收集

其し Loud

系统支持三种方式的资产收集

主动扫描

资产扫描任务管理,需在资产管理→资产收集→主动扫描→扫描任务管理页面添加、删 除、编辑、开始、暂停。



当前位置:	ND置: 资产收集/主动归播/扫描任务管理								
主动扫描	主动扫描 被动发现 手工添加								
待确认资产 扫描端口坦管理									
请输入搜索内容 以搜索 + 添加出 提									
	序号	任务名称	扫描状态	开始时间	任务状态	操作			
+	1	测试任务05	100%	2018-12-14 10:46:52	完成	③ 开始 / 2 编辑 / 1 删除			
+	2	测试任务04	100%	2018-12-14 10:46:52	完成	③ 开始 【2 編編 】 副除			
+	3	测试任务03	100%	2018-12-14 10:46:52	完成	③ 开始 【2 編編】 1 删除			
٠	4	测试任务02	100%	2018-12-14 10:46:52	完成	③开始 区编辑 ① 删除			
+	5	测试任务01	100%	2018-12-14 10:46:52	完成	③ 开始 2 编辑 1 删除			

添加扫描任务时,需要填写任务名称、扫描的资产(扫描资产可以从内网资产中选择, 也可任意添加)、扫描端口(系统内置多个类型的端口组,也可以任意添加单个或多个)、扫 描类型(支持单次或周期)、扫描速度(支持慢速、中速、快速,扫描速度根据单位带宽情况 选择)、允许扫描时间段。

添加扫描任务		×
*任务名称:		
*扫描资产:	选择扫描资产 v 支持标准CIDR格式,可以一次输入多个IP/IP段 使用换行分隔	
*扫描端口:	选择已有端口分组 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
477444 M/ 701	日 另存为端口组	
扫描类型: *扫描速度:	 単次 切換扫描类型 选择扫描速度 	
允许扫描时间段:	开始时间 ① 到 结束时间 ①	

扫描端口组管理,根据不同的网络环境,系统内置多个扫描的端口组,支持添加、编辑、删除扫描端口组。

资产概范	资产列表	资产收集								
当前位置: 资产;	心位量: 资产收集 / 主动归施 / 归施满口地管理									
主动扫描	被动发现	手工添加								
待确认资产	扫描任务管	理 扫描演口组	E#							
				+ 添加第日組						
	分组名称		详情信息	操作						
	企业常用講師		21221225130.01(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)	∠ 编辑 0 8時						
	救援库演口	I	1433,1521,3306,5432,5984,6379,0007,5042,9200,11211,27017,50000	▲ 编辑 ① 田時						
	全部满口		1-6555	▲ 编辑 0 部時						
	公安阿萊用講		21,22,23,25,00,81,137,139,161,443,445,515,554,992,1433,1900,3306,3389,6379,8080,22105,9000,37777,49152	▲ 網羅 ① 粉除						
	常用調口TOP	500	21+23/0-111/161/389-443-445312-554,875.999-1080;1111;1254,1433;1521;1531;1531;1531;1531;1532;1552;2552;2	∠ 编辑 0 80%						
	常用調口TOP	50	132/12232323(53)(68)(0.0)(10)(11)(12)(15)(17)(39)(41)(17)(39)(41)(45)(45)(15)(20)(42)(42)(42)(42)(42)(42)(42)(42)(42)(42	∠ 编辑 0 删除						
	常用読口TOP	10	21,22,23,25,80,110,139,443,445,3389	▲ 编辑 ○ 田時						
	视频网常用演	ю	21,22,23,00,01,1137,161,443,545,1900,3306,3309,4090,37777,49152,59100	▲ 编辑 ○ 田田						
	常用講口TOP	20	21,22,23,25,53,00,110,135,137,139,143,145,443,445,515,1433,1900,3306,3309,5378,7547,0000,9200	▲ 编辑 0 田時						
	邮件服务器装	П	25,110,143,445,995,993	2.编辑 0.888						
	工控調口		102,789,1200,1201,1911,1962,2404,2455,5006,5007,5094,9600,10245,20000,20574,30710,44810,47808	2. 编辑 0. 80%						

主动扫描发现的资产,可以通过开关控制,是否需要人工确认,如不需要进行人工确 认,发现的资产直接进入资产列表。如需要人工确认,扫描发现的资产进入资产管理→主动 扫描→待确认资产页,可以单个或批量确认资产,确认后进入资产列表。

资产概范	资产列表	资产收集						
当前位置: 资产(政集 / 主动扫描	/ 待确认资产						
主动扫描	被动发现	手工添加						
- 日本語の学校では、日本語の学校では、日本語の学校では、 - 日本語の学校では、 - 日本語の学校校校 - 日本語の学校校 - 日本語の学校校校 - 日本語の学校校校 - 日本語の学校校校 - 日本語の学校校校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校 - 日本語の学校 - 日本語の学校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校 - 日本語の学校 - 日本語の学校 - 日本語の学校校 - 日本語の学校 - 日本語の学校 - 日本語の学校 - 日本語の学校校 - 日本語の学校 - 日本語のの学校 - 日本語の学校校 - 日本語の学校校 - 日本語の学校								
						IP:	任务名称:	按索 重翌
	序号	IP	操作系统	第日	服务	组件	任务名称	操作
	1	192.168.1.49	embedded	443,5003,6646,7680,50500,54345	https;filemaker,unknown,unknown		192.168.0.0/16	2 确认 0 809:
	2	192.168.1.43	Linux 3.X	22	ssh		192.168.0.0/16	日 時以 🕤 日時
	3	192.168.1.64	embedded	135,139,445,2425,6000,7680,49667,65170	msrpc,netbios-ssn,microsoft-ds,fjitsuappm gr,X11		192.168.0.0/16	日 論认 〇 副除
	4	192.168.1.117	Linux 3.X	22,443,9093,47030	sshuhttps	生) ^{ae} -Strict-Transport-Security,Web服务器 -NgInx	192.168.0.0/16	🖸 1844 🔿 1858
全选	确认已选进户	确认全部资产						

被动发现

在资产管理→资产收集→被动发现页面,展示通过对流量分析发现的存活资产及操作系统。被动发现的资产,可以通过开关控制,是否需要人工确认,如不需要进行人工确认,发现的资产直接进入资产列表。如需要人工确认,在被动发现页面,可以单个或批量确认资产,确认后进入资产列表。

当前位置: 资产	位置: 资产收集/被动发现								
主动扫描	被动发现	手工添加							
				IP:	搜索 重置				
序号		IP	操作系统		操作				
			暂无数据						



在资产管理→资产收集→手工添加页面,添加资产 IP、归属信息、责任人、联系方式、 硬件信息、厂商等信息后点击保存。

主动扫描 被动发现 手工添加	
* IP:	
* 所属公司:	
* 高)门:	
*地区:	
责任人:	
联系电话:	
联系邮箱:	
硬件序列号:	
硬件厂商:	
自定义标签:	+ 新建标签

资产确认设置

天翼口 e Cloud

> 主动扫描、被动发现的资产,通过开关控制,是否需要人工确认,资产入库配置开关, 在系统管理→系统设置→功能配置菜单页面,默认关闭。

当前	当前位置:系统管理/系统设置/功能配置							
NV.	系统状态	thinkflow管理	内部IP管理	白名单管理	忽略规则管理	功能配置		
	云平	石品置						
	统计数	据上传云中心 🌍	ŧ					
	国家信	蒼库自动更新 开	C					
	资产	一入库配置						
	系统扫描	手动确认入库 🔵	é					
	被动探测	手动确认入库 🔵	é					
	违规	的联配置						
	违规	以外联功能启用 🔵 🖇	ŧ					
	威胁	的检测配置						
	恶意	网站检测启用 🔵	ŧ					

资产列表

资产管理→资产列表页显示确认的全部资产 IP 地址、操作系统、组件、标签、资产归属、责任人、更新时间等信息,支持高级搜索及资产导出。点击操作按钮,可以自定义显示

列表字段。点击列表左侧"+"按钮,可以查看资产的硬件序列号、硬件厂商、端口、服务、 漏洞、威胁等信息。

天翼**云** e Cloud



点击资产详情,查看资产的属性信息,查看资产的端口开放、资产的漏洞数量、威胁数 量、历史更新。

当前位置:资产管	理/资产列表/资产调查								
10.1.4.35									
硬件序列号	A101435 区编组	资产名称	10.1.4.35						
硬件厂商	DELL 区编辑	操作系统	Windows XP						
资产归屋	北京 / 北京 / 档案 / 贾燕青 ビ網構	发现方式	系统扫描						
标签	系统设备	添加时间	2018-12-19 14:03:36						
组件	「其他安全产品-WebEngine」 项目管理·神道系统 Web组件-PHP								
端口信息	漏洞调查 威胁调查 历史更新								
> 10.1.4.35	4444								
Ƴ 10.1.4.35	443								
开放									
> 10.1.4.35 3306									

资产概览

天翼**云** e Cloud

> 在资产管理→资产概览页面,查看资产的相关统计情况。资产总量,统计了收集到的所 有资产。开放端口数,统计了资产使用的端口情况。资产总量变化,显示最近7次的扫描结 果变化情况。设备类型分类,统计各种设备类型及数量。资产归属统计,按照部门统计资产 数量。端口分布,统计端口的使用情况占比。操作系统分布,统计资产的操作系统占比。



3.4脆弱性检测

漏洞扫描

在脆弱性检测→漏洞扫描页面,对漏洞扫描任务进行管理,支持添加、暂停、编辑、删 除漏洞扫描任务。



manymas	mtm796UU mtm72770* mtm73-0m								
当前位置:	胞弱性检测 / 漏洞的	刮描	转输入搜索内容						
	序号	任务名称	扫描状态	還詞高/中/低危以下个数	开始时间	任务状态	操作		
+	1	TCP	100%	0/0/0	2018-11-14 10:03:40	完成	③ 开始 〇 勤除		
٠	2	88866	100%	0/0/0	2018-11-13 14:14:08	完成	③ 开始 10 删除		
٠	3	192.168.1.27	100%	1/1/1	2018-11-13 14:14:11	完成	③ 开始 〇 副除		
	4	192.168.1.102	0%	0/0/0	2018-11-13 15:40:48	已停止	③ 开始 10 删除		
+	5	192.168.1.0/15	0%	0/0/0	2018-11-14 10:33:17	已停止	③ 开始 🕇 删除		
٠	6	8	100%	0/0/0	2018-11-13 14:12:32	完成	③ 开始 0 删除		
+	7	192.168.1.27	100%	1/1/1	2018-11-13 14:12:09	完成	③ 开始 ① 删除		
٠	8	192.168.1.0/24	100%	15 / 54 / 25	2018-11-13 14:14:29	完成	③ 开始 🖞 副除		

添加漏洞扫描任务,填写任务名称,选择扫描的资产即可。

*任务名称:	
	选择扫描资产
*扫描资产:	支持标准CIDR格式,可以一次输入多个IP/IP段 使用换行分隔

漏洞列表

在脆弱性检测→漏洞列表页面,可以查看漏洞扫描的结果。漏洞列表以资产和漏洞维 度,分别列出资产存在的漏洞列表及漏洞影响资产列表。资产存在漏洞列表展示资产 IP、漏 洞名称、等级、影响组件、更新时间,点击查看详情可以看到漏洞描述、危害和解决方案信 息。支持根据漏洞名称、对应资产、漏洞等级、更新时间等条件的检索。

天翼云 e Cloud
Cloud

SUPPORT	門 测问影明到产					
潤洞名称:		对应资产: 通问等级: 运问等级	✓ 更新时间: 开始	始日期 - 航東日期 凸	28	* #3
序号	资产IP	講詞名称	等级	影响给任中	发现时间	銀作
11 - F	192.168.1.250	缺少httpOnly' Cookie属性	時間	在cookie中使用会话处理的应用程序。	2018-11-13 17:29:43	○ 童后详情
2	192.168.1.250	DCE / RPCROMSRPC服务收单指告	中位		2018-11-12 20:00:15	0 25175
3	192.168.1.235	3CP#2回時載:	低危		2018-11-12 19:49:09	○ 查看详续
4	192.168.1.235	MacOS X Finder/DS_Store 但愿被需	中位		2018-11-12 19:49:09	〇皇香祥賞
5	192,168,1,200	TCPP的问题	低化		2018-11-09 13:49:50	◎ 查看详情
6	192.168.1.200	SSL/TLS: SSL+3协议CBC座码套件信息准备推阅 (POODLE)	中位		2018-11-09 13:49:50	〇 東新祥橋
7	192.168.1.200	SSL/TLS: RSA临时密码处理RSA_EXPORT降级问题 (FREAK)	中間	- 主机接受 RSA_EXPORT 电码卷件 - 在3.9.8.84之影的OpenSSL版本,1.0之前的 1.0.0.0p和1.0.1.1k之前的0.1.	2018-11-09 13:49:50	〇重香洋情
8	192.168.1.200	55L/TL5: 报告销售码器件	#15		2018-11-09 13:49:50	0 26#\$
9	192.168.1.200	SSL/TLS: 报告HTTPS的雇党攻击的电码靠件	中間	接受易受攻击的SSL/TLS密码的服务套件通过HTTPS.	2018-11-09 13:49:50	〇 京 石洋情
10	192.168.1.200	SSL/TLS:已再用的SSLv2和SSLv3协议检测	中間	使用SSLv2和/盒SSLv9协议提供加密通信的所有面势。	2018-11-09 13:49:50	○ 查看详续
11	192.168.1.200	SSL/TLS:中间安金绕过藻周(LogJam)中的DHE_DCPORT人	中位	- 主机接受 DHE_DIPORT 寄码套件 - 1.0.20 构1.0.1n之前的OpenSSL版本	2018-11-09 13:49:49	◎ 宣告详情
12	192.168.1.200	逐转SSH翻MAC网)自	低歌		2018-11-09 13:49:49	〇東新洋橋
13	192.168.1.200	变持55H赣加南韓迪	中茂		2018-11-09 13:49:49	〇 度石评估

漏洞影响资产列表,以漏洞维度展示对资产的影响情况。展示漏洞名称、漏洞类型、等级、更新时间、影响资产数量,点击查看详情可以看到漏洞描述、危害和解决方案信息。支持根据漏洞名称、漏洞类型、漏洞等级、更新时间等条件的检索。

漏洞概范	漏洞列表 灑洞扫描					
当前位置: 脆弱	性检测/漏洞列表					
资产存在	羅洞 <u>満</u> 洞影响资产					
潤洞名称:	潤同 英型:	澳同等级 : 凯阿等级	> 更新时间: 开始日期	~ 结束日期 芭		搜索 里靈
序号	通詞名称	漏洞类型	等级	更新时间	影响资产数	操作
1	Fedora更新为星号FEDORA-2013-24108	Fedora本地安全检查	中茂	2018-12-14 06:46:17	3	◎ 室石洋情
2	mod_day_svn CESA-2015的CentOS置新: 0166 centos7	CentOS本地安全检查	中危	2018-12-14 06:45:48	2	○ 重新评估
3	针对phpMyAdmin的Fedora更新FEDORA-2014-9555	Fedora本地安全检查	低性	2018-12-14 06:45:48	2	◎ 重看洋情
4	Apple Safari安全更新(HT208223)	通用	中危	2018-12-14 06:45:48	2	◎ 重看洋情
5	Amazon Linux Local 检查: ALAS-2015-502	Amazon Linux本地安全检查	高忠	2018-12-14 06:45:48	2	◎ 童香洋情
6	针对vte3 FEDORA-2011-9330的Fedora更新	Fedora本地安全检查	低幣	2018-12-14 06:45:49	2	○ 宣誓洋情
7	针对gemu FEDORA-2016-3d3218ec41的Fedora應新	Fedora本地安全检查	(E)S	2018-12-14 06:45:49	2	◎ 重碳评情
8	Linux USN-2803-1的Ubuntu運動	Ubuntu本地安全检查	中危	2018-12-14 06:45:49	2	○ 重香洋情
9	针对netty FEDORA-2015-8684的Fedora選新	Fedora本地安全检查	中危	2018-12-14 06:45:50	2	◎ 重若洋情
10	Microsoft Windows參介購開 (KB4338826)	Windows: Microsoft公告	南范	2018-12-14 06:45:50	2	○ 豊香洋情
	思科邮件安全设备Drop Bypass雇用	cisco	中危	2018-12-14 06:45:51	2	◎ 宣誓洋衛
12	WordPress GDI评级系统插件多个漏洞	Web应用程序运用	中茂	2018-12-14 06:45:51	2	○ 宣誓评情
13	针对vino FEDORA-2013-17121的Fedora遺新	Fedora本地安全检查	高忱	2018-12-14 06:45:51	2	◎ 重要评情

漏洞概览

在脆弱性检测→漏洞概览页面分析整体 IT 资产漏洞趋势、等级和类型分布。漏洞趋势统 计最近 7 天的高危、中危、低危漏洞的数量变化曲线。资产漏洞排行,根据漏洞扫描的结 果,统计漏洞风险值最高的前 5 个 IP 资产。最近扫描任务,统计最近 5 次的漏洞扫描任务结 果,统计每个任务的漏洞总数、高危漏洞数、中危漏洞数、低危漏洞数。漏洞等级分布,统 计高危、中危、低危每个等级发现的漏洞总数及占比。漏洞类型分布,统计漏洞数最多的前 15 种漏洞类型的数量及占比。





3.5威胁检测

威胁检测无需特殊配置,接入网络后即开始工作。

威胁概览

在威胁检测→威胁概览页面,主要统计分析当前用户环境所面临的威胁情况。具体包括 异常行为的总量及高危异常行为类型 TOP3。统计最近 24h 的异常行为类型及数量。根据最近 24h 的异常行为数量,统计受影响主机 TOP5,表格展示资产 IP、资产归属、异常行为数。根 据威胁数量统计最近 24h 的威胁方排行,国内、国际分别统计 TOP5,表格展示威胁方 IP、所 在地、异常行为数。威胁方归属地统计异常行为数最多的威胁方所在地,国内、国际分别统 计 TOP10。

当前位置:威胁检测/威胁概范							
月常行为8章 53394	-4.49%	···· 7876	-3.60%	• 7782	-4.21%	(学) 5799	-4.50%
威胁行为类型				受影响主机排行 (最近24h)			
10,000				风险资产	异常行为分布	资产日属	异常行为数
		1		10.1.1.155	Α	北京分公司/北京/北京/财务/王劳	150
\$000		Å		10.1.3.69		北京分公司/北京/北京/财务/王芳	147
0				192.168.1.49	A	北京分公司/北京/北京/财务/王劳	147
18:00:00 21:00:00	02-15 03:00:00	06:00:00 09:00:00	12:00:00 15:00:00	10.1.1.248		北京分公司/北京/北京/财务/王芳	146
— C&C通讯 — WEB欧击 —	暴力破解 — 恶意软件 — 系统后门] — 其他 — 粉索软件 — 扫描目	测 — 漏漏利用 — 系统提权	10.1.2.4	A	北京分公司/北京/北京/财务/王芳	143
国内威胁方排行 (最近24h)				国际威胁方排行 (最近24h)			
威胁方	地区	异常行为分布	异常行为数	威胁方	地区	异常行为分布	异常行为数
58.19.228.217	测制化	A	2129	52.60.57.146	加拿大	A	2121
58.42.242.58	貴州		2126	77.53.89.97	瑞典		2112
222.186.112.209	11 1 5	A	2097	95.78.57.184	张罗斯	A	2082
117.23.2.58	快西		2077	154.95.188.49	28		2073
47.107.247.180	36I		2074	89.107.184.192	19 M	A	2069
国内威胁方归属地				国际威胁方归属地			
8				4			
				1			
2				2			
1							
IRIX LN	云南 安慶 山东	广东 江市 日	日本 知此 豊州	· 美国 加拿大 #5	信罗斯 土耳其	巴西 新加坡 日本	第二日

威胁列表

在威胁检测→威胁列表页面,列表详细记录了威胁事件发生的时间、源 IP、目的 IP、协议、流向、威胁类型、威胁明细、严重级别、攻击阶段、来源、威胁方归属地、探针 IP。威

胁事件支持按照时间、按照事件的属性进行筛选。威胁事件根据威胁类型和威胁明细统计, 影响最多的前十类。列表右侧操作项,威胁事件支持下载数据包取证。



列表右侧操作项,威胁事件支持针对事件和规则的忽略。忽略事件,仅忽略当前一条事件日志。忽略规则,包括忽略此条检测规则和此资产 IP 相关的事件。

? 确定忽略此事件吗?			?	请选择忽略的类型: 		
	取消	确定			取消	确定

忽略的规则,通过系统管理→系统设置→忽略规则管理页面管理,将已经忽略的规则删 除后,规则继续生效。

当前位置:系统	管理/系统设置/忽略规则管	锂				
系统状态	thinkflow管理 内部	P管理 白名单管理	忽略规则管理	功能配置		
序号	资产IP		大类描述	规则描述	忽略时间	操作
1	1 192.168.1.8		全部	无	2019-02-15 18:07:50	白趣味
2	全部		其他	SSL指纹黑名单恶意SSL证书	2019-02-15 18:07:44	ロ副院

警告配置

天翼**云** e Cloud

> 威胁检测→警告配置页面的攻击源警告,用于对攻击源警告。当系统检测到远端 IP 地址 存在恶意入侵或者探测行为时,可以对相应的 IP 进行告警,对其推送告警界面,以做警示, 并记录告警事件时间和攻击源 IP 地址。

天翼云
CCIUUU

威胁概范 曼	む 影响主机	威胁列表 流量松	测 警告配盟		
当前位置:威胁感知	1/警告配置				
攻击源警告	恶意网站警告				
会计向攻击者	·聽告801次				
				64/B	144
ほう	5			8318)	以山原
1				2018-11-13 13:43:54	192.168.1.111
2				2018-11-13 13:42:53	192.168.1.111
3				2018-11-13 13:41:52	192.168.1.111
4				2018-11-13 13:40:51	192.168.1.111
5				2018-11-13 13:39:50	192.168.1.111
6				2018-11-13 13:38:49	192.168.1.111
7				2018-11-13 13:37:48	192.168.1.111
8				2018-11-13 13:36:47	192.168.1.111
9				2018-11-13 13:35:46	192.168.1.111
10				2018-11-13 13:34:45	192.168.1.111
11				2018-11-13 13:33:38	192.168.1.111

威胁检测→警告配置页面的恶意网站警告,用于对系统用户警告。当系统用户访问恶意 网站时,对自己的用户推送提示页面,可以使用默认的提示内容,也可以自定义提示页面, 自定义页面仅支持上传 html 的文件包。

恶意网站的数据,来源于国家能力中心。也支持用户自定添加,用户将自己整理的恶意 网站的名称、域名添加到系统中,系统支持对自定义添加的恶意网站的编辑、删除、停用、 启用。

い警告両後 🤒	自定义警告页面						
	權被名称	详情	8	后面新时间	操作		
	· 至意用站警告(1810月的网站被列入了国家信誉展布单,可能会存在安全风险,建议停止访问:	2018-11-07 19:05:25		● 到注 已 编辑		
网站管理							
#9	网络名称	減去	備注	源加时间	状态	操作	
1	2222.00k	ANABAB.COM		2018-11-07 1948:15	正端	0 ## 2 #8 0 ##	
2		51testing.com		2018-11-06 18:03:05	停用	0 mm 2 mm 0 mm	
3		sina.com.cn		2018-11-07 19:51:08	仲司	6 2 A 2 4 6 0 8 10	

恶意网站检测的功能开关,在系统管理→系统设置→功能配置菜单页面,默认关闭。

系	统设置	用户管理	报表管理	帮助中心	5 关于			
当前位	立置: 系统	管理/系统设置	/功能配置					
系	统状态	thinkflow管理	裡 内部IF	管理	3名单管理	忽略规则管理	功能配置	
	궀꾁	石配置						
	统计数	据上传云中心	Ħ ◯					
	国家信	營库自动更新	म 🔵					
	资产	一入库配置						
	系统扫描	手动确认入库(¥					
	被动探测	手动确认入库(¥					
	违规	则外联配置						
	违规	以外联功能启用(म 🔵					
	威胁	检测配置						
	恶意	网站检测启用(X					

3.6国家能力中心

国家信誉库

基于国家计算机网络应急技术处理协调中心(简称"国家互联网应急中心",英文简称 CNCERT 或 CNCERT/CC)拥有的国内最为先进且独一无二的公共互联网网络安全监测平台,能 够将诸如僵尸木马活动、恶意代码传播、恶意攻击行为、恶意站点数据等网络安全事件及信 誉数据同步至本系统,与国家级监测平台形成联动能力,及时发现用户单位网络安全威胁。

国家信誉库 威胁情报	2				
当前位置:国家能力中心/国	家信誉库				
国家信誉库					
序号	类型	更新时间	版本号	更新来源	操作
1	URL信整库	2018-11-08 17:14:03	URL01.20181023.01	本地上传	上 上様
2	戸信誉库	2018-11-09 09:34:04	IP.01.20181111.01	本地上得	上上段
3	城名信誉库	2018-11-08 18:15:30	DOMAIN.01.20181024.01	本地上停	上任
4	异苯检测规则库	2018-11-13 11:47:23	RULE.01.20181105.002	本地上传	土土传
5	漏渴检测规则库	2018-11-12 09:41:48	NVTS.01.20181021.001	自动同步	土 上侯

国家中心云平台配置,在系统管理→系统设置→功能配置菜单页面,统计数据上传云平 台开关默认关闭,国家信誉库自动更新开关默认开启。



系统设置	用户管理	报表管理	帮助中心	关于			
当前位置:系统	管理/系统设置,	/功能配置					
系统状态	thinkflow管理	内部IP管	理 白名峰	单管理	忽略规则管理	功能配置	
云平	台配置						
统计数	据上传云中心(¥					
国家信	營库自动更新	Ŧ					

威胁情报

对接国家中心的威胁情报和安全资讯,及时更新,包括:网络安全信息与动态周报、国家信息安全漏洞共享平台周报、CNCERT 互联网安全威胁报告、突发漏洞安全公告等。

黨家倍號库 威胁情报	
当期位置: 国家能力中心/威胁情报/安全损讯	
安全網訊 威胁情报	
 同場会全理意与功态周囲-2016年編333期 	2018-09-27
 国家信息安全規則共享平台(CNVD)用級-2018年第33期 	2018-09-27
* 国家信息安全规则共享平台(CNVD)周股-2018年第37期	2018-09-20
 网络安全信息与动态网络-2010年第37期 	2018-09-20
 同倍安全信息与动志周田-2010年第16期 	2018-09-12
• 国家信息安全通用共享平台(CWUD)阐报-2018年第36期	2018-09-12
 网络安全信息与动态周景-2016年第15期 	2018-09-06
 国家德島安全羅與其專平台(CN/D)現後-2018年編35期 	2018-09-08

3.7控制台

控制台用来统计分析用户单位的资产情况、所面临的威胁情况、单位整体的安全态势评 分、威胁资产、漏洞资产、威胁方、实时消息提示及威胁情报。

〇 1007 资产总量 ⑧ 377 高危風洞宮/	·政 51 · · · · · · · · · · · · · · · · · · ·	■ 5 失赖主机政量	8°7 教家软件主机政	● 5 恶意软件主机数	6 第四利用主机数 697474 成物总量	\rightarrow
安全市時代 中 59.71	实时地图 + -	-	A		消磨想示 时间2019-04-25 060003.或約严重吸制中编述192.168 时间2019-04-25 060003.或約严重吸制中编述192.168 时间2019-04-25 060003.或約严重吸制中编述192.168 时间2019-04-25 060003.或約严重吸制中编述192.168 时间2019-04-25 060003.或約严重吸制中编述192.168 时间2019-04-25 060003.或約严重吸制中编述192.168	 04-25 04-25 04-25 04-25 04-25 04-25 04-25
资产减助排行	实时威胁				威胁情报	更多
192.168.1.200	发生时间	受影响主机 归属	威胁方	成肋类型 威胁明细	*关于MongoDB数据库不当配置导致信息泄露风	02-22
192.168.1.108 192.168.1.209	2019-04-25 06:00:03	192.168.1.102 阿安/舆试部	47.107.247.180	日屆探測 137號口扫描	关于境内大量家用路由器DNS服务器被篡改情况	02-21
192.168.1.143	2019-04-25 06:00:03	192.168.1.174 网安/测试部	58.243.104.26	WEB攻击 Microhard Systems 3G/.	"" * 关于一种新型数表输声有关核况的译相	12-05
0 1000 2000 3000 4000	2019-04-25 06:00:03	192.168.1.143 网安/测试部	94.138.223.142	系统后门 Backdoor.Elise SSL证书		12-03
资产漏洞排行	2019-04-25 06:00:03	192.168.1.26 网安/测试部	66.51.164.209	Dyre/Trickbot/Dridex SS	* 关于PHPCMS 2008存在代码注入漏洞的安全公告	11-27
10.1.3.81	2019-04-25 06:00:03	192.168.1.76 网安/测试部	122.114.34.169	新統課税 Metasploit Meterpreter	* 关于Oracle WebLogic Server存在反序列化远程	07-18
192.168.1.40	2019-04-25 06:00:03	192.168.1.200 阿安/测试部	124.5.23.9	新聞 Linux/Kimodin SSH 后.	" 安全總理	85
10.1.3.121	2019-04-25 06:00:03	192.168.1.135 网安/测试部	35.237.53.169	Dyre SSL 证书	SCEDUA	8.9°
0 2 4 6 8 10	2019-04-25 06:00:03	192.168.1.20 网安/舆试部	89.107.184.192	C&CIBIR Perl/Calfbot C&C DNS.	◎ CNCERT互联网安全威胁报告-2019年2月	03-26
威胁方排行	2019-04-25 06:00:03	192.168.1.213	105.75.43.28	系统提权 Metasploit Meterpreter	 网络安全信息与动态周报-2019年第11期 	03-25
58.19.228.217	2019-04-25 06:00:03	192.168.1.102 阿安/期试部	47.107.247.180	日編探測 137第日扫描	* 国家信息安全漏洞共享平台(CNVD)周报-2019年	03-21
29,138,223,192 77,53,89,97 95,72,857,184	2019-04-25 06:00:03	192.168.1.20 网安/测试部	89.107.184.192	C&C透讯 Perl/Calfbot C&C DNS.	。 网络安全信息与动态周报-2019年第10期	03-15
52.60.57.146 0 500 1000 1500 2000 2500	2019-04-25 06:00:03	192.168.1.172 网安/测试部	154.95.188.49	ed Hat DHCP Client Scri	- 国家信息安全漏洞共享平台(CNVD)周报-2019年	03-15



控制台首行数字贴,统计显示资产总量、高危漏洞资产、受攻击资产、失陷主机、勒索 软件主机、恶意软件主机、漏洞利用主机、威胁总量。



安全态势评分,是系统基于当前单位的资产情况、漏洞情况、威胁情况量化出来的一个 分值。分值越高,表示系统安全系数越高,系统的安全级别分为:优、良、中、差、危五个 级别。



实时地图和实时威胁,展示系统检测到的实时异常行为情况,攻击线表示威胁方针对资 产的异常行为,箭头代表了攻击方向。

实时地图						
+ -						
实时威胁						
发生时间	受影响主机	归属	威胁方	威胁类型	威胁明细	检测源
2019-03-20 06:	192.168.1.27	北京分公司/安	58.42.242.58	其他	SSL指纹黑名单	系统预定义
2019-03-20 06:	10.1.2.77	北京分公司/安	58.19.228.217	WEB攻击	XML外部实体	系统预定义
2019-03-20 06:	10.1.1.113	北京分公司/安	117.23.2.58	暴力破解	Anuna PHP 后	系统预定义
2019-03-20 06:	10.1.1.56	北京分公司/安	124.5.23.9	系统后门	Linux/Kimodin	系统预定义
2019-03-20 06:	10.1.2.218	北京分公司/安	35.237.53.169	勒索软件	Dyre SSL 证书	系统预定义
2019-03-20 06:	10.1.3.249	北京分公司/安	121.32.129.253	其他	SSL指纹黑名单	系统预定义
2019-03-20 06:	10.1.2.162	北京分公司/安	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:	10.1.2.199	北京分公司/安	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:	10.1.3.99	北京分公司/安	47.107.247.180	扫描探测	137端口扫描	系统预定义
2019-03-20 06:	10.1.2.73	北京分公司/安	58.19.228.217	WEB攻击	XML外部实体	系统预定义
2019-03-20 06:	10.1.3.120	北京分公司/安	58.19.228.217	WEB攻击	XML外部实体	系统预定义

天翼 Cloud

资产威胁排行,根据最近 24 小时的异常行为次数统计了风险资产的 top5。



资产漏洞排行,根据最近 24 小时的漏洞数值统计了风险资产的 top5。



威胁方排行,根据最近24小时的攻击情况,统计了威胁方 top5。





消息提示,展示系统产生的操作提示,高危漏洞、威胁等检测结果,动态滚动提示。

消息提示

0	10.1.1.175发现系统后门	03-20
0	10.1.1.193发现系统后门	03-20
0	192.168.1.191发现系统后门	03-20
0	192.168.1.70发现其他	03-20
0	10.1.1.155发现系统后门	03-20
0	10.1.3.115发现系统后门	03-20
0	10.1.1.125发现其他	03-20

威胁情报,对接国家中心的威胁预警,包括:漏洞公告、恶意代码通告等。

威胁情报	更多
◎ 关于一种新型勒索病毒有关情况的	12-05
● 关于PHPCMS 2008存在代码注入漏…	11-27
■ 关于Oracle WebLogic Server存在反	07-18
● 关于Oracle WebLogic Server存在反…	07-18
● 关于第三方支付平台JAVA SDK存在	07-09

安全资讯,对接国家中心的安全态势报告,包括:网络安全信息与动态周报、国家信息 安全漏洞共享平台周报、CNCERT 互联网安全威胁报告等。

更多



安全资讯

- 国家信息安全漏洞共享平台(CNVD)... 01-24
- 网络安全信息与动态周报-2019年第... 01-24
- CNCERT互联网安全威胁报告-2018... 01-24
- 网络安全信息与动态周报-2019年第... 01-17
- 国家信息安全漏洞共享平台(CNVD)... 01-17

3.8系统管理

系统设置

系统状态

显示系统当前的使用状态。包括: IP、CPU、内存、硬盘、管理口、检测口,点击查看详 情。

系统状态	thinkflow管理 内音	和P管理 白名单管理 忽略/	观则管理 功能配置				
序号	地址	CPU	内存	硬盘	管理口	检测口	操作
1	192.168.1.43 thinkflow	0% 0核	0.00% 0 KB		网卡名: enol 预进: 0 bps 预入: 0 bps	岡卡名: Port0 帝宽: 0 bps	查看详想
2	192.168.1.111 thinkserver	3.89% 24核	10.89% 125.74 GB	/opt 1 4.24%	网卡名: em1 派出: 78.08 Kbps 强入: 9.49 Kbps	同卡名: em2 带宽: 0 bps	查看详情

Thinkflow 管理

系统支持对接多个流量探针,支持探针的添加、编辑、删除。

当前位置: 3	系统管理/系统设置/th	inkflow管理						
系统状态	thinkflow管理	内部P管理	白名单管理	忽略规则管理	功能配置			
							添加	
序号		IP		名称		更新时间	操作	
1	1	92.168.1.43			thinkflow	2018-12-04 14:06:55	◎ 編載 ① 删除	

内部 IP 管理

管理内网的 IP/IP 段,及 IP 的归属信息。通过内网 IP 管理添加 IP 后,可以明确流量流向,明确威胁检测的异常行为阶段,明确资产扫描发现的资产的详细归属信息,在资产扫描、漏洞扫描时明确扫描范围,方便快速添加扫描资产。



当前位置: 3	品位置:系統管理/系統設置/内部P管理											
系统状态	thinkflow管理 内部P管理 白名单	管理 忽略频	则管理 功能	配置								
									添加IP			
序号	IP/IP段	公司	部门	省/直辖市	市/地区	责任人	联系电话	联系邮箱	更新时间	操作		
1	10.1.1.1/24,10.1.2.1/24,10.1.3.1/24,10.1.4.1-10.1.4.38	c	c	北京市	北京市				2018-12-14 15:4 0:27	◎ 編編 合 删除		
2	192.168.1.135	华赛在线	研发部	北京市	北京市				2018-12-10 16:4 0:30			
3	192.168.1.0/24	华赛在线	研发部	北京市	北京市	XXX	12345678	XX@XX.com	2018-12-10 16:4 0:38	◎ 編編 ① 删除		

白名单管理

全局白名单,包括威胁检测、违规外联检测、攻击源警告等,支持添加 IP 和 URL。

当前位置: 系统管	管理/系统设置/白	3名单管理								
系统状态	thinkflow管理	内部IP管理	白名单管理	忽略规则管理	功能配置					
IP白名单	URL白名单									
										添加IP/IP段
序号		IP/IP段			添加时间		状	* *	1	操作
						暂无数据				

忽略规则管理

威胁检测→威胁列表,忽略的规则,在此页面统一管理,删除规则后,在威胁检测中忽 略的规则继续生效。

当	前位置: 系统	充管理/系统设置/忽	略规则管理							
	Note: / Molecul / Molec									
	序号	资产	Р		大类描述		规则描述	忽略时间	操作	
	1	192.168	.1.8		全部		无	2019-02-15 18:07:50	0 删除	
	2 全部			其他		SSL指纹黑名单恶意SSL证书	2019-02-15 18:07:44	○ 删除		

功能配置

系统各配置功能的开关,包括:系统与云平台配置、资产入库配置、违规外联配置、威 胁检测→警告配置→恶意网站警告→恶意网站检测配置。



当前位置:系统	管理/系统设置/功	能配置									
系统状态	thinkflow管理	内部IP管理	白名单管理	忽略规则管理	功能配置						
궀꾁	Z台配置										
统计数据上传云中心 () 关											
国家信	營库自动更新 开)									
资产	入库配置										
系统扫描	手动确认入库 🔵 🗧	9									
被动探测	手动确认入库 🔵 🔅										
违规	的联配置										
违规	以外联功能启用 🔵 🛪										
威胁	的检测配置										
恶意	网站检测启用 🔵 🛪										

用户管理

用户管理

系统支持用户分权分级管理,可以创建不同的用户,分配不同的角色,进行系统的管理。用户管理显示登录名称、用户名称、邮箱、角色、备注、状态,支持登录用户的添加、 编辑、删除、锁定。

前位置:系统	管理/用户管理						
用户管理	角色管理 审计日	志					
							添加
序号	登录名称	用户名称	邮箱	角色	备注	状态	操作
1	security	security	software16@163.com	安全管理员		正常	区编辑 0 删除 A 批定
2	yangjp	yangip	yangjianping@luvsec.com	系统管理用户角色,普通用户角色,安全 管理员		正常	
3	yangran01	yangran01	yang@163.com	普通用户角色系统管理用户角色		正常	
4	luokezhen	lkz	lkz@lkz.com	系统管理用户角色,普通用户角色		正常	
5	777777	yobin	yobin@110.cn	普通用户角色、系统管理用户角色		正常	
6	test123	test123	qq@qq.com	普通用户角色、系统管理用户角色		正常	🗹 9341 🔿 ### 8 tha
7	888888	初始化用户	888888@yourdomain.com	普通用户角色系统管理用户角色	系统初始化用户。	正常	☑ 編輯 ① 删除 吕 锁定
8	sys_operator	系统操作员	sys_operator@yourdomain.com	普通用户角色	系统操作员。	正常	
9	sys_admin	系统管理员	sys_admin@yourdomain.com	系统管理用户角色	系统管理员。	正常	12 編編 12 無除 8 時度

添加用户时,填写登录名称、用户名称、邮箱、设置密码、选择用户角色(支持多选)、 填写备注,点击保存即可。

* 登录名称: 清填写登录名称 只允许输入数字、英文字母和下划线、长度限制为6-30个字节 * 用户名称: 请填写用户名称 * 邮箱: 请填写用户邮箱	
 只允许输入数字、英文字母和下划线长度限制为6-30个字节 * 用户名称: 请填写用户名称 * 邮箱: 请填写用户邮箱 	
* 用户名称: 请填写用户名称 * 邮箱: 请填写用户邮箱	
* 邮箱: 请填写用户邮箱	
* 设置密码 : 请设置密码	
* 确认密码: 请确认密码	
* 分配角色: 3 项 可用角色 0 项 选定角色	
普通用户角色	
系统管理用户角色	
□ 安全管理员 天匹配结果	
备注: 备注	

角色管理

用户角色的添加、编辑、删除、权限管理。系统包括三种用户角色: 普通用户、系统管 理员、安全管理员。系统管理员全功能。普通用户只可以查看数据,没有系统设置、用户管 理的功能权限。安全管理员,只能使用安全检查功能模块。

当前位置:系	統管理/角色管理				
用户管理	角色管理 审计日志				
					添加
序号	中文名称	英文名称	备注	功能项数量	操作
1	安全管理员	security		1	◎編編 白 删除 ♀ 权限
2	普通用户角色	ROLE_USER	具有普通用户权限的角色。	2	◎編編 ● 動除 ● 权限
3	系统管理用户角色	ROLE_SYS_USER	具有系统管理权限的角色。	1	区編輯 白 删除 P 权限

审计日志

只有系统管理员可以查看审计日志,审计日志页面记录包括:日志类型、操作类型、用 户名、用户角色、操作对象、行为详情、时间。审计日志页面支持按照日志类型、操作类 型、用户名、时间的日志检索,支持日志的导出、重置。

当前位置: 3	系统管理/审计日志						
用户管理	角色管理	审计日志					
日志类	型日志美型	∨ 操作类型 操	作美型 > 用户名	3:	时间: 2019	9-02-08 18:22:21 ~ 2019-02-15 18:22:21	素 重置 导出
序号	日志类型 👙	操作类型 💠	用户名	用户角色	操作对象 👙	行为详情	时间
1	操作	添加	初始化用户	普通用户角色系统管理用户角色	BlockPolicyVO	添加屏蔽规则: 規則记录id=TUag8Gg8fqyd3al3Y8ML资产IP=19 2.168.1.8检测规则sid=null	2019-02-15 18:07:50
2	操作	添加	初始化用户	普通用户角色系统管理用户角色	BlockPolicyVO	添加屏蔽规则: 规则记录id=SEag8GgBfqyd3al3TcOm资产IP=nu II检测规则sid=902333201	2019-02-15 18:07:44
3	登录	登录成功	初始化用户	普通用户角色系统管理用户角色		登录成功	2019-02-15 17:01:07
4	操作	修改	初始化用户	普通用户角色。系统管理用户角色	AssetVO	修改被动发现资产开关状态:修改后状态为false;	2019-02-15 16:27:57
5	操作	修改	初始化用户	普通用户角色。系统管理用户角色	AssetVO	修改主动扫描资产开关状态: 修改后状态为false;	2019-02-15 16:27:53
6	操作	修改	初始化用户	普通用户角色。系统管理用户角色	AssetVO	修改主动扫描资产开关状态:修改后状态为true;	2019-02-15 16:27:18
7	登录	登录成功	初始化用户	普通用户角色。系统管理用户角色		登录成功	2019-02-15 16:19:39

报表管理

控制台、概览页管理

控制台、资产概览、漏洞概览、威胁概览四个概览页面,可以通过页面来管理数据图表的展示,点击编辑,进入相应概览页面的可编辑状态。

当前位置:系统管理/报表管理/Dashboard		
Dashboard 定时报表		
序号	Dashboard名称	操作
1	控制台	む 進入 区 編編
2	资产概范	の 進入 区 編輯
3	漏洞戦炎	∂ 进入 ☑ 編輯
4	威胁概定	ピ 進入 区 編編

进入到编辑状态后,点击选中的数据图表,可以将图表拖拽到任意位置,可以拉伸图表 的高度和宽度,重新对页面排版。重新排版后,顶部会出现保存、取消按钮,点击保存后, 所有修改生效,点击取消按钮,修改被重置,页面数据不变。

当前位置:报表管理/Dashboard管理/详情 漏洞模仿					保存	< 返回 取消 添加图表
漏洞趋势 現代	作 🗸 最近扫描的	傍				操作 >
1500	最近扫	描任务	漏洞总数	高危	中危	低危
	12	13	0	0	0	0
1000	te	st	0	0	0	0
F20	测试日	E第05	0	0	0	0
		E务04	141	47	42	29
0	测试行	6券03	172	47	49	40
- 低於 - 高於 - 中战	a mananemizi					
20031995057位 総統、点社: 12.0K 高統、点社: 45.7K 中秋、点社: 41.7K	ff ∨ 建酸间溴电型分 Amaz F	Y中 Ce con Linux本地安 产量 edora本地安全社	ntoo本地安全检查,占比: 政策,占比: 1.6% ;全检查,占比: 1.9% 始徵,占比: 5.2% 给查,占比: 25.0% 继冲联盟出,占比: 1.1% Web战用的安置用,占比	1.5X Ubuntu	AR 地名全省地路、古法: 3.6% Debian 基地会会检查。在法 週刊、古法: 10.1% SuSEX 地名全场会。在 Windows: Microso IE 地區等。在法: 3.7 Oracie Linux名 地会会检查。 Slackware X 地会会检查。 Slackware X 地会会检查。	展示 ∨ : 4.8% htt: 2.7% htt: 2.7% htt: 1.4% % htt: 1.3%

对页面的数据图表进行管理,可以添加图表、删除图表、编辑图表标题。





控制台																添加图表
\leftarrow	10 資	005 产总量	•	366 高危漏洞…	di	233 受攻击资产		0 失陷主机…	<mark>8⁰49</mark> 勒索\$	次件	● 15 恶意软件	0	<mark>9 29</mark> 漏洞利用…	٢	3524347 威胁总量	\rightarrow
安全态势	許分			操作 > 实	时地图							操作~	消息提示			操作 >
		THE REAL						-		1		编辑标题	10.1.3.123发现	其他		02-15
	SY		-				~					TEMPAK	10.1.1.233发现	其他		02-15
		中						- /		F			= 10.1.1.26发现	其他		02-15
		59.89								Sec.			= 10.1.3.195发现	其他		02-15
				-	_			1	131				= 10.1.3.69发现题	暴力破解		02-15
				-	-								。 10.1.3.178发现	lC&C通讯		02-15
					-											

编辑图表标题后,页面顶部出现保存、取消按钮,点击保存后,所有修改生效,点击取 消按钮,修改被重置,页面数据不变。

当前位置:报表管理/Dashboard管理/详情 资产概览	< 返回 保存 取消 法加密表	
资 ^{资法最最} 1010	原作 マ 新作 マ 新作 マ 新作 マ 新作 マ 1010 1	
^{资产组件信息} ? 确定保存吗?	##* > ### > ### > ### >	
	取消 确定 取消 确定	

添加图表,需要填写图表的标题、描述、选择数据来源、选择图表类型、是否自动刷新 等设置项。



新建图表				×
* 标题:				
描述:				
*选择数据来源:	资产 威胁	漏洞	其他	
	资产总量变化	开放端口数	资产总量	端口分布
	操作系统分布	资产归属统计	资产组件信息	
*选择图表类型:	请先选择数据来源			
* 自动刷新:	无	~		
				取消添加

删除图表, 会有弹窗提示是否真的删除。

?	确定删除吗?		
		取消	确定

定时报表

定时报表,用户可以根据实际需求,选择特定时间段生成报表,报表类型主要包括:日 报、周报、月报。定时报表的列表显示定时报表名称、描述、定时生成时间、创建时间、操 作项。支持定时报表的添加、编辑、删除,编辑查看报表详情。

当前位置: 3	系统管理/报表管理/定时报表				
Dashboar	rd 定时报表				
					添加
序号	定时报表名称	描述	定时生成时间	创建时间	操作
1	日报		日报 每天09:00:00	2018-11-29 14:39:34	区編輯 🗅 删除 \ominus 详情

创建一个新的定时报表,填写报表名称,选择报表类型、定时生成时间,保存。



添加定时报表		×
* 定时报表名称:	请填写定时报表名称	
描述信息:	描述信息	
* 定时报表类型:	日报 周报 月报	
* 定时生成时间:	请选择时间 ①	
	取	消保存

创建一个报表后,点击详情,进入报表内容编辑页面,新创建的报表没有图表,需要添 加图表。



添加图表,需要填写图表的标题、描述、选择数据来源、选择图表类型、是否动刷新等 设置项。



新建图表				×
* 标题:				
描述:				
*选择数据来源:	资产 威胁	漏洞	其他	
	资产总量变化	开放端口数	资产总量	端口分布
	操作系统分布	资产归属统计	资产组件信息	
▶选择图表类型:	请先选择数据来源			
* 自动刷新:	无	V		
				取消 添加

添加图表后,点击选中的图表,可以将图表拖拽到任意位置,可以拉伸图表的高度和宽度,重新对页面排版。重新排版后,顶部会出现保存、取消按钮,点击保存后,所有修改生效,点击取消按钮,修改被重置,页面数据不变。



可以删除图表、编辑图表标题、添加至其他报表。



编辑图表标题后,页面顶部出现保存、取消按钮,点击保存后,所有修改生效,点击取 消按钮,修改被重置,页面数据不变。

前位置:系统管理/报法管理/近时报表评符 <返回					
日报 目核 每天09:00:00	保存 取消 添加路表 历史文件 立即导出				
dSが明囲 Palo Alto PA-COS 地域でき位置 Windows Palo Alto PA-COS 地域でき位置 Unap VSS net Windows Palo Alto PA-COS 地域できた PALo Zava PALo	18代* V 成的使用 単位 V 目前代 V 日本 13.0% A Lik: 13.0% N 目前代 V 日本 13.0% N 目前代 V 日本 13.0% N 日本				
⑦ 确定保存吗? 取消 确定	 ? 确定取消吗? 取消后页面信息将会被重置 定 取消 确定 				

历史文件,就是此定时报表的生成记录。点击历史文件,可以看到生成列表,显示文件 名称、生成时间、生成状态,支持下载、删除操作。

当前位置:系統管理/报表管理/定时报表详情 日报 日期 每天09:00:00		< 返回 添加副志 历史文件 立即导出
成的月始 Palo Alto PAN-OS=地质企社会整 Nimap NSE net	操作 >	成防火型 最力能研, 点比: 13.0%
Windows HP-UX-Rise2e独自 RPC Oracle Linux-Rise2e独自 展门闩图频本		MAURIZ, čile: 13.0%
产能验验 IT-Coundschutz 服务的题 FTP - SMTPP2置		WEB以出,在社: 13.0% 王帝和14年,在社: 13.0%
0 100 200 300 400 500 600 700	008 C	C&C通讯,占比: 13.0% / 漏洞利用,占比: 2.7%

历史报表			Х
文件名称	生成时间	生成状态	操作
日报_20190321090001.pdf	2019-03-21 09:00:01	成功	下载 删除
日报_20190320090001.pdf	2019-03-20 09:00:01	成功	下載 删除
日报_20190319090001.pdf	2019-03-19 09:00:01	成功	下载 删除
日报_20190318090042.pdf	2019-03-18 09:00:43	成功	下載 删除
日报_20190317090042.pdf	2019-03-17 09:00:43	成功	下载 删除
日报_20190316090042.pdf	2019-03-16 09:00:43	成功	下载 删除
日报_20190315090042.pdf	2019-03-15 09:00:43	成功	下载 删除
日报_20190314090042.pdf	2019-03-14 09:00:43	成功	下载 删除
日报_20190313090042.pdf	2019-03-13 09:00:43	成功	下载 删除
日报_20190312090042.pdf	2019-03-12 09:00:43	成功	下载 删除
日报_20190311090042.pdf	2019-03-11 09:00:43	成功	下载 删除
日报_20190310090042.pdf	2019-03-10 09:00:43	成功	下载 删除
日报_20190309090042.pdf	2019-03-09 09:00:43	成功	下载 删除
日报_20190308090042.pdf	2019-03-08 09:00:43	成功	下载 删除
日报_20190307090042.pdf	2019-03-07 09:00:43	成功	下载 删除
共 115条 〈	1 2 3 4 5	6 7 8	> 跳至 〕
			关闭

天翼云 e Cloud

r

立即导出,就是立即生成定时报表,在历史报表列表可以马上看到记录,显示生成时间 是当前时间。可以下载、删除。

历史报表	Ę			Х
	文件名称	生成时间	生成状态	操作
	日报_20190321195121.pdf	2019-03-21 19:51:22	成功	下载 删除
	日报_20190321090001.pdf	2019-03-21 09:00:01	成功	下载 删除
	日报_20190320090001.pdf	2019-03-20 09:00:01	成功	下载 删除
	日报_20190319090001.pdf	2019-03-19 09:00:01	成功	下载 删除
	日报_20190318090042.pdf	2019-03-18 09:00:43	成功	下载 删除
	日报_20190317090042.pdf	2019-03-17 09:00:43	成功	下载 删除



4 操作指南

4.1 申请双网卡弹性云主机

开通态势感知服务需要开通 3 台双网卡弹性云主机,其中一台云主机为态势感知系统,最低 配置建议为 4 核 CPU/32G 内存/500G 硬盘。另外两台云主机为虚拟网关系统(主备双机),最 低配置建议为 2 核 CPU/2G 内存/50G 硬盘。弹性云主机的规格参数可以参考购买指南下的 2.1 规格

需要单独在天翼云控制中心下的虚拟私有云中去申请一个态势感知的子网。态势感知的网段 和防火墙、业务、负载均衡的网段不在同一个网段。如果有多余的网段,就不用再去申请。

开通态势感知弹性云主机

在天翼云官网下的控制中心下的弹性云主机中创建弹性云主机

≡	云主机控制台	弹	弾性云主机 ② 地区可以油酸193合云主机。他用77766-CFUEL515GBBA研, 7%配数研修							创建弹性云主机		
ම ස	总元	如果五生机一键式重要在网边能失生说,建议这教教网质重要加作开启一键重要在网边能。10月晚前期间受教知时?										
λΩ.	弹性云主机物理机服务		开机 关机 重重运得 更多 ▼				所有项目	∃ v	所有运行状态	* 名称	*	
	云硬盘		名称/ID	可用分区	秘密	规档/挽徽	IPItht			计模模式	企业项目	操作

态势感知云主选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品,请选择操作系统版本下拉选择态势感知-控制端(100GB)。



态势感知的 eth0 网段和业务是同一个网段, ip 地址可以自己手动分配或者自动分配 态势感知的 eth1 (扩展网卡) 网段是态势感知的网段,和业务不同网段。ip 地址可以自己手动 分配或者自动分配



安全组入方向中放行 22 端口以及 18443 端口,弹性 ip 的带宽建议 5M

弹性云主机	
网络	vpc-期就(192:168.0.0/16) ▼ C 自動分類内報論 ▼ 可用品用印题第247个 ①
	如常创建新的曲料私有资。影响前往这时有创建。
扩展网卡	◎ subnet-活動類型(192.168.400/*) 自我分類が知識 * 可用私用が設備247个
	 (2) (10年月年 동王可以第511年月年)
安全组	Syn-HullAccess (6/74649-8/417-4541-83an-93868ar7 ① C 新聞金金組 ① 国際研究指数全部回己提示2010 (Linux S24102) . 3359862 (Windows:ERER) REICHP 102 (Fing) . .
3世性1P	○ 不便用 ⑥ 自然分配 ○ 使用已有 ⑦ 回动力师告示主机分配指导带面的外担中, 金融网络开生的定期外担心和规则不是。
公阿带竞	「使用気は食食の 「洗量かが気は和豆の外活業 」 「加量から気は和豆の外活業 」 「洗量から気は和豆のか活業 」 「加量から気は和豆のか活業 」 日本の目的にはあた ・
带宽大小	1 2 5 10 100 200 自意文 - 5 + 再宽限: 1-2000 Mbb/s

设置密码并同意相关协议即可开通态势感知云主机,等待创建即可。

开通态势感知虚拟网关云主机

态势感知网关 eth0 的网段设置:

A. 网络环境中有云下一代防火墙。则态势感知网关的 eth0 网段和防火墙的外网出口(即防火墙做目的 NAT 的内网 ip)同一个网段。如果是多个外网出口的防火墙 ip,需要更改防火墙为同一个外出口。不清楚的请与态势感知厂家联系确认后联系防火墙厂家更改。

B. 网络环境中没有云下一代防火墙,有负载均衡器。则态势感知网关的 eth0 网段和负载均 衡器的 ip 同一个网段。

C. 网络环境中没有云下一代防火墙和负载均衡器,则态势感知网关的 eth0 网段和业务同一个网段。

D. 网络环境中有云下一代防火墙和负载均衡器,则态势感知网关的 eth0 网段和云下一代防火墙的外出口同一个网段。如果是多个外网出口的 ip,需要更改防火墙为同一个外出口。不清楚的请与态势感知厂家联系确认后联系防火墙厂家更改。

态势感知网关 eth1 网段是态势感知网段,和业务防火墙负载均衡不在同一个网段。

. 态势虚拟主网关选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品,请选择操作系统版本下拉选择态势感知-虚拟网关1(40GB)

ക					
AXA.	规格	最新系列 + vCPUs 2vCPUs	▼ 内存 4GB ▼ 規格名称	Q	
-		规结名称	vCPUs 内存 J三	基准/最大帶竅 ② ↓目	内网教发包 ⑦ ↓Ξ
0		s3Jarge.2	2vCPUs 4GB	0.12/0.5 Gbit/s	60,000
ē)		S6Jarge.2	2vCPUs 4GB	0.2/1.5 Gbit/s	150,000
Ð		図 c3.large.2 (已售額)	2vCPUs 4GB	0.6/1.5 Gbit/s	300,000
4		C6.Jarge.2	2vCPUs 4GB	1.2/4 Gbit/s	400,000
۲		颐 t6.Jarge.2 (已绘画)	2vCPUs 4GB	0.1/0.5 Gbit/s	100,000
		当前现格 適用型 s3.large.2 2vCPUs 4GB			
	19.9	公共協会 私有機会 共享機会	▼ C		

天翼口 e Cloud

> 态势感知主网关 eth0 网段根据网络环境中是否有云下一代防火墙、负载均衡器配置, eth1(扩展网卡)和态势感知是同一个网段。安全组入方向方向 22 端口,弹性 ip 带宽建议 5M

网络	vpc-動試(192.168.0.0/16) で G subnet-防火境(192.168.20.0/24) で 自動分配P地址 可用私有IP数量246个 ② 如需他建新的虚拟私有云,您可解往投制台锁温。 2 <td< th=""></td<>
扩展网卡	 Subnet-志频镭和(192.168.40.0/▼ 自动分割P地址 ▼ 可用站有PP数量247个
	④ 増加−块丙卡 怨还可以増加10块网卡
安全组	Sys-FullAccess (6f744ef9-8f47-45d1-83aa-938d8ac7 ● ▼ C 新建安全組 ⑦ 清确保所选安全組已認通22編口 (Linux SSH登录), 3389編口 (Windows返程登录)和 ICMP 协议 (Ping), 配置安全組規則 萬升安全組規則 へ
弹性IP	○ 不便用 ● 自动分配 ○ 使用已有 ⑦ 自动方每台云主机分配独享每宽的弹性PP。创建弹性与主机过程中,请确码弹性PP配顺允足,
公网带宽	按研究计表 ① 流量达大域故障定的场景
带宽大小	1 2 5 10 100 200 自定义 — 5 十 带宽范围: 1-2000 Mbit/s

设置密码并同意相关协议即可开通态势感知云主机,等待创建即可。

. 态势虚拟备网关选择的镜像在公共镜像下->请选择操作系统下拉选择安全产品,请选择操作系统版本下拉选择态势感知-虚拟网关2(40GB)

规格	最新原列 v vCPUs 2vCPUs	▼ 内存 4GB ▼ 現階名称	Q	
	規格名称	vCPUs 内存 J三	基准/最大印度 ⑦ ↓三	内间收发包 ⑦ 三
	s3.large.2	2vCPUs 4GB	0.12/0.5 Gbit/s	60,000
	S5.large.2	2vCPUs 4GB	0.2/1.5 Gbit/s	150,000
	図 c3.large-2 (已售職)	2vCPUs 4GB	0.6/1.5 Gbit/s	300,000
	Cő.large.2	2vCPUs 4GB	1.2/4 Gbit/s	400,000
	関 t6Jarge-2 (已告谢)	2vCPUs 4GB	0.1/0.5 Gbit/s	100,000
	当前现答 通用型 s3.large.2 2vCPUs 4GB			
28	公共编章 私有領導 共聚復會			
	 (e) 安金严品 ▼ 本勝極和-虚拟同关2(40GB) 	* C		

态势感知备网关 eth0 网段根据网络环境中是否有云下一代防火墙、负载均衡器配置, eth1(扩展网卡)和态势感知是同一个网段。安全组入方向放行 22 端口,弹性 ip 带宽建议 5M

网络	vpc-期試(192.168.0.0/16) マ C 目初分配P地址 可用私有PP数量246个 ⑦ 如需領護新約点與私有云、您可能往控制合物識。
扩展网卡	 ○ aubnet-态势感知[192.168.40.0/ ▼ 自动分散/P地址 ▼ 可用私有/P型量247个
	⑦ 増加−块网卡 総正可以増加 10 块网卡
安全组	Sys-FullAccess (6f744ef9-8f47-45d1-83aa-938d8ac7 ● C 新建安全組 ⑦ 谘詢保所选安全組已認過22調口 (Linux SSH登录), 3389鍋口 (Windows运程整录) 和 ICMP 协议 (Ping)。 配置安全組規則 展开安全組成則 へ
弹性IP	○ 不使用 ● 自助分配 ● 使用已有 ⑦ 目动为每台云主机分配股等带宽的弹性IP。创建弹栏云主机过程中,请确铝弹性IP配额充足。
公网带宽	按符究计费 ① 流温较大或级稳定的级最 近面小或流量波动较大场最
带宽大小	1 2 5 10 100 200 自定义 - 5 + 研究范围: 1-2000 Mbit/s

设置密码并同意相关协议即可开通态势感知云主机,等待创建即可。

4.2 申请虚 IP

双网卡弹性云主机开通完成后申请虚 IP,并且绑定虚拟网关系统。流程如下:

步骤一:在天翼云控制中心所有服务下的计算中找到弹性云主机,点击开通的弹性云主机。

(天異 Geode 在 制中心 服务列表 ▼ 收 載 ▼		
	所有服务 我的收藏		
	计算 ~	存储 ~	网络 ~
	() 弹性云主机(43) 弹性可扩展的计算服务器	云硬盘(98) 弹性可扩展的块存储	「□」」「「」」」「」」「「」」」 「「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「 「」 「」 「」 「 「」 「」 「」 「 「」 「」 「 「」 「」 「」 「 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「 「」 「」 「 「」 「」 「 「」 「 「」 「 「」 「 「」 「 「 「 「」 「 「 「 「」 「
	• 初理机服务 (1) 租户专届的物理服务器	专属存储(0) 专属存储服务	弹性负载均衡(4) 多台云服务器间目动流量分发
	○ 云容器引擎 高性範可扩展的容器服务	云主机备份(4) 安全、可靠的云主机备份	(PPN) VPN (2) 远程安全接入VPC网络
	 語: : <li:< li=""> <li:< li=""> : : :</li:<></li:<>	云硬盘备份(10) 安全可能的快存储备份	内网DNS 稳定、安全、快速的内网域名解析服务
	()))、 ()	对象存储服务 可扩展的云存储	(FPN) 云间高速(0) 跨资源池云主机高速互联
	(回) 专属云(1) 云中的专履进拟化资源池	弹性文件服务 弹性可扩展的文件服务	いれて网关(2) 高性能的公网网关

步骤二: 在态势感知网关弹性云主机网卡 eth0 选项中点击管理虚拟 IP 地址。特别注意: 这 里的 eth0 是和态势感知网段不同的那个网段。具体的网段是根据网络环境中是否有云下一代 防火墙、负载均衡器配置的,在最前面的就是 eth0 网卡。

く ecs-态势网关1	-)测试	────────────────────────────────────					
 名称 状态 ID 磁血 可用分区 郵托系称 企业项目 云主明組 	ecc-市務局決1-和武 選行中 Su2fetel-2c7-13-8-866-472ebc09100d 1ペ 可用区1 - 企 ① 面面通知た約 defutt - 股音元主利組	虚拟私由云 规格 簡章 同卡 创建时间 启动时间	×pc-別に 副用間 (sLarge-2) 2×CPUs 4GB 記録900 480/04251 2ぐ↑ 2020-03-30 10:25:38 GMT+08:00 2020-03-30 10:25:55 GMT+08:00				
三確血 第十 安全田 弾性P 編建 構造 諸医院や 電話可以認知の時時や							

步骤三: 在虚拟 IP 选项下申请虚拟 IP 地址, 可以自动分配或者手动分配。

子岡谷称 subnet-版大場 ↓ 岡裕田 4b8b3a9d-a9b2-4b31-9ee1-6ce611e72427 IPv4子剛D de33ca2d-6623-4c2t-8715-141530eafd03 IPv6子剛D 子冏IPv4段段 192.168.20.0/24 子冏IPv6段段开館IPv6 ⑦	 申请虚拟IP地址 当前子网 subnet-防火境 当前子列Pv4网段: 192.168.20.0/24 * 創建方式 自动分配 手动分配 	× 8 1.125.0.250,114.114.114.114 ✔ 重度 PetRe 2.168.20.1				
已用IP地址 虚拟IP 服务器 标签 申请虚拟IP地址 解绑弹性IP	納定 取消		虚拟IP地址	~	Q	C
虚拟IP地址	绑定的弹性IP	鄉定的服务器 (网卡)		操作		
192.168.20.82	140.246.21.119	ecs-态势网关1-测试 (192.168.20.185) 查看全部 (2)		解绑弹性IP 绑定服务器 更多	5 -	

完成虚拟 IP 申请后,在操作选项下的绑定服务器中绑定 2 台虚拟双网关云主机。一次只能绑 定一台态势感知网关,操作两次即可。弹性 ip 先暂时不绑定。后面网络配置的时候配合态势 感知技术人员操作绑定。

子网名称 网络ID IPv4子网ID IPv6子网ID	subnet-防火墙 》 4b8b3a9d-a9b2-4b3 de33ca2d-6623-4c2	绑定的服务器			名称	•	Q	× C	.,《 重置					
子网IPv4网段	192.168.20.0/24	名称	类型	状态	私有IP地址	企业项目	操作							
子网IPv6网段	开启IPv6 ⑦	ecs-态势网关2-测试	弹性云主机	⊙ 运行中	192.168.20.12	2 default	解绑							
		ecs-态势网关1-测试	弹性云主机	● 运行中	192.168.20.18	5 default	解绑							
已用IP地址	虚拟IP 服务器							- 1						
申请虚拟IP	地址 解绑的单性IP									虚拟IP地址	-		Q	C
虚拟日	P地址		绑定的弹性IP			绑定的服务器 (网卡)					操作			
192.1	68.20.82		140.246.21.119	9		ecs-态势网关1-测试 (1 查看全部 (2)	192.168.20.185)				解绑的单性IP	绑定服务器	更多 ▼	

4.3 订购态势感知基础版/高级版

通过天翼云控制中心下的安全选项下的态势感知进入订购态势感知授权页面,订购页面如 下,填写对应的信息。态势感知网络配置的场景(场景 A: VR 做为 NAT 网关,直挂业务主 机。需要提供业务主机的端口映射关系表。场景 B: VR 下挂负载均衡。场景 C: VR 下挂防火 墙,外部访问业务流量经过防火墙,业务主动访问外部流量不经过防火墙。场景 D: VR 下挂 防火墙,外部访问业务流量经过防火墙,业务主动访问外部也经过防火墙。)态势感知的机器



态势感知							
购买质知	1、态势感知系统需与弹性云主机配含购买,共需3台弹性云主机,其中1台用于部署态势感知系统,2台用于部署虚拟网关系统(双机备份)。 2、本页面订购的是产品提权,请确保已完成部署再行订购。一经订购立即生效,除不可抗力因素之外,不支持退订。						
订购规格:	就如素 高级版						
	功能調筆:						
	✓ 智能完量分发 ✓ DPI完量解析 ✓ 协议识别 ✓ 网络资产发现 ✓ 网络资产管理 ✓ 资产能能性检测						
实例名称	ctsa2-3fis						
	请真型头的S称						
最大授权委	- 1 +						
	服务台散总和,综可调整到预期增加例的规权数,不支持减小 部署态势够知论元主机建议为最低配置为:4核CPU 32G内存 500G硬直;部署虚印风关语像的云服务最低配置:2核CPU/2G内存/50G硬盘						
机器码:							
	这时态势够知经的明。登录页面库可重着经权机器机、计信况(态势够知用户使用指编)						
虚拟IP:							
	需要为必别感知家统中语一个虚拟P,要求虚拟P与重业务系统在四一网段。参照 (企务感知用PA发用组成)						
待监控云日	EðUP:						
业务本王朝	UP: 季联态为感知系统应示主机的内阁印地址。此处要求是取得七主机,际以需要真常2个内阁印地址。2个印地址用英文谱号分编。						
购买时长:	日 6 今日 1 fm 2 fm 3 fm						
	17.17.1 14F 24F 34F						
	71 (25/2019/01)						

在订购完成后会有态势感知技术人员联系对接网络配置,请确保联系方式顺畅。

4.4 虚拟网关配置

确保态势感知网关的安全组放行 22 端口,三台态势感知云主机网卡下关闭源/目的检查。虚 拟网关的配置需要配合态势感知技术工程师。由态势感知技术工程师配置。

Z	云硬盘 <mark>月</mark> 卡 安全组 弹性IP 监控 标签							
添	加网卡 您还可以增	20.0 10/94-1-						
^	192.168.20.185				切换VPC 修改私有IP 管理虚拟IP地址 更改			
Γ	名称 冈-+ ID 状态 弹性IP SC型斑 圆/目的检查	 cx2cdc12-5scf-4789-483df-125d3aof0fe7 @ 2018 Xy/F TURKCOST @ 0	子网 私有IP地址 IPv6地址 建筑IP地址 MAC地址	subnet-82X88 (192.168.20.0/24) 192.168.20.185 192.168.20.82 (a16:3e:52.60.69				
^	192.168.40.100				切换VPC 管理虚拟IP地址 更改			
Γ	名称 同十 ID 状态 弹性IP 安全组 週/目的检查	 e262240f-64(8-49e4-aa7f-6292a1da2206 ◎ 第2% 	子网 私有1P地址 IPv6地址 虚祝IP地址 MAC地址	subnet-#\$\$\$\$\$20 (192.168.40.0/24) 192.168.40.100 fa:16:3e:7b:69:24				

4.5 网络配置

场景 A

天翼云 e Cloud

VR 作为 NAT 网关,直接下挂业务场景,网络配置步骤:

步骤一:在天翼云控制中心所有服务中点击网络下的虚拟私有云。

CCC 天房石・ 控制中心 服务列表 v 改憲 v		
所有服务 我的收藏		
计算 ~	存储 ~	网络 ~
一 弹性云主机(43) 弹性可扩展的计算服务器	云硬盘(98) 强性可扩展的块存储	「」」」 虚拟私有云 (11) 全纪周期的虚拟网络
• 物理机服务(1) 租户专属的物理服务器		弹性负载均衡(4) 多名云服务器间目动流量分发
◎ 云音器引擎 ◎ 10 高性能可扩展的容器服务	云主机备份(4) 安全、可能的云主机备份	VPN (2) 远程安全接入VPC网络

步骤二:在虚拟私有云中找到对应开通的3台云主机网段,点击进入。

	控制	中心 服务列表 ▼ 収蔵 ▼					• 贵州 ▼
\bigcirc		虚拟私有云 ③					
网络控制台					所有项目 🔻	名称	•
总览		名称	IPv4网段	状态		子网个数	企业项目
虚拟私有云		TEST-2	192.168.1.0/24	可用		2 个	default
访问控制	~	ipv6test	192.168.0.0/16	可用		1个	default
弹性公网IP和带宽	~	demoVPC	192.168.0.0/16	可用		3 个	default
NAT网关		vpc-workspace	192.168.0.0/16	可用		7个	default
弹性负载均衡	~	vpc-dualstack-zzy	192.168.0.0/16	可用		1个	default
对等连接		vpc-646b	192.168.0.0/16	可用		1个	default
虚拟专用网络		vpc-ad63	192.168.0.0/16	可用		1个	default
云专线	~	vpc-sldtest	192.168.0.0/16	可用		3 个	default
弹性云服务器	s	TEST-GPH	192.168.0.0/16	可用		2 个	default
		vpc-b3b3	192.168.0.0/17	可用		1个	default
		10 - 总条数:11 < 1 2 >					

步骤三: 点击路由表选项下添加路由信息, 配置路由, 下一跳的 IP 地址为虚拟 IP 地址

そ第二・	控制中心 服务列表 ▼ 收藏 ▼		
Ø	虚拟私有云 、vpc-sidtest		
网络控制台	谷标 vpc-sldtest ✔ ID 7bd993f9-f5be-46cf-be0e-585a1a07d50f 添加路由信息	× 用 12.168.0.0/16 <i>\$</i>	
虚拟私有云	子网个数 3个 目的地址 例如: 192.168	3.1.0 / 0 ⑦	
访问控制	✓ 子网 路由表 拓扑图 标签 下→跳地址 例如: 192.168	3.1.1 ②	
弹性公网IP和带宽	➤ 自定义路由表		
NAT网关	添加路由信息	取消	
弹性负载均衡	Y 目的地址 下一跳地址	操作	
对等连接	0.0.0.0/0 192.168.1.100	修改 删除	

场景 B

e oud

VR 下挂负载均衡器场景,网络配置步骤:

步骤一:在天翼云控制中心所有服务中点击网络下的虚拟私有云。

CCC F開石・ 控制中心 服务列表・ 収職・		
所有服务 我的收藏		
计算 ~	存储 ~	网络 ~
3 3 增佳 云主 机 (43) 3 弹性 可扩展的计算服务器	云硬盘(98) 弹性可扩展的块存储	[w] 虚拟私有云 (11) 安全隔离的感以网络
• 物理机服务(1) 租户专属的物理服务器	を属存储(0) を属存储(8)	3時住负载均衡(4) 多台云服务器间自动流量分发
(1) 云容韻引擎 (2) 高性範可扩展的容離服务	云主机备份(4) 安金、可靠的云主机备份	(FPR) (2) 远程安全接入VPC网络

步骤二:在虚拟私有云中找到对应开通的3台云主机网段,点击进入。

Co 天賀石・	控制	中心 服务列表 ▼ 収慮 ▼					• 贵州 ▼
\bigcirc		虚拟私有云 ⑦					
网络控制台					所有项目 🔻	名称	•
总览		名称	IPv4网段	状态		子网个数	企业项目
虚拟私有云		TEST-2	192.168.1.0/24	可用		2 个	default
访问控制	~	ipv6test	192.168.0.0/16	可用		1个	default
弹性公网IP和带宽	~	demoVPC	192.168.0.0/16	可用		3 个	default
NAT网关		vpc-workspace	192.168.0.0/16	可用		7个	default
弹性负载均衡	~	vpc-dualstack-zzy	192.168.0.0/16	可用		1个	default
对等连接		vpc-646b	192.168.0.0/16	可用		1个	default
虚拟专用网络		vpc-ad63	192.168.0.0/16	可用		1个	default
云专线	~	vpc-sldtest	192.168.0.0/16	可用		3 个	default
弹性云服务器	s	TEST-GPH	192.168.0.0/16	可用		2 个	default
		vpc-b3b3	192.168.0.0/17	可用		1个	default
		10 ▼ 总条数:11 < 1 2 >					

步骤三:点击路由表选项,配置路由,下一跳的 IP 地址为虚拟 IP 地址

	で見ている	中心 服务列表 ★ 收藏 ★	♥ 贵州
	(\mathcal{P})	虚拟私有云 [,] vpc-sidtest	
	网络控制台	Silver vpc-sldtest vpc-sldtest vpc-sldtest vpc-sldtest アbd9939-f5be-46cf-be0e-585a1a07d50f 添加路由信息 本 市 2,168.0.0/16 vpc-sldtest 本 市 2,168.0.0/16 vpc-sldtest 和 Compared Silver Silver	
l	虚拟私有云	子所介板 3 个 目的地址 例如: 192.168.1.0 / 0 ⑦ Hault	
	访问控制	子网 路由表 拓扑图 标签 下→跳地址 例如: 192.168.1.1 ②	
l	弹性公网IP和带宽	自定义路由表	
	NAT网关	添加路由信息	
	弹性负载均衡	目的地址 下一跳地址 操作	
	对等连接	0.0.0.0/0 192.168.1.100 修改 删除	

场景 C

VR 下挂防火墙,外部访问业务流量经过防火墙,业务主机主动访问外部不经过防火墙,网络 配置步骤:

步骤一:在天翼云控制中心所有服务中点击网络下的虚拟私有云。

を Cloud ・ 控制中心 服务列表 ・ 収藏 ・		
所有服务 我的收藏		
计算 ~	存储 ~	网络 ~
弹性云主机(43) 弹性可扩展的计算服务器	云硬盘 (98) 弹性可扩展的块存储	[w] 虚拟私有云 (11) 一 安全隔高的虚拟网络
• 物理机服务 (1) 租户专属的物理服务器	专属存储(0) 专属存储服务	计计算机 (4) 多台云服务器间自动流量分发 书目 音
○ 云容翻引擎 ○○○ 高性知可扩展的容器服务	云主机备份(4) 安金、可是的云主机备份	(PPN (2) 远程安全规入VPC网络

步骤二:在虚拟私有云中找到对应开通的3台云主机网段,点击进入。

用户使用指南

	控制	中心 服务列表 ▼ 收藏 ▼					♀ 贵州 ▼
\bigcirc		虚拟私有云 ③					
网络控制台					所有项目 🔻	名称	•
总览		名称	IPv4网段	状态		子网个数	企业项目
虚拟私有云		TEST-2	192.168.1.0/24	可用		2 个	default
访问控制	~	ipv6test	192.168.0.0/16	可用		1个	default
弹性公网IP和带宽	~	demoVPC	192.168.0.0/16	可用		3 个	default
NAT网关		vpc-workspace	192.168.0.0/16	可用		7个	default
弹性负载均衡	~	vpc-dualstack-zzy	192.168.0.0/16	可用		1个	default
对等连接		vpc-646b	192.168.0.0/16	可用		1个	default
虚拟专用网络		vpc-ad63	192.168.0.0/16	可用		1个	default
云专线	~	vpc-sldtest	192.168.0.0/16	可用		3 个	default
弹性云服务器	s	TEST-GPH	192.168.0.0/16	可用		2 个	default
		vpc-b3b3	192.168.0.0/17	可用		1个	default
		10 - 总条数:11 〈 1 2 〉					

步骤三:点击路由表选项,配置路由,下一跳的 IP 地址为虚拟 IP 地址

CCC 天翼石・	控制中心 服务列表 ▼ 收藏 ▼		♀ 贵州
Ø	虚拟私有云 〉vpc-sidtest		
网络控制台	谷称 vpc-sldtest ♪ ID 7bd99319-f5be-46cf-be0e-585a1a07d50f 700-0年 2 ▲	× 用 2.168.0.0/16 ダ	
虚拟私有云	T 6 X211241T	目的地址 例如: 192.168.1.0 / 0 ⑦	
访问控制	✓ 子网 路由表 拓扑图 标签	下一跳地址 例如: 192.168.1.1 ⑦	
弹性公网IP和带宽	◇ 自定义路由表		
NAT网关	添加路由信息	确定 取消	
弹性负载均衡	> 目的地址	下一段地址	操作
对等连接	0.0.0.0/0	192.168.1.100	修改删除
虑拟专用网络			

步骤四: 防火墙所在的网卡上关闭 源/目的检查

員 Cloud

	控制中心 服务列表 * 收贏 *		♀ 贵州
	25		une slitteet
云主机控制台	 ロ(CE(1230)ス場。 状态 运行中 	规格	通用入门型 t6.large.1 2vCPUs 2GB
急覽	ID 7d310283-6df1-443d-9cfd-1ba1c32ebf94	镜像	yunfanghuoqiang
弹性云主机	磁盘 1个	図卡	1个
云主机备份	可用分区 可用区1	创建时间	2019-08-06 17:14:42 GMT+08:00
物理机服务	委托名称 🖉 ③ 新建委托名称	启动时间	2019-08-06 17:14:55 GMT+08:00
云硬盘	企业项目 default		
云硬盘备份	云主机组 查看云主机组		
镜像服务			
弹性伸缩 >			
弹性负载均衡 (外网)	添加网卡 您还可以增加 0 块网卡		
密钥对	▲ 192.168.1.8		
云主机组			
	网卡ID 6c44ad9d-10f0-4bb7-9c49-f67a1a788026	子网	subnet-1.0 (192.168.1.0/24)
	状态 💿 激活	私有IP地址	192.168.1.8
	弹性IP	IPv6地址	
	安全组 quantong	虚拟IP地址	
	源/目的检查 〇一 ③	MAC地址	fa:16:3e:37:87:68



步骤五: 防火墙上的 IP 地址需要更改为静态 IP 地址

	下一代防火墙 _{ECFW}	首页	威胁监控中	中心 监控 別	链 对象	网络	系统						2
	夠 安全域	+ 新建 ~ ✔ 编辑	一 删除										
I	□ 接口	□ 接口名称	状态	获取类型. IP/掩码	IPv6/前缀长度	MAC	安全域	虚拟系统	接入用户/IP数	上行	速率	下行速率	功
+	DNS	ethernet0/0	@ @ @ E	thernet 接口						×	Mbps	204.94 K	
+	④ 路由	vswitchif1	Q. Q. Q.	基本配置 IPv6 配置	属性 高	级					0 bps	0 bps	
	◎ 应用层网关		_	基本配置									
+ .	臺 全局网络参数			接口名称:	ethernet0/0								
				描述:			(0 - 63)字符						
				绑定安全域:	○ 二层安全域	◉ 三层安全:	域 〇 TAP	○ 无绑	定				
				安全域:	trust	\sim							
				HA同步:	□ 启用								
				IP配置									
				类型:	● 静态IP	() 自	动获取						
				IP地址:	192.168.1.8								
				子网掩码:	255.255.255.0								
				□ 配置为Local IP									
				管理方式									
				Telnet SSI	H 🖂 Pina		HTTPS D S	SNMP					

步骤六: 防火墙上的网络配置, 在防火墙上面添加默认路由 0.0.0.0/0 下一跳为 VR 的虚 IP 地址

云下	一代防火墙	ECFW										网	络		
ĉ	安全域		+	新建。	/ 编辑 — 删除	ý.									
Ē	接口			状态	IP/掩码	下一跳	类型	下一跳网关/虚排	\$ 下一	跳接口	协议		时间表	优先权	度量
+ ONS	DNS				0.0.0/0	网关		192.168.1.100	ethe	rnet0/0	静态			1	0
- (***	路由				192.168.1.0/	接口			ethe	rnet0/0	直连			0	0
					192.168.1.8/	接口		- W7 898	ethe	rnet0/0	主机			0	0
	目的路田						日的路日	出記直							~
	目的接口路由						目	的地:	0	0.0.0					
	源路由						子	网掩码:	C)					
	源接口路由						下	—跳:	(◎ 网关			○ 当前系	统虚拟路由器	
52	应用层网关								()接口					
	12 DAMA						20	关:	1	92.168.1	.100				
+ 30	全局网络参数						B रा	间表:	-			\sim			
							优	先权:	1				(1-255), 缺	省值: 1	
							路	由权值:	1				(1-255), 缺	省值: 1	
							Та	g值:					(1 - 42949672	95)	
							描	述:					(1 - 63)字符		
														确定	取消

步骤七:去掉防火墙绑定的弹性公网 IP 地址,通过 VR 虚 IP 绑定的弹性 IP 来访问防火墙。 端口为 10443,<u>https://VIP</u>对应的弹性 IP:10443

← → C ▲ 不	安全 140.246.158.130:10443/#	homepage									z	2) (
云下一代防火墙	ECFW 首页	威胁监控中心	监控	策略	对象	网络	系统			A ec	:fwadmin@roo	t	
										个性化 周	」新间隔: 5%	计	
系统信息					c –×	许可证						с –	·×
序列号: 主机名称: 硬件平台: 系统时间: 私状态: 软件版本: 启动文件: 病毒过滤特征库:	0010060380659654 ECFW-6000 編辑 ECFW-6000-VM01 2019/9/26 星閉四 09:17:34 47 分钟 46 秒 Standalone 編辑 Version 5.5 ECFW6000-6.5R8P2.3-v6 2011 2.1.190920 2019/09/20 00:52:4	编辑 3/12/13 15:12:50 54 升级				客户 天翼云 天翼云 天翼云 天翼云 试用授权 试用授权		类型 URL DB 应用特征库 入侵防菌 病毒过滤 SCVPN IPSEC VPN QoS 云沙箱 平台 虚拟CPU 僵尸网络C&	有效时间 永久有效、升极有效期20 永久有效、升极有效期20 永久有效,升极有效期20 术及取制余60天。 未授权 有效期制余55天。 未授权 有效期制余55天。 未授权 未授权	19/11/26(喇索61天 19/11/26(喇索61天. 19/11/26(喇索61天 19/11/26(喇索61天	其他信息 可购买延6 可购买延6 可购买延6	R服务延. R服务延. R服务延.	
威胁视图			最近一天	×	G -×	总流量				最近一天	×	с –	·×
∲ 成助 	<mark>0</mark> بر	<mark>0</mark> Ф		 任		1.5k (sd) 비행 500 0	09/25 12:00	09/25	18.00 09/2	16	09/26 06:00	Ν	

场景 D

天翼**云** e Cloud

VR 下挂防火墙, VM 内外流量均经过防火墙, 网络配置步骤:

步骤一:将防火墙上的 IP 地址更改为静态 IP

云下一代防火墙 _{ECFW}					网络						۶
	┣ 新建 ~ 🖋 编辑	— 删除									
□ 接口 □	接口名称	状态 获取3	类型。IP/掩码	IPv6/前缀长度	MAC	安全域	虚拟系统	接入用户/IP数	上行速	率 下行速率	功
+ 🔤 DNS	ethernet0/0	👲 💿 💿 Ethernet	接口						XIM	ops 204.94 K	
+ 😳 路由	vswitchif1	👤 🔍 👷 📕 基本配	置 IPv6 配置	属性 高级	级				0	bps 0 bps	,
B 应用层网关		基本	配置								
+ 译 全局网络参数		拍	8口名称:	ethernet0/0							
		ħ	i述 :			(0 - 63)字符					
		ti ti	8定安全域:	○ 二层安全域	◉ 三层安全域	₫ O TAP	〇 无维	『定			
		3	2全域:	trust	\sim						
		H	IA同步:	□ 启用							
		IP配	置								
		ġ	*型:	静态IP	() 自行	动获取					
		IF	9地址:	192.168.1.8							
		9	一网掩码:	255.255.255.0							
			配置为Local IP								
		管理	方式								
			Telnet SSI	H 🖂 Pina	□ HTTP	M HTTPS MS	SNMP				

步骤二:防火墙网络配置上添加默认路由 0.0.0.0/0 下一跳地址为 VR 虚 IP 地址



云下一代防火墙 _{ECFW}	首页 履	成胁监控中心 监控	策略 对象	网络 系统	
 · · · · · · · ·	 + 新建 / 编辑 一冊 試态 IP/種码 ✓ ▲ 0.0.0.0/0 ▲ 192.168.1.0/. ▲ 192.168.1.8/. 	下一跳类型 下一跳网关// 网关 192.168.1.10 . 接口 . . 接口 . 目的路由配置	虚拟 下一跳接口 协议 00 ethernet0/0 静态 ethernet0/0 直连 ethernet0/0 主机	时间表 优先机 1 0 0	双 度量 0 0 0 ×
目的接口路由 源路由 源接口路由 180 应用层网关 + 译 全局网络参数		目的地: 子网掩码: 下一跳: 网关: 时间表: 优先权: 路由权值: Tag值: 描述:	0.0.0.0 0 例关 分接口 192.168.1.100 1 1 1	 当前系统虚拟路部 (1 - 255), 缺省值: 1 (1 - 255), 缺省值: 1 (1 - 4294967295) (1 - 63)字符 625 	由器

步骤三:去掉防火墙绑定的弹性公网 IP 地址,通过 VR 虚 IP 绑定的弹性 IP 来访问防火墙。 端口为 10443, <u>https://VIP 对应的弹性 IP:10443</u>

← → C ▲ 不	安全 140.246.158.130:10443/#home	epage								ž	2) (
云下一代防火墙	ECFW 首页 威胁)监控中心 🔹	监控 策略	对象	网络	系统			٩ م	cfwadmin@roo		
									个性化	创新间隔: 55	钟	
系统信息				c -×	许可证						c -	- ×
序列号: 主机名称: 硬件平台: 系统时间: 系统运行时间: 以以态: 软件版本: 启动文件: 病离过滤特征库:	0010060380659654 ECFW-6000 編輯 ECFW-6000-VM01 2019/9/26 星期四 09:17:34 創 47 分钟 46 秒 Standalone 編輯 Version 5.5 ECFW6000-5.5R6P2.3-v6 2018/12/12 2.1.190920 2019/09/20 00:52:54	启辑 3 15:12:50 升级			客户 天赋云 天赋赋云 天赋赋云 式用授权 试用授权		类型 URL DB 应用特征库 入侵防御 病毒过滤 SCVPN QoS 云沙箱 平台 虚拟CPU 僵尸网络C&	有效时间 永久有效,升级有效限2011 永久有效,升级有效限2011 永久有效,升级有效限2011 永久有效,升级有效限2011 有效期剩余60天。 未废权 有效期剩余55天。 未废权 有效期剩余55天。 未废权 未废权	//11/26(開余61天, //11/26(開余61天, //11/26(開余61天, }/11/26(開余61天,	其他信息 可购买延6 可购买延6 可购买延6	^{米服务延} ^{展服务延} ^{展服务延}	
威胁视图		最	后一天 🗸	G -×	总流量				最近一天	~	C -	- ×
☆ 成語 	<u>0</u> 商	о Ф	 55		1.5k 1.5k 1k 60 8H 500 0	09/25 12:00	09/25	18.00 09./26		09/26 06:00	Ν	

步骤四: 防火墙网卡上关闭 源/目的检查

cloud				用户使用指南
	空制中心 服务列	表▼ 收職▼		● 豊州
	名称	cncert_云防火墙 🖉	虚拟私有云	vpc-sldtest
云主机控制台	状态	运行中	规格	通用入门型 t6.large.1 2vCPUs 2GB
总资	ID	7d310283-6df1-443d-9cfd-1ba1c32ebf94	镜像	yunfanghuoqlang
· 通供云主机.	磁盘	1个	网卡	1个
云主机备份	可用分区	可用区1	创建时间	2019-08-06 17:14:42 GMT+08:00
物理机服务	委托名称	🖋 ③ 新建委托名称	启动时间	2019-08-06 17:14:55 GMT+08:00
云硬盘	企业项目	default		
云硬盘备份	云主机组	查看云主机组		
镜像服务				
弹性伸缩 >	云硬盘	网卡 安全组 弹性IP 监控 标签		
弹性负载均衡 (外网)	添加网卡	您还可以增加 0 块网卡		
密钥对	192.1	68.1.8		
云主机组				
	网卡 ID	6c44ad9d-10f0-4bb7-9c49-f67a1a788026	子网	subnet-1.0 (192.168.1.0/24)
	状态	⑧ 激活	私有IP地址	192.168.1.8
r	弹性IP		IPv6地址	
	安全组	quantong	虚拟IP地址	
	源/目的检查		MAC地址	fa:16:3e:37:87:68

步骤五:在天翼云控制中心所有服务中点击网络下的虚拟私有云。

記

Coloud · 控制中心 服务列表 v 收藏 v		
所有服务 我的收藏		
计算 ~	存储 ~	网络 ~
3弹性云主机(43) 弹性可扩展的计算服务器	云硬盘 (93) 弹性可扩展的块存储	ですう 虚拟私有云 (11) 安全病面的感知网络
• 物理机服务(1) 租户专属的物理服务器	を属存储(0) を属存储(8)	3射性负载均衡(4) 多台云服务器间自动流量分发
の 云容器引擎 (中国) 高性能可扩展的容器服务	云主机备份(4) 安金、可率的云主机备份	(JPN) (2) 這程安全線入VPC网络

步骤六:在虚拟私有云中找到对应开通的3台云主机网段,点击进入。

	控制	制中心 服务列表▼ 收藏▼					♀ 贵州 ▼
\bigcirc		虚拟私有云 ^②					
网络控制台					「「有面目」▼	名称	*
总览		名称	IPv4网段	状态		子网个数	企业项目
虚拟私有云		TEST-2	192.168.1.0/24	可用		2 个	default
访问控制	~	ipvőtest	192.168.0.0/16	可用		1个	default
弹性公网IP和带宽	~	demoVPC	192.168.0.0/16	可用		3 个	default
NAT网关		vpc-workspace	192.168.0.0/16	可用		7个	default
弹性负载均衡	~	vpc-dualstack-zzy	192.168.0.0/16	可用		1个	default
对等连接		vpc-646b	192.168.0.0/16	可用		1个	default
虚拟专用网络		vpc-ad63	192.168.0.0/16	可用		1个	default
云专线	~	vpc-sldtest	192.168.0.0/16	可用		3 个	default
弹性云服务器	ſ	TEST-GPH	192.168.0.0/16	可用		2 个	default
		vpc-b3b3	192.168.0.0/17	可用		1个	default
		10 🔻 总条数:11 < 1 2 >					

步骤七:点击路由表选项,配置路由,下一跳的 IP 地址为防火墙静态 IP 地址

天翼 Coloud			用户使用指南
网络控制台	名称 vpc-sldtest ID 7bd993f9-f5be-46cf-be0e-585a1a07d50f 子网个数 3个	状态 VPC网段 企业项目	正常 192.168.0.0/16 🖋 default
总览	子网 路由表 拓扑图 标签		
虚拟私有云	自定义路由表		
访问控制 ~	添加路由信息 您还可以申请99个路由信息。		
弹性公网IP和带宽 ~	目的地址	下一跳地址	操作
NAT网关	0.0.0.0/0	192.168.1.8	修改删除
弹性负载均衡 ~			

4.6 部署完毕

部署完毕并测试。设备重启大约数分钟后便完成部署。测试、首先在分析器看是否有流 量、是否可以进行分析。

其次在控制台将一台 Vrouter 关闭,看业务是否受影响,如不受影响,将该 Vrouter 开 启(必须要确认已经启动、最好启动后等待 5 分钟),再关闭另一台测试,业务是否正常。 Vrouter 采用透明传输方式,不影响在负载均衡器和防火墙上的设置。



5 常见问题

Q:态势感知产品有哪些规格?

态势感知产品根据提供的功能不同分为两个版本:基础版、高级版。

Q:为什么检测口没有流量?

- 1)确认在虚拟路由已经进行了镜像,且能看到流量;
- 2) 确认接入系统的端口是设置了检测口;
- 3) 确认 thinkflow 组件是否正常运行;
- 4) 查看 thinkflow 日志;
- 5) 根据日志信息再进一步排障。

Q:为什么威胁检测没有数据?

- 1) 确认检测口是否有数据;
- 2) 确认知识库是否正常加载。

Q:为什么信誉库没有同步?

- 1) 确认同步开发是否开启;
- 2) 确认同步配置是否设置正确;
- 3)确认与信誉库平台连接是否正常。