

Check Point R81 基于阿里云部署手册

上海溪盘科技有限公司 2022.10

©2022 SHANGHAI SHONE TENCHNOLOGY CO., LTD. All rights reserved





第一章 概述

- 1.1 产品介绍
- 1.2 安装要求及注意事项

第二章 购买实例的相关参数

- 2.1 新建主机
- 2.2 选择地域与机型
- 2.3 选择镜像
- 2.4 选择存储和带宽
- 2.5 设置安全组和主机
- 2.6 确认配置信息

第三章 配置主机网络

3.1 使用新密钥登录主机

第四章 Gaia(底层系统)初始化

4.1 登陆 Gaia 系统并配置

第五章 通过 SmartConsole 配置防火墙的相关功能

- 5.1 下载并安装 SmartConsole 客户端
- 5.2 Get 底层的拓扑及接口地址信息
- 5.3 定义接口域并关闭接口地址防欺骗功能
- 5.4 编辑策略
- 5.5 开启内网段的 SNAT
- 5.6 下发策略并生效



1.1 产品介绍

Check_Point_CloudGuard 提供行业领先的威胁防护安全保护,以确保即使遭遇最复杂的攻击,也能保障腾讯公有云和混合云网络的安全。完全集成式安全保护包括:

- 1. **防火墙、入侵防护系统 (IPS)、防病毒**和**防僵尸网络**技术保护云中服务免遭未授权访问, 并阻止攻击
- 2. 应用程序控制帮助阻止应用程序层拒绝服务 (DoS) 攻击,并保护混合云服务安全
- 3. 移动访问允许移动用户使用具有双重身份验证和设备配对的 SSL 加密连接, 连接到混合云
- 4. 数据丢失防护保护敏感数据免遭窃取或意外丢失
- 5. SandBlast 零日保护沙盒技术提供最高级的保护,防范恶意软件和零日攻击本地和混合云基 础设施的集中化管理通过单一控制台对云和本地安全进行集中配置与监控,统一安全策略管 理,达到所有公司数据安全轨迹的一致性。与来自物理基础设施的日志记录一样,混合云工 作负载流量会被记录,并可在同一仪表板中轻松查看。这可确保跨混合云和物理网络应用适 当级别的保护。
- 6. 整合性日志记录和报告 Check Point 跨云和本地网络整合监控、日志记录和报告功能。可针 对云工作负载流量生成安全报告,以跟踪整个混合云网络的安全合规性,从而简化报告和审 核流程。通过单个仪表板集中安全管理的各个方面,如策略管理、日志记录、监控、事件分 析和报告,安全管理员可全面了解整个组织的安全状态。

1.2 安装要求及注意事项

■ 购买主机的配置要求**建议选择 4 核 CPU,内存最低 16G**(因为系统是 64 位系统, 建议给 4G 内存)。

产品授权方式分为试用版本和正式版本,镜像本身默认提供给用户 15 天的试 用期,在此期间所有的功能都可以正常试用。试用期过后如果没有新的授权,所有 的功能均不能使用。正式版本需要您购买相应的许可服务。

SOFTWARE TECHNOLOGIES LTD.

第二章 购买实例的相关参数

2.1 新建主机

☰ (-) 阿里云 ♠ エ	作台			Q 搜索	费用	工单 ICP 备案 企业 支持 🗜
云服务器 ECS	云服务器 ECS / 概览					
概范	概覧 资源搜索	资源报表 功能概览				
事件						
标签	我的资源					号出数据 > 🛛 🖒
自助问题排查	云服务器	运行中	即将过期②	已过期	近期创建 ②	快照
发送命令/文件 (云助手)	0	0	0	0	0	230.24 _{GiB/7}
应用管理 🚥	创建实例 资源概	覧 Q 可按ID、名称、IP等属性	性模糊搜索云服务器,多个关键字用英文逗号 (,)	分隔		
实例与镜像 へ			您当前没有保	有实例 立即创建 >>		
实例						
镜像						
弹性容器实例 ECI 🖸						
专有宿主机 DDH						
云盒						
超级计算集群						
预留实例券	<					
资源保障 NEW	_					

2.2 选择地域与机型

这里建议选型计算型 4C 16G 主机起步,因为系统为 64 位系统

付费模式 地域及可用区 如何选择地域	包年包月 シ シ た会け第に5支持停机に部分 指配节音计划,按量影单最高可 使用旅游保障服务进行客量预留 华 年2 (上海) ▼ 不同地域的实例之间内网互不相	校量付费 把源不论意功能。可以有效特征 耳季变 2.4折折扣。目计划内产品 3.确保您的应用用有扩容所需 随机分和 可用区 M 通,说得能比您客户的地域。	抢占式实例 成本,了解相关限制 品不受地域升降配可 容量。点击了解更多 可用区 C 可 可降低网络时延、提	⑦ 印刷检发条件 查看详情 2更規格族限制,前化 > J用区 D 可用E 高級客户的访问速度	\$> 注介绍页了解更多 【 E 可用区 , ⑦	> L 可用区 F	可用区 G 同	J用区 A	可用区 N 可用区	K 可用区 8
实例规格 实例规格质 结果配置查型 可购买的地域 申请按量高配	 分黄造型 塔景化造型 当前代 所有代 当前代 所有代 前法 送帰 vCPU ▼ 2 梁构 X86 计算 ARI 分类 通用型 计算算 	 調内存 → 推測規模 M 计算 算初计算 協行費 大政策 	容称,如: ecs.g5.la 弹性裸金羅服务器 型 本地 SSD	rge Q 1/0 f	光化突例 ⑦ 共享型	是否支持P>6 ▼ 措强型 最新	推荐			
	规格族 ③	实例规格 vCP	U 🌲 内存 🌲	处理器主须/睿频	内网带宽 🔷 👔	内网收发包 💿 🌲	存储IOPS 基准/峰值 ⑦	IPv6	参考价格 💿 🌲	处理識型号
	○ 通用型 g6 ⑦	ecs.g6.8xlarge 32 v	CPU 128 GiB	2.5 GHz/3.2 GHz	10 Gbps 2	200万 PPS	6.3 万/-	是	¥ 8.0 /81	Intel Xeon(Cascade Lake) Platinum 8269CY
	通用型 g6	ecs.g6.13xlarge 52 v	CPU 192 GiB	2.5 GHz/3.2 GHz	12.5 Gbps	300万 PPS	10.5 万/-	문	¥ 13.0 /Bg	Intel Xeon(Cascade Lake) Platinum 8269CY
	○ 通用型 g6	ecs.g6.26xlarge 104	vCPU 384 GiB	2.5 GHz/3.2 GHz	25 Gbps	500万 PPS	21 万/-	是	¥ 26.0 /B	Intel Xeon(Cascade Lake) Platinum 8269CY
	通用平衡增强型 g6e	ecs.g6e.large 2 vC	PU 8 GiB	2.5 GHz/3.2 GHz	最高 10 Gbps	90万 PPS	2.1 万/-	是	¥ 0.55 /Bj	Intel Xeon(Cascade Lake) Platinum 8269CY
	● 通用平衡増强型 g6e	ecs.g6e.xlarge 4 vC	PU 16 GiB	2.5 GHz/3.2 GHz	最高 10 Gbps	100万 PPS	4.2 万/-	是	¥ 1.1 /81	Intel Xeon(Cascade Lake) Platinum 8269CY
	通用平衡増强型 g6e	ecs.g6e.2xlarge 8 vC	PU 32 GiB	2.5 GHz/3.2 GHz	最高 10 Gbps	160万 PPS	5.25 万/-	是	¥ 2.2 /时	Intel Xeon(Cascade Lake) Platinum 8269CY
	通用平衡增强型 g6e	ecs.g6e.4xlarge 16 v	CPU 64 GiB	2.5 GHz/3.2 GHz	最高 10 Gbps	800万 PPS	8.4 万/-	是	¥ 4.4 /时	Intel Xeon(Cascade Lake) Platinum 8269CY



2.3 选择镜像

在镜像市场选择镜像

不同的镜像对应不同的实例类型:

CloudGuard Check Point Security Management (BYOL)对应实例类型是通用型 g7, g6e CloudGuard Check Point Network Security Gateway (BYOL)对应实例类型是增强型 g7ne, g5ne

镜像市场[华东 2 (上)	更)]		×
	CloudGuard Check	搜索	
精选镜像	全部操作系统 全部架构 按分值筛选	\sim	
镜像分类 ∧ ✓ 全部 操作系统 262	CloudGuard Check Point Security Management (BYOL) 基础系统: linux 架构: 64位 最新更新: 2022-09-26 R81 ✔ R81 安全管理平台是Check Point公司推出的最新的威胁防护和安全	★★★★★ 6人已使用	¥0 /时 使用
运行环境 687			

镜像	公共镜像	自定义镜像	共享镜像	镜像市场	社区镜像	0			
当前选择的镜像 CloudGuard Check Point Security Management (BYOL) R81 ⑦									
	重新选择镜像								

2.4 选择存储和带宽

根据自己需求购买相关的硬盘和宽带速度

存储	系统盘				
云盘参数和性能	高效云盘	•	100	GiB	2600 IOPS
	不同云盘性能指标不	同, 查看 各	云盘性能指标>	_	
	数据盘 您已选择(+ 增加一块数据	0 块盘,还可 盘	[以选择 <mark>16</mark> 块盘。		
	> 共享盘 NAS				

SOFTWARE TECHNOLOGIES LTD. Check Point 基于阿里云的部署 ✓ 分配公网 IPv4 地址 公网 IP 系统会分配公网 IP,也可采用更加灵活的弹性公网 IP 方案,了解如何配置并绑定弹性公网 IP 地址> 公网带宽计费 带宽计费模式 按使用流量 按固定带宽 带宽费用合并在ECS实例中收取 带宽值 - 7 + Mbps 0 100M 75M 1M 50M 25M 阿里云免费提供最高 5Gbps 的恶意流量攻击防护。了解更多 | 提升防护能力

2.5 设置安全组和密钥对

安全组可自定义

配	置	密	钥	 对
	请确保所选安全组开放包含 22	(Linux) 或者 3389 (Windows) 端口,否则无法	表远程登录ECS。您可以进入ECS控制台设置。前:	往设置>
配置安全组	所选安全组 1). xiang_group / sg	-uf6ak2cblnw0qakdw1a9 (已有 4 个实例+辅助	如今卡,还可以加入 1996 个实例+辅助网卡)	
安全组	重新选择安全组 ⑦ 安全纲	送似防火墙功能,用于设置网络访问控制,您也	也可以到管理控制台新建安全组> 安全FAQ>	

登录凭证	密钥对	创建后设置				
登录名	 root 					
				-		
密钥对②	cp_key		•	○ 创建密钥对 如何使用密钥对	ġ.	

密钥对用于远程 SSH 连接设备。

2.6 确认配置信息

所选配置							
基础配置 🖉	付赛模式: 按量付费 购买数量: 1 台	地球及可用区: 华东 2 可用区 N 锦鏡: 「NouthTimed Charle Daile Canville Mansarament (BYOL) R81 xi,ang.vpc/ vpc-utfer89m76d8zrs65jul1f	实例级格 : 通用平衡增强型 g6e / ecs.g6e.large (2xCPU 8GB) 系统盘 : ESSD云盘 100GB,PLD (单盘)OPS性能上页1万)				
网络和安全组 🖉	网络 :	VPC: xi_ang_vpc/vpc-uf6x89m76d8zrs65jul1f 安全相: 1).xiang_group/sg-uf6ak2cbinw0qakdw1a9	交換机 : CP-Out/ vsw-uf69aq88hy7c3gagrb53t/ 172.16.0.0/24				
系統配置 🖉	登录凭证: 密钥对:cp_key	实例名称 : launch-advisor-20221012	尖砌元数据访问模式 : 普通模式 (兼容加固模式)				
	保存为启动搜索 ① 生成Open API最佳实践脚本 ⑦ 保存当前购买配置为ROS操板 ⑦						
使用时限	□ 设置自动释放服务时间 ECS实例将在忽预约的时间点进行释放,实例释放后数据及IP地址不会被保留且无法找回,请谨慎操作。						
服务协议	✓ (无服务器 ECS 服务条款) (精像亮品使用条款) 您可以点此查查购买例如, 订单约应的发展信息,请在 管理处制合,费用中心-发展管理,中查看, 云产品款认.费用 TCP 25 第几和基于此满口的邮箱服务,特殊猜况需报备审核后使用,查看评情>						

配置完就可以开通了

SOFTWARE TECHNOLOGIES LTD.

Check Point 基于阿里云的部署

实例							
创建实例	或者输入关键字识错	割捜索 🥝 🔍 标签				高级搜	素创建诊断 批量操作 С 上 傘
实例ID/名称	标签	监控 可用区 ₽	IP地址	状态	网络类型 🔽 配置	付爨方式 ▽	摄作
i-uf6275hb357lp00cq4jj launch-advisor-20221012	۹ ۵	□ 上海可用区N	139.196.92.126 (公) 172.16.0.185 (私有)	●运行中	专有网络 2 vCPU 8 GiB (I/O优化) ecs.g6e.large 5Mbps	按量 2022年10月12日 11:14 创建	管理 远程连接 更改实例规格 更多 ▼
日 日本 停止 重启 重置交	议例密码 续费	按量付费转包年包月	释放设置 更多▲			共有1条,每页5	显示: 20 ♥ 祭 《 〈 1 〉 »

第三章 SSH 远程连接主机

3.1 使用新密钥文件登录主机

使用 SecureCRT 远程工具, 配置会话

Session Options - 阿里Cl	^o test	\times
类别(<u>C</u>):		
▼ 连接	SSH2	
登陆动作 ▼ SSH2 SFTP Session	主机名	139.196.92.126
● 高级 ● ● ○ 端口转发	端	22
· 远程/X11	防火墙	None ~
│ ◇ 玲端 │ ◇ 仿真	用户名	admin
模式 Emacs	鉴权	
模式 Emacs 映射键 高级 ◇ 外观 ANSI 颜色 窗口 日志文件 打印 X/Y/Zmodem	 ✓ 密码 ✓ 公钥 ✓ 键盘交 ✓ GSSAPI ✓ GSSAPI ✓ ecdh-sh ✓ ecdh-sh ✓ ecdh-sh ✓ diffie-he ↓ diffie-he ↓ diffie-he ↓ diffie-he 	五 五 五 五 五 五 五 五 五 五 五 五 五 五 五 五 五 五 五
		确定取消



选择对应的文件

公钥属性		
 ○ 使用全局公钥设置(U) ● 使用会话公钥设置(K) 会话设置(S) ● 使用身份或证书文件(E) 		确定 取消
C:\Users\admin\Documents\cp_key.pem		
 ○使用个人存储证书(CAPI)(<u>S</u>) CAPI □ □□□: 要使用的证书 □Try all certificates> □使用证书作为原始 SSH2 密钥 (服务器不支持 X.509)(<u>T</u>) 指纹 (%1): SHA-2: d7:70:0c:bf:a4:c0:e7:2d:18:26:1e:ae:bc:28:d8:ba:5b:82:55:7e:54:32:9 SHA-1: a3:42:03:13:3f:99:61:af:ae:66:3e:fb:82:de:7c:62:eb:9f:84:00 MD5: 4b:a5:dc:dd:30:71:e6:e7:b5:7f:b4:eb:a5:54:1e:c1 	 	
< 创建身份文件(I) 上传(<u>o</u>) 导出公钥(⊻) 更改通行短语(> <u>P</u>)	

点击跳过,进入系统

输入安全外壳密码						
admin@139. 入密码。	196.92.126 需要一个密码。请输	确定				
		取消				
用户名	admin					
密码(<u>P</u>):						
🗌 保存密码	∃(<u>S</u>)	跳过(<u>K</u>)				

Check Point 基于阿里云的部署



配置 admin 密码

iZuf6275hb357lp00cq4jjZ> set user admin password New password: Verify new password: iZuf6275hb357lp00cq4jjZ>

保存退出,进行初始化

iZuf6275hb357lp00cq4jjZ> save config iZuf6275hb357lp00cq4jjZ>

第四章 Gaia (底层系统) 初始化

4.1 登陆 Gaia 系统





Check Point 基于阿里云的部署

Deployment Options	
---------------------------	--

Cabur				
Setup				
Continue with R8	l configuration			
Installation				
Install from Check	Point cloud			
Install from USB d	levice			
Recovery				
Import existing sn	apshot 🕜			
		< Back	Next >	Cancel
Management	: Connection		(•	Check Point
Management	: Connection		(•	Check Point oftware technologies lto
Management	: Connection		(•	Check Point oftware technologies lto
Management	Connection		() () () () () () () () () () () () () (Check Point oftware technologies lto
Management	eth0		())	Check Point oftware technologies lto
Management Interface: Configure IPv4: IPv4 address:	eth0 Manually		())	Check Poinť
Management Interface: Configure IPv4: IPv4 address: Subnet mask:	eth0 Manually		())	Check Point oftware technologies lto
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253			Check Point oftware technologies lto
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253			Check Point oftware technologies lto
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway: Configure IPv6:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253 Off			Check Point oftware technologies lta
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway: Configure IPv6: IPv6 Address:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253 Off			Check Point oftware technologies ltd
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway: Configure IPv6: IPv6 Address: Mask Length:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253 Off			Check Point oftware technologies ltd
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway: Configure IPv6: IPv6 Address: Mask Length: Default Gateway:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253 Off			Check Point oftware technologies ltd
Management Interface: Configure IPv4: IPv4 address: Subnet mask: Default Gateway: Configure IPv6: IPv6 Address: Mask Length: Default Gateway:	eth0 Manually 172, 16, 0, 185 255, 255, 255, 0 172, 16, 0, 253 Off			



配置主机名

Device Informat	ion			Check Point SOFTWARE TECHNOLOBIES LTD.
Host Name:	SMS			
Domain Name:	Optional			
Primary DNS Server:	100.100.2.136			
Secondary DNS Server:	100.100.2.138			
Tertiary DNS Server:				
Proxy Settings				
Use a Proxy server				
Address:				
Port:	8080			
		< Back	Next >	Cancel
Date and Time S	ettings		T	Check Point SOFTWARE TECHNOLOGIES LTD.
Date and Time S	ettings			Check Point SOFTWARE TECHNOLOBIES LTD.
© Set time manually:	Settings			Check Point SOFTWARE TECHNOLOGIES LTD.
Date and Time S Set time manually: Date: Time:	Wednesday, October 12, 2022			Check Point BOFTWARE TECHNOLOGIES LTD.
Date and Time S Set time manually: Date: Time: Time: Time Zone:	Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00)			Check Point BOFTWARE TECHNOLOGIES LTD.
Date and Time S Set time manually: Date: Time: Time Zone:	Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00)		1	Check Point Boftware technologies LTD
Date and Time S Set time manually: Date: Time: Time Zone: Use Network Time Prof Primary NTP server:	Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00) cocol (NTP): ntp7.cloud.alivuncs.com	Version: 4		Check Point Boftwurke technologies Ltd
 Date and Time S Set time manually: Date: Time: Time Zone: Use Network Time Prot Primary NTP server: 	Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00) cocol (NTP): ntp7.cloud.aliyuncs.com	Version:		Check Point BOFTWURRE TECHNOLOGIES LTD
Date and Time S Set time manually: Date: Time: Time Zone: O Use Network Time Prof Primary NTP server: Secondary NTP server: Time Zone:	Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00) cocol (NTP): ntp7.cloud.aliyuncs.com ntp11.cloud.aliyuncs.com Taipei, Asia (GMT + 9:00)	Version: 4		Check Point Software technologies LTD
Date and Time S Set time manually: Date: Time: Time: Time Zone: Ouse Network Time Prof Primary NTP server: Secondary NTP server: Time Zone:	Settings Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00) cocol (NTP): ntp7.cloud.aliyuncs.com ntp11.cloud.aliyuncs.com Taipei, Asia (GMT +8:00)	Version: 4 Version: 4		Check Point Software technologies LTD
Date and Time S Set time manually: Date: Time: Time Zone: Ouse Network Time Prot Primary NTP server: Secondary NTP server: Time Zone:	Settings Wednesday, October 12, 2022 12 : 19 Taipei, Asia (GMT +8:00) socol (NTP): ntp7.cloud.aliyuncs.com ntp11.cloud.aliyuncs.com Taipei, Asia (GMT +8:00)	Version: 4 Version: 4		Check Point BOFTWARE TECHNOLOGIES LTD

©2022 SHANGHAI SHONE TENCHNOLOGY CO., LTD. All rights reserved

根据需要选择安装的产品类型

- Security Gateway:安全网关(防火墙)
- Security Management: 管理服务器

通常是二选一,不建议两个产品装在同一台云主机上。

Products	SOFTWARE TECHNOLOGIES LTD.
Products	
Security Gateway	
V Security Management	
Clustering	
Unit is a part of a cluster, type:	ClusterXL 👻
Define Security Management as:	Primary 🗸
Automatically download Blade Co recommended)	ntracts, new software, and other important data (highly
For more information click he	re
	< Back Next > Cancel



Check Point 基于阿里云的部署

Security Mai	nagement GUI Clients	
GUI clients can log i	into the Security Management from:	
Any IP Address		
This machine		
IP address:	50.7.250.202	
Network		
IP Address:		
Subnet:		
Range of IPv4 ac	ddresses:	
	< Back	Next > Cancel
First Time Co	onfiguration Wizard Summary	
First Time Co	onfiguration Wizard Summary	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gatewar	onfiguration Wizard Summary	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products:	BOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products:	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	SOFTWARE TECHNOLOGIES LTD.
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	CONCURRENT AND A SUBJECT AND A
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: <i>y</i> ement: Primary Security Management	CRECK POINT BOFTWARE FECHNOLOGIES LTD
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	
First Time Co Your device will be o Security Gateway Security Manage	configuration Wizard Summary configured with the following products: y ement: Primary Security Management	

Check Point' Deftware technologies ltd.	Check Point 基于阿里云
First Time Configuration Wizard Summary	SOFTWARE TECHNOLOGIES LTD.
Your device will be configured with the following products: Security Gateway	
Securit Mercenet Driver Consiste Mercenet First Time Configuration Wizard	×
This will start the configuration process. Are you sure you w	vant to continue?
Yes No	
Improve product experience:	
Send data to Check Point more > Send crash data which might contain personal data to Check Point. I more >	
< Back	Finish Cancel

First Time Configuration Wizard Su		
Verifying Configuration	0	
C Security Gateway	6 %]
Security Management		_
Compatibility Packages		_
Finalizing Configuration (this may take several min		_
	< Back Finish	Cancel

©2022 SHANGHAI SHONE TENCHNOLOGY CO., LTD. All rights reserved



第五章 通过 SmartConsole 配置防火墙的相关功能

©2022 SHANGHAI SHONE TENCHNOLOGY CO., LTD. All rights reserved

SOFTWARE TECHNOLOGIES LTD.

5.1 下载和安装 SmartConsole 客户端

🖸 🌢 Case: 6-00034 x 🗅 Check Point C. x 🖻 快科技科技 x G asa5525-fpwr· x 賞 首页 - Chiphel x G 翻译 - Google x 💺 Google 翻译 x 🎸 Practical trout x 👔 Gaia x + - 🗇 >							
← C 🗅 https://139.196.92.1	26/_38efe1b8ce16a7f2ee34dcf71b0c6e31/cgi-bin/home.tcl	2 A to 🔮 💱 🌒	G G 1/2 m 1/2 ····				
Aliyun 🔨 🖬 🔓		Search	👤 admin 🗗 🔛 Check Point 🔍				
44	Manage Soft	ware Blades using SmartConsole 👽 Download Now!	- -				
Overview	System Overview	Blades 🔨 🗙					
Artwork Management Artwork Interfaces ARP DUCD Senses	Check Point Security Gateway R81 Kernel: 3.10.0-957.21.3cpx86_64 Edition: 64-bit	Packets accepted: 14112 Packets dropped: 0 Packets Accepted: 519 connections: Number of 3	ه ۵				
Hosts and DNS Hosts and DNS Hov4 Static Routes NetFlow Export	Build Number: 392 System Uptime: 4 hours 43 minutes Software Updates: 2 new recommended updates	connections:	a . +				
\$\vec{Proxy} \$\vec{Proxy} \$\vec{Proxy} \$\vec{Proxy} \$\vec{Time} \$\vec{Prox}\$ Cloning Group	(-)	IPS Application Control					
SNMP Job Scheduler Mail Notification Messages	Alibaba Cloud	URL Filtering					
Display Format Session	Platform: Aliyun	Anti-Virus					
 Crash Data System Configuration System Logging 	Network Configuration	Anti-Bot					
 Network Access Certificate Authority 	Name IPv4 Address IPv6 Address Link Status	Threat Emulation					
 Host Access LLDP Advanced Routing 	eth0:1 139.196.92.126 - 🙂 Up eth1 172.16.1.100 - 🙂 Up	Threat Extraction					
C DHCP Relay	lo 127.0.1 - 🕐 Up	Anti-Spam and Mail	· · · · · · · · · · · · · · · · · · ·				

安装 SmartConsole



登陆 SmartConsole



SmartConsole 主页面

<u>©</u> ≞ • ∣	😭 Objects	- 🔮 Install Poli									Check Point' - SmartConsole'	_ 8 ×
	Columns:	General	÷	*•	Scripts 👻 📩 Ac	tions 🔹 🖒 Moni	tor 🕒 Current session change	s Q Search	T	1 오	Q Search)) (
	Status	Name	IP Versi	Active Blades	Hardware	CPU Usa	Recommended Updat	Recommended Jumbo		Comme	← 📸 🗄 🕂 😽 New •	pjects
GATEWAYS & SERVERS	0	🖀 SMS 1	72.16.0.185 R81	55 4 E	Open server	1 2%	2 updates available	Check_Point_R81_JUMBO_	HF_MAIN_Bundle_T69_FULL.tgz		Object Categories	Valio
											A Network Objects	17 01
SECUDITY											services	521
POLICIES											Polications/Categories	8313
											🗱 VPN Communities	2
~											≜o Data Types	62
LOGS & MONITOR											Users/Identities	1
											Servers	1
ţ.											O Time Objects	з
MANAGE &											🗴 UserCheck Interactions	13
											Limit	4
										Ŧ		
	Summa	ary Tasks	Errors Lic	enses								
		SMS					Access Blades					
	IDv4.4	ddress:	172.16.0.185		Open s	erver	Firewall					
	05.	4001033.	Gaia									
	Versie	on:	R81				Management Blades Network					
	Licen	se Status:	A Not Activat	ed			Policy	ES Logging & Status				
							Management					
0												
COMMANID					CPU:	12%						
LINE					Memory:	54%						
0					, _							
WHAT'S					Device & Licen	se Information				Activate Blades		
	No tasks in r	orogress +					2 139 196 9	126			No changes	admin
	the cashs in p						a 155.150.5					

5.2 Get 底层的拓扑信息

让上层 FW 获取底层接口信息及拓扑

🞑 Check Poinť

	SOFTWARE TECHNOLOGIES LTD.				Check Poi	int 基于阿里云的	的部署
≌:-	🤘 Update 🎲 Objects 🕶 🕑 Install Policy		🏛 Discard Session 🝷 2 斎 Publish			Check Point' – Smart Console '	~
	Columns: 💿 General 🔹 🔭 🗙	🕤 Scripts - ґ Actions - 🄇	Monitor Durrent session changes	T	1 오	Q Search	
ATEWAYS SERVERS ECURITY POLICIES LOGS & MONITOR	Status Name IP Versi Active Blader	Check Point Gateway - SMS General Properties Stateway Kanagement System Backup VPN Domain Proxy RNAT HTTPS Inspection HTTPS Inspection HTTPS Inspection HTTPS Inspection HTTPS Inspection HTTPS Inspection HTTP Attract Cogs Optimizations Htt Count Cogs Optimizations Optim	Get Interfaces. CEdit CActions C Name Topology IP Centernal 172.16.0.185/24 Centernal 172.16.1.100/24	Search 2	O X	A policit Categories Network Objects Network Objects Services Applications/Categories VPN Communities Vort Communities Users/Identities Servers Time Objects W Usercheck Interactions	17 521 8313 2 62 1 1 3 3 13
	Summary Tasks Errors Licenses Free SMS IPv4 Address: 172.16.0.185 OS: Gaia Version: R81 License Status: Not Activated	< >>		OK Cancel	*	O Limit	4

5.3 定义接口域并关闭接口地址防欺骗功能





Check Point 基于阿里云的部署

5.4 编辑策略

Standard ** ** **	🖳 -	👕 Objects 🕶 😍 Install Policy								Check Point SmartCons	ole: - 🗗 💌
Image: Source State Source Source State Source So		Standard +									
• Access Control • Access Tools • Access Tools • Origine							ID 11 is at		0		00
Summary Details Logs History Surves Surves Reference Surves Surves <th></th> <th>- Access Control</th> <th></th> <th>트 48 시 오 듯 5</th> <th>= • Install Policy C Action</th> <th>Search for</th> <th>IP, object, action, .</th> <th></th> <th>Q V</th> <th></th> <th>Ĩ</th>		- Access Control		트 48 시 오 듯 5	= • Install Policy C Action	Search for	IP, object, action, .		Q V		Ĩ
	& SERVERS	Policy	No. Sour	ce	Destination	VPN	Services &	Applications Action	In	ck	Install On
• Threat Prevention • Policy · Exceptions · Origin		NAT	1 *	Any	* Any	* Any	* Any	🕒 Act	cept 🔳	Log	🔁 gate
Policy If Exceptions Accept 分許 Drop 拒絶 Drop 拒他 Drop Drop Drop Drop Drop Drop Drop Drop Drop Dro		- Threat Prevention			Missing cleanup r	ule - Unmatched tra	ffic will be dropped a	and not logged.			
if Exceptions inspection Settings inspectings inspection Settings inspection S	SECURITY POLICIES	Policy									
Access Tools Summary Details Logs History Visition Visit Summary Details Logs History Visition Visit Summary Details Logs History Visition Visit Summary Details Logs History Visition Visition Visit Q O All Time · Log File: Latest Log File Current Rule * Enter search query (Ctrl+f) = Visit Visit Current Rule * District Source User		Exceptions									
Shared Policies	~						Accep	て 允许 	日志	策略安装到	到哪—个
 Image: Source of the second of	LOGS & MONITOR	Shared Policies					Diop	1640		gateway_	E 🔤
Image: Summary Details Summary Details Summary Details Logs History Summary Details Logs Marge: Stores Summary Details Summary Details Logs History Summary Details Logs History Commary Details Logs History Summary Details Logs Summary Details Logs Summary Details Logs History Commary Details Logs History Commary Details Logs History Commary Details Logs History Commary Details Logs History Commary Details Logs Logs History		🛛 🕜 Geo Policy									
Access Tools Summary Details Logs History Image: Current Rule * Enter search query (Ctrl + F) Image: Rule Rule Rule	¢	🔑 Inspection Settings 🖻									
Access Tools	SETTINGS										
Koress Tools VPN Communities Updates VS Updates VS UserCheck Client Certificates Application Wiki Installation History Today, 100325 VS V Installation History Summary Details Logs History Sum											
Summary Details Logs History Summary Details Logs History Access Tools											ź
Access Tools			Summary De	tails Logs Hist	ory						
Access Tools Showing first 50 results (1.1 sec) out of at least 50 results Curry Syntax			C CA Q	🗿 All Time 🝷 🛛 Log File: L	atest Log File Current Rule	* Enter search	query (Ctrl+F)				=
Image: VPN Communities Time o Origin Source Source User Destination Service Ac Access Rule N Policy Descrip Outplates Today, 1:03:35 III O I I I I I I I I I I I I I I I I I		Access Tools	Showin	g first 50 results (1.1 sec.) ou	t of at least 50 results						Query Syntax
Image: Community of Updates Today, 1:03:35 III (D) (1,03:35		🗱 VPN Communities	Time	Origii	n Source	Source User	Destination	Service	Ac Access Rule I	I Policy	Descrip
Commany Commany New No UserCheck Today, 1:03:35 III (I) (I) (I) (I) (I) (I) (I) (I) (I)	2	🗘 Updates	Today, 1:03:35	🗰 🤁 🍾 🏦 📼 ga	teway-1 🛛 🔛 gateway-1 (1		100.64.0.3	domain-udp (UDP/53)	1 Cleanup rule	Standard	domain-u
UNE Today, 1:03:30 III (0 \ 1, 1:03:32 III (0	COMMAND	🛇 UserCheck	Today, 1:03:35	🎫 😲 🍾 🏦 📼 ga	teway-1 🛛 🔚 gateway-1 (1		🔚 public1.sdns	domain-udp (UDP/53)	1 Cleanup rule	Standard	domain-u
Image: Constraint of the standard domain with the standard domain withe standard domain with the standard domain wi	LINE	🙀 Client Certificates 🖻	Today, 1:03:30	🖽 🤁 🍾 🏦 📼 ga	teway-1 🔛 gateway-1 (1		100.64.0.3	domain-udp (UDP/53)	1 Cleanup rule	Standard	domain-u
WHATS NEW O Installation History Today, 1:03:25 III O Standard Smtp Traff Today, 1:03:24 III O Standard III O Standard III O Standard III O Standard Smtp Traff Today, 1:03:24 III O Standard III O Standard III O Standard III O Standard Smtp Traff	?	Application Wiki	Today, 1:03:29	🔛 😲 🍾 🏦 📼 ga	teway-1 🔛 gateway-1 (1		public1.sdns	domain-udp (UDP/53)	1 Cleanup rule	Standard	domain-u
New Today, 1:03:24 Today, 1:03:24 and the standard smtp Traff	WHAT'S		Today, 1:03:25	🔛 🤁 🍾 🛨 📼 ga	teway-1 37.49.225.71		gateway-1 (1	smtp (TCP/25)	1 Cleanup rule	Standard	smtp Traff
	NEW	• Installation matory	Today, 1:03:24	🎫 🤁 🍾 🛨 📼 ga	teway-1 37.49.225.71		gateway-1 (1	smtp (TCP/25)	1 Cleanup rule	Standard	smtp Traff
No tasks in progress 🔺 🗧 139.198.1.92 No changes 💧 admin		No tasks in progress 🔺			2 139.1	98.1.92				N	o changes admin

5.5 开启内网段的 SNAT

首先新建内网路地址段

<u>0</u> : •	📬 Objects 🕶 😍 Install Policy	🌐 Discard Session 👻 🏹 Publish	Check Point — Smart Console	8 ×
GATEWAYS & SERVERS	Standard + ** * Access Control Im Policy	Image: Actions Image: Search for IP, object, action, Q Image: Search for IP, object, action, No. Original Source Original Destination Original Services Translated Source Translated Destin Translated Services	Q. Search ← 音 ⋮ ★ New▼ Network Object Categor	2 Objects
SECURITY POLICIES LOGS & MONITOR	 Threat Prevention Threat Prevention Policy Exceptions Shared Policies 	Automatic Generated Rules: Machine Static NAT (No Rules) E Automatic Generated Rules: Machine Hide NAT (No Rules) Automatic Generated Rules: Address Range Static NAT (No Rules) Automatic Generated Rules: Network Static NAT (No Rules) Automatic Generated Rules: Network Static NAT (No Rules) Automatic Generated Rules: Network Hide NAT (No Rules) Automatic Generated Rules: Network Hide NAT (1-4) 1 & 192.168.1.0/24 & Any = Original = Original 2 & 192.168.1.0/24 & Any & Any = Original = Original 3 & CP_default_Ofn. & Any & Any = Original = Original 4 & CP_default_Ofn. & Any & Any & Original = Original 4 & CP_default_Ofn. & Any & Any & Original = Original 4 Manual Lower Rules (No Rules)	Network Ot Network Gro Services More Applications/Categores VPN Communities Otata Types Users Servers Time Objects UserCheck Interactions Limit	up 7508 2 62 1 1 3 13 4
COMMAND LINE WHAT'S NEW	Access Tools VPN Communities Updates UserCheck Client Certificates Application Wiki Installation History No tasks in progress	€ 139.196.1.92	No changes d	admin





开启 NAT

: •	🗊 Objects 🕶 🛛 😍 Install Policy	Check Point — 🗗 🗙 Smart Console		
	Standard Xiang policy × +	.≣• X 🖸 ÷ L ^A Actions • Search for IP, object, action, Q, V ∧ Y	Q. Search ← 圖 Ξ 米 New ▼	
GATEWAYS & SERVERS SECURITY POLICIES LOGS & MONITOR MANAGE & SETTINGS	 Actess Control Im Policy Im Policy Im Policy Shared Policies O Geo Policy Im Policy Gateways Im Exceptions ✓ Inspection Settings Im 	No. Original Source Original Destinati Original Services Translated Source Translated Destin Translated Services Install On Commer 1 * Any Fxe-wan * TCP-13389 = Original Image: Services Image: Ser	Networks 3 CP_default_Office_Mode_addresses IPv6_Link_Local_Hosts Lan-172.16.1.0	
COMMANE LINE WHAT'S NEW	Access Tools VPN Communities Updates UserCheck Client Certificates Application Wiki Installation History No tasks in progress	OK Cancel	Image: Constraint of the second se	

5.6 下发策略并生效

<u>]=</u> -	🜍 Objects 🕶 🕑 Install Policy		Ticard Session - M Publish								Check Point	
i	Standard Xiang policy × +										🔍 Search	
	 ↔ Access Control 	🚊 🗙 🔄 🚔 Ґ Actions 🔹 Search for IP, object, action, 🔍 🔍 🗸 🗸									← 🏦 ☷ 🔺 New▼	
EWAYS ERVERS	🚺 Policy	No.	Original Source	Original Destinati	Original Services	Translated Source	Translated Destin	Translated Services	Install On	Commer	Networks	
	🗱 NAT	1 Automatic	* Any	E Fw-wan	+ TCP-13389	= Original	🚍 _s lan-server2016	Remote_Desk	🖀 Xiang-FW		CP_default_Office_Mode_addre	
URITY	 HTTPS Inspection 	Automatic	Generated Rules : Mac	hine Hide NAT (No R	ules)						IPv6_Link_Local_Hosts	
LICIES	🚺 Policy	Automatic Generated Rules : Address Range Static NAT (No Rules)									👗 Lan-172.16.1.0	
		Automatic Generated Rules : Network Static NAT (No Rules)										
^^	Shared Policies ······	Automatic	Generated Rules : Add	ress Range Hide NAT	(No Rules)							
NITOR	🗸 🧭 Geo Policy	 Automatic 2 	Generated Rules : Net	CD default Off			- Original	- Original				
	💵 Policy	2	CP_default_Of	A Arris	Ariy	Ch default Office			* All			
OF MGE 81	📾 Gateways	3	CP_default_Of	* Any	* Any				* All			
TINGS	Exceptions	-	Lan-172.10.1.0	25. Lan-1/2.10.1.0	* Any	- Original			- Xiang-FW			
	🎾 Inspection Settings 🏾	5	A Lan-1/2.16.1.0	* Any	* Any	а _н Lan-1/2.16.1.0 (I	= Original	= Original	Cang-FW			
											🚣 Lan-172.16.1.0	
	Access Tools ······										IP Address: 172.16.1.0	
	🕸 VPN Communities										Subnet mask: 255.255.255.0	
J.	🗘 Updates										Last Modifier : admin	
	🔊 UserCheck											
.INE	🙀 Client Certificates 🖥											
?	🔩 Application Wiki 🖗											
<u> </u>												

注: 只要内部计算机的网关指向防火墙的内部接口地址, 内网计算机就可以上网了

有问题请联系相关的技术人员

yejf@zenitera.com