华为乾坤安全云服务

产品文档

文档版本 01

发布日期 2023-04-30

华为技术有限公司

版权所有 © 华为技术有限公司 2023。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 典型配置案例 1
1.1 企业边界天关透明直路 1
1.1.1 组网需求 1
1.1.2 配置思路 2
1.1.3 数据规划 3
1.1.4 配置全局白名单 3
1.1.5 配置天关（Eudemon1000E-T1） 4
1.1.6 结果验证 7
1.2 企业边界天关旁挂策略路由直路（三层) 8
1.2.1 组网需求 8
1.2.2 配置思路 10
1.2.3 数据规划 10
1.2.4 配置全局白名单 10
1.2.5 配置交换机 11
1.2.6 配置天关（Eudemon1000E-T1） 12
1.2.7 结果验证 16
1.3 企业边界天关旁路镜像流状态检测 17
1.3.1 组网需求 17
1.3.2 配置思路 18
1.3.3 数据规划 19
1.3.4 配置全局白名单 19
1.3.5 配置交换机 20
1.3.6 配置天关（Eudemon1000E-T1） 21
1.3.7 结果验证 24
1.4 企业边界天关旁挂直路检测场景 25
1.4.1 组网需求 25
1.4.2 配置思路 26
1.4.3 数据规划 27
1.4.4 配置全局白名单 28
1.4.5 配置交换机 29
1.4.6 配置天关（Eudemon1000E-T1） 29
1.4.7 结果验证 32
1.5 企业内部存在 NAT 转换场景 33

 版权所有 © 华为技术有限公司

1.5.1 组网需求 33
1.5.2 配置思路 35
1.5.3 数据规划 35
1.5.4 配置全局白名单 36
1.5.5 配置天关（Eudemon1000E-T1） 37
1.5.6 结果验证 41
1.6 企业内部存在 DNS 服务器场景 42
1.6.1 组网需求 42
1.6.2 配置思路 44
1.6.3 数据规划 44
1.6.4 配置全局白名单 45
1.6.5 配置交换机 46
1.6.6 配置天关（Eudemon1000E-T1） 46
1.6.7 结果验证 53
1.7 企业边界防火墙单机组网（三层） 53
1.7.1 组网需求 53
1.7.2 配置思路 54
1.7.3 数据规划 55
1.7.4 配置防火墙 56
1.7.5 结果验证 64
2 边界防护与响应 66
2.1 产品介绍 66
2.1.1 什么是边界防护与响应 66
2.1.2 功能特性 68
2.1.3 产品优势 69
2.1.4 应用场景 70
2.2 服务开通 73
2.2.1 开通商用服务 73
2.2.1.1 租户身份开通 73
2.2.1.1.1 注册华为乾坤帐号 73
2.2.1.1.2 开通服务套餐 73
2.2.1.2 MSP 身份开通 75
2.2.1.2.1 MSP 代建租户 75
2.2.1.2.2 委托 MSP 管理 77
2.2.1.2.3 开通服务套餐 79
2.3 部署指南 81
2.3.1 配置天关上线 81
2.3.2 配置设备安全域 81
2.3.3 配置全局白名单 83
2.3.4 黑白名单授权 84
2.3.5 订阅告警与报告 84
2.3.6 查看威胁事件 85

 版权所有 © 华为技术有限公司

2.4 用户指南 86
2.4.1 查看网络安全状态 86
2.4.1.1 查看安全防护大屏 86
2.4.1.2 查看服务首页 88
2.4.2 快速配置 90
2.4.3 处置威胁事件 91
2.4.3.1 事件概览 91
2.4.3.2 外部攻击源 93
2.4.3.3 失陷主机 96
2.4.3.4 恶意文件 99
2.4.4 管理黑白名单 101
2.4.4.1 一键清除指定设备的 IP 黑名单 101
2.4.4.2 手工创建 IP 黑白名单 102
2.4.4.3 快速查看 IP 黑白名单 104
2.4.4.4 手工创建域名黑名单 105
2.4.4.5 快速查看域名黑名单 106
2.4.5 查看安全报表 107
2.4.6 地址安全域管理 109
2.4.6.1 监测安全域状态 109
2.4.6.2 配置全局白名单 109
2.4.6.3 配置不可信内网地址 111
2.4.6.4 配置设备安全域 112
2.4.7 授权管理 114
2.4.7.1 黑白名单授权 114
2.4.8 配置 Metadata 检测防护规则 115
2.4.9 MSP 代维指导 117
2.4.9.1 代维方式介绍 117
2.4.9.2 MSP 首页介绍 117
2.4.9.3 执行代维操作 117
2.4.10 更多操作 122
2.4.10.1 租户基础操作 122
2.4.10.2 MSP 基础操作 123

 版权所有 © 华为技术有限公司

1 典型配置案例

1.1 企业边界天关透明直路

1.1.1 组网需求

适用产品和版本

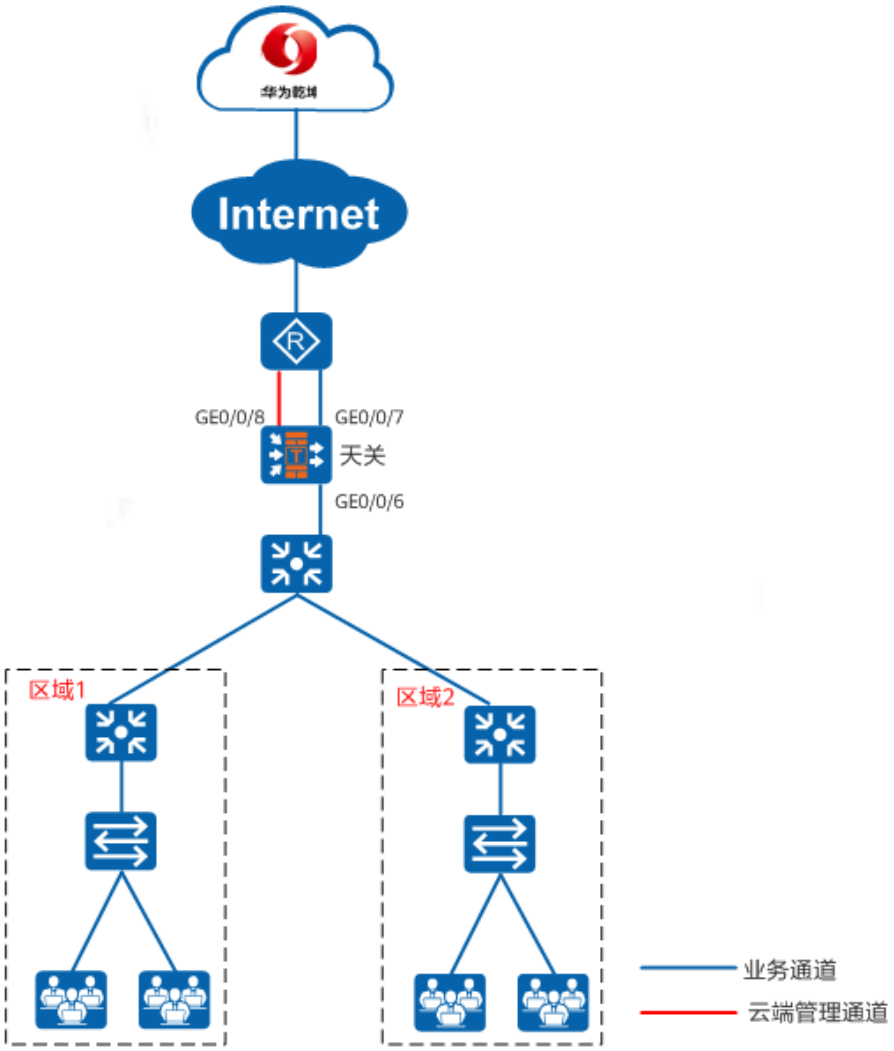
设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务： V600R007C20SPC602及其后续版本	-

组网需求说明

下图以Eudemon1000E-T1的GE0/0/6和GE0/0/7为例，用于转发内外网的业务流量，同时使用三层接口GE0/0/3与云端对接。

版权所有 © 华为技术有限公司

图 1-1 方案组网



约束或注意事项

Eudemon1000E-T1接口使用限制：

- Eudemon1000E-T1不支持硬件Bypass功能。
- 默认情况下，接口编号相邻的接口两两组成二层接口对。
- 奇数编号接口用于连接上行设备，偶数编号接口用于连接下行局域网设备。

1.1.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

版权所有 © 华为技术有限公司

配置思路

1. 登录华为乾坤控制台，配置全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。
2. 登录天关，主要配置以下内容：
   a. 配置业务接口对，用于转发内外网业务流量。
   b. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   c. 配置边界防护与响应服务业务参数。

1.1.3 数据规划

项目	数据	说明
租户内网资产IP地址	● 区域1地址：192.168.55.0-192.168.55.255 ● 区域2地址：172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5	请向租户获取，此处为示例。
转发业务流量接口	GE0/0/7和GE0/0/6	-
云端管理接口	GE0/0/3：172.16.10.10/24	请向租户获取，此处为示例。

1.1.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

说明

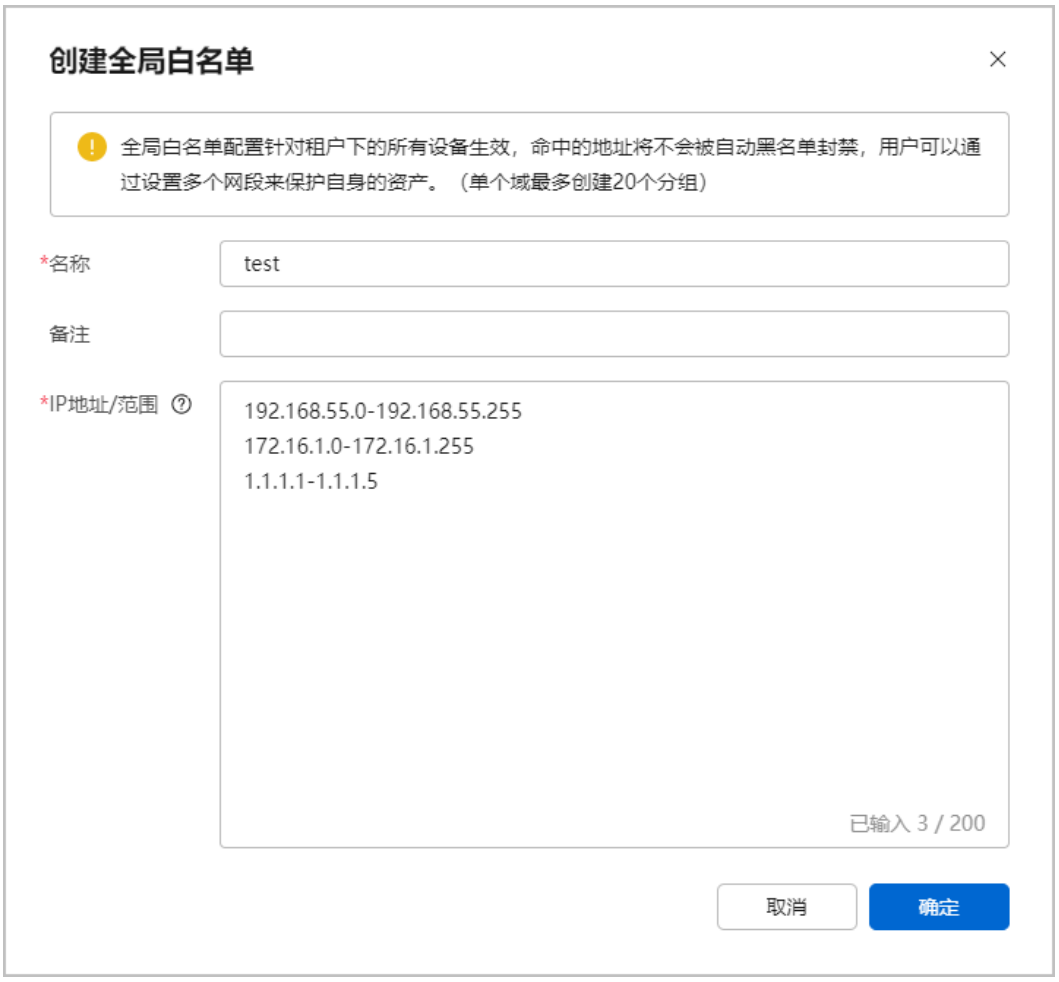
已购买边界防护与响应服务时需要配置全局白名单。

操作步骤

1. 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。
2. 在“全局地址管理 > 全局白名单”页签中，单击“ + ”，按照下图所示配置全局白名单。

版权所有 © 华为技术有限公司

图 1-2 创建全局白名单



1.1.5 配置天关（Eudemon1000E-T1）

操作步骤

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置业务接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/6，按如下参数配置，单击“确定”。

安全区域	trust
模式	接口对

   c. 参考上述步骤按如下参数配置GE0/0/7接口。

安全区域	untrust
模式	接口对

 版权所有 © 华为技术有限公司

3. 配置业务接口对。
   a. 选择“网络 > 接口对”。
   b. 单击“新建”，按如下参数配置，单击“确定”。

名称	interface_bypass1
工作模式	不同口进出
成员	
接口一	GE0/0/6
接口二	GE0/0/7
允许的VLAN	1-4094
接口对状态同步	不开启

4. 配置云端管理接口。
   GE0/0/3默认为二层接口，请按照如下方式配置成三层接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/3对应的，按照如下参数配置接口。

安全区域	untrust
模式	路由
IPv4	
IP地址	172.16.10.10/24

   c. 配置云端管理接口的静态路由。
      i. 选择“网络 > 路由 > 静态路由”。
      ii. 单击“静态路由列表”区域下的“新建”，添加静态路由。下一跳配置为网关地址。

版权所有 © 华为技术有限公司

图 1-3 配置静态路由

5. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

图 1-4 配置系统时间

6. 配置业务参数（边界防护与响应服务）。
   a. 加载License。

      说明

      如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

      i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。
      ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。

版权所有 © 华为技术有限公司

c. 确认安全策略已成功下发。

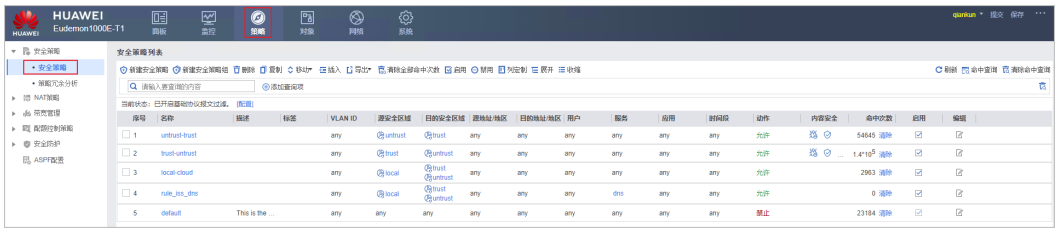
设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

安全策略下发后，如图1-5所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

说明

如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

图 1-5 安全策略

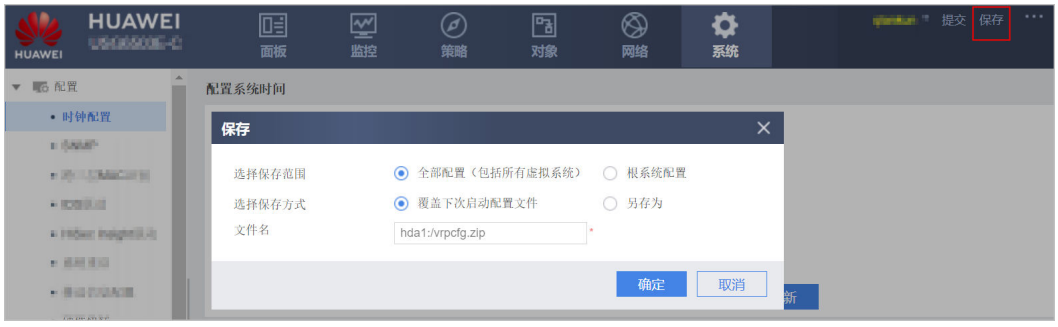


d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-6 特征库升级

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-7 保存配置



1.1.6 结果验证

1. 验证设备上线是否成功、业务套餐是否激活成功。

   a. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。

版权所有 © 华为技术有限公司

设备状态为“正常”表示设备已上线成功。

b. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。

套餐状态为“正常”表示套餐已激活成功。

2. 验证边界防护与响应服务是否正常。

a. 检查黑名单是否能够正常下发。

i. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”，在右上角菜单栏选择“黑白名单”。

ii. 在“黑名单 > IP黑名单”页签中创建并部署一个黑名单。

iii. 登录设备的标准界面**https://192.168.0.1:8443/**。

- Eudemon1000E-T1：在“策略 > 安全防护 > 黑名单”中检查是否存在下发的黑名单。

如果存在则表示黑名单能够正常下发。

说明

- 请获取一个当前没有业务使用的IP地址作为黑名单，否则可能会影响当前业务。
- 验证后请务必在“黑名单 > IP黑名单”页签中删除刚创建的黑名单。

b. 验证云端是否能够正常接收设备的威胁日志。

i. 等待一段时间后，登录设备的标准界面**https://192.168.0.1:8443/**，在“监控 > 日志 > 威胁日志”中查看是否存在威胁日志，如果存在表示设备已产生威胁日志。

ii. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。在右上角菜单栏选择“威胁事件”，查看是否存在威胁事件，如果存在则表示云端能够正常接收设备的威胁日志。

1.2 企业边界天关旁挂策略路由直路（三层)

1.2.1 组网需求

适用产品和版本

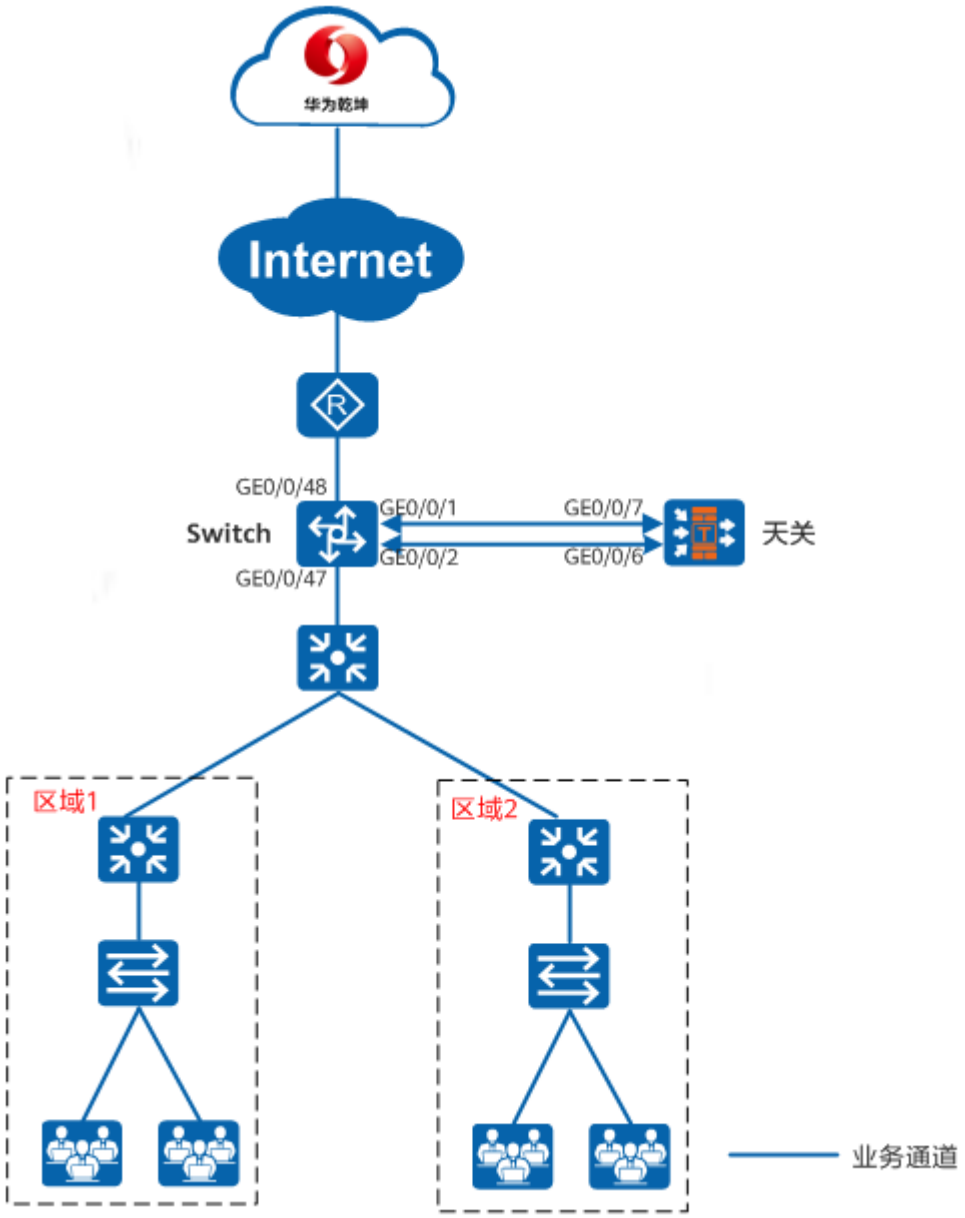
设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本	-

组网需求说明

客户已有网络通过交换机组建三层网络直接访问互联网；在已有网络基础上，直路交换机上旁路部署天关，采用接口对连接方式，将交换机上的流量通过策略路由引向天关，实现天关对于流量的旁路检测。

版权所有 © 华为技术有限公司

图 1-8 方案组网



本场景不设置独立管理口，直接使用GE0/0/7作为管理口。

约束和注意事项

- 天关和交换机采用三层网络连接。
- 天关连接交换机的上/下行接口需要加入同一组link-group。
  该部署方式下，不论上行还是下行链路故障，交换机上配置的策略路由都会自动失效，不将流量发送给天关。

版权所有 © 华为技术有限公司

1.2.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

配置思路

步骤1 登录华为乾坤控制台，配置全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

步骤2 配置交换机。

1. 配置连接天关的接口对。
2. 配置策略路由。

步骤3 配置天关。

- Eudemon1000E-T1
  a. 配置天关业务接口对，三层部署连接交换机，通过交换机的策略路由将流量引入天关进行检测。
  b. 配置天关路由。
  c. 配置边界防护与响应服务业务参数。

----结束

1.2.3 数据规划

项目	数据	说明
租户内网资产IP地址	● 区域1地址：192.168.55.0~192.168.55.255 ● 区域2地址：172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5	请向租户获取，此处为示例。
交换机	● GigabitEthernet0/0/1：10.1.10.2 ● GigabitEthernet0/0/2：10.2.10.2	请向租户获取，此处为示例。
天关	● 转发业务流量接口（接口对） – Eudemon1000E-T1 – 流量上行GE0/0/7：10.1.10.7 – 流量下行GE0/0/6：10.1.10.6	请向租户获取，此处为示例。

1.2.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

版权所有 © 华为技术有限公司

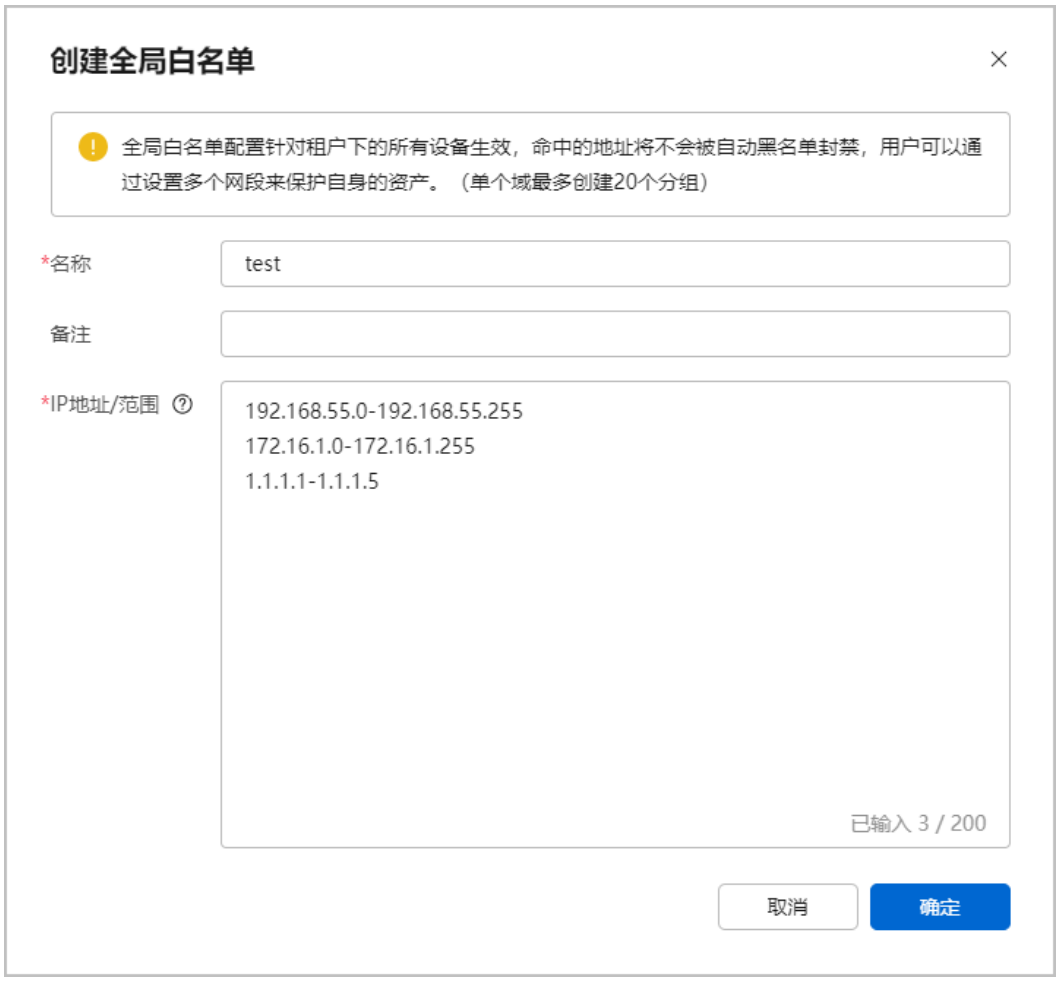
说明

已购买边界防护与响应服务时需要配置全局白名单。

操作步骤

1. 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。
2. 在“全局地址管理 > 全局白名单”页签中，单击“ + ”，按照下图所示配置全局白名单。

图 1-9 创建全局白名单



1.2.5 配置交换机

操作步骤

步骤1 配置接口对。

1. 配置接口GigabitEthernet 0/0/1。

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.10.2 24
[HUAWEI-GigabitEthernet0/0/1] quit
```


版权所有 © 华为技术有限公司

2. 配置接口GigabitEthernet 0/0/2。
```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] undo portswitch
[HUAWEI-GigabitEthernet0/0/2] ip address 10.2.10.2 24
[HUAWEI-GigabitEthernet0/0/2] quit
```

步骤2 配置策略路由。

1. 配置流分类。
```
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
```
2. 配置下行流行为和流策略，指定下一跳地址为10.2.10.6。
```
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect ip-nexthop 10.2.10.6
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
```
3. 配置上行流行为和流策略，指定下一跳地址为10.1.10.7。
```
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] redirect ip-nexthop 10.1.10.7
[HUAWEI-behavior-b2] quit
[HUAWEI] traffic policy p2
[HUAWEI-trafficpolicy-p2] classifier c1 behavior b2
[HUAWEI-trafficpolicy-p2] quit
```
4. 在下行口GigabitEthernet0/0/47应用流策略。
```
[HUAWEI] interface gigabitethernet 0/0/47
[HUAWEI-GigabitEthernet0/0/47] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/47] quit
[HUAWEI] quit
```
5. 在上行口GigabitEthernet0/0/48应用流策略。
```
[HUAWEI] interface gigabitethernet 0/0/48
[HUAWEI-GigabitEthernet0/0/48] traffic-policy p2 inbound
[HUAWEI-GigabitEthernet0/0/48] quit
[HUAWEI] quit
```

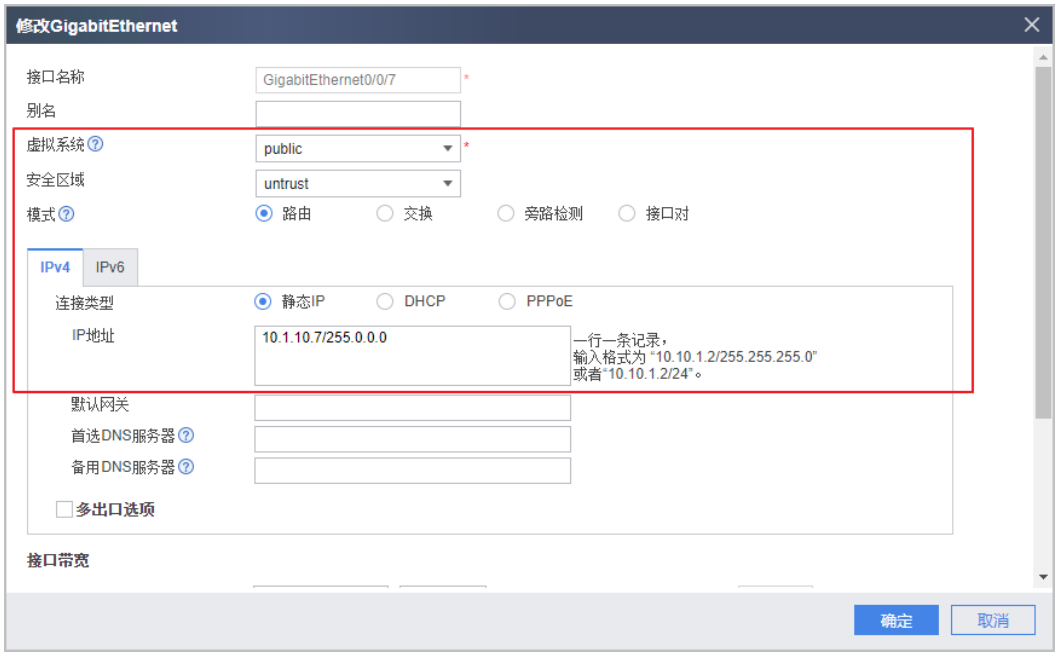
----结束

1.2.6 配置天关（Eudemon1000E-T1）

1. 配置业务接口对。
   a. 选择“网络 > 接口”。
   b. 单击上行接口GE0/0/7对应的，按照下图所示配置接口。

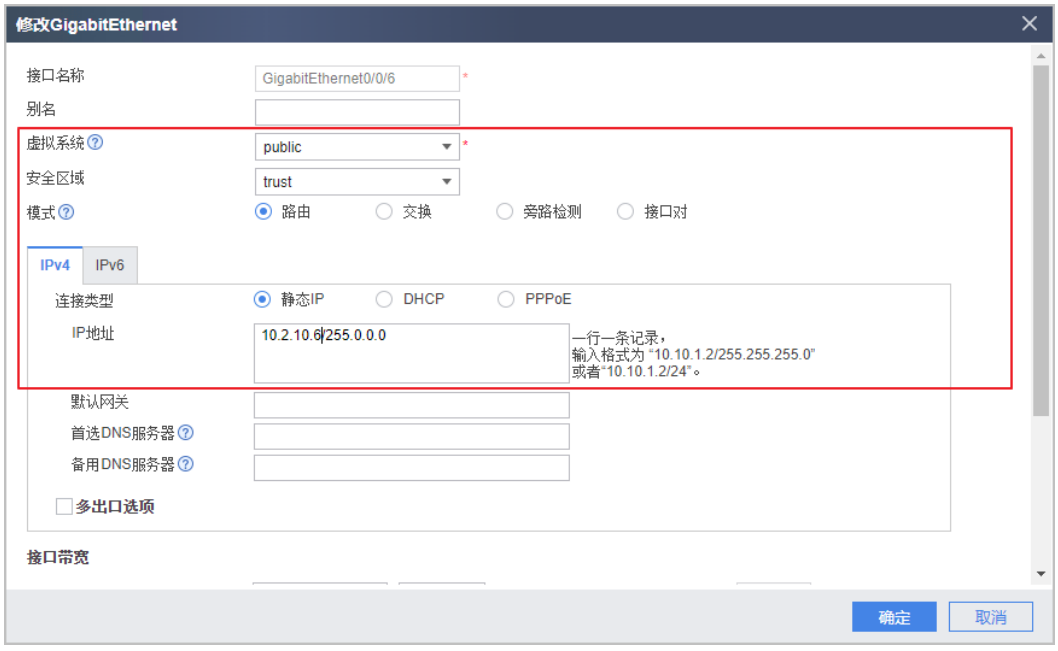
版权所有 © 华为技术有限公司

图 1-10 修改接口配置



c. 单击下行接口GE0/0/6对应的对应的，按照下图所示配置接口。

图 1-11 修改接口配置

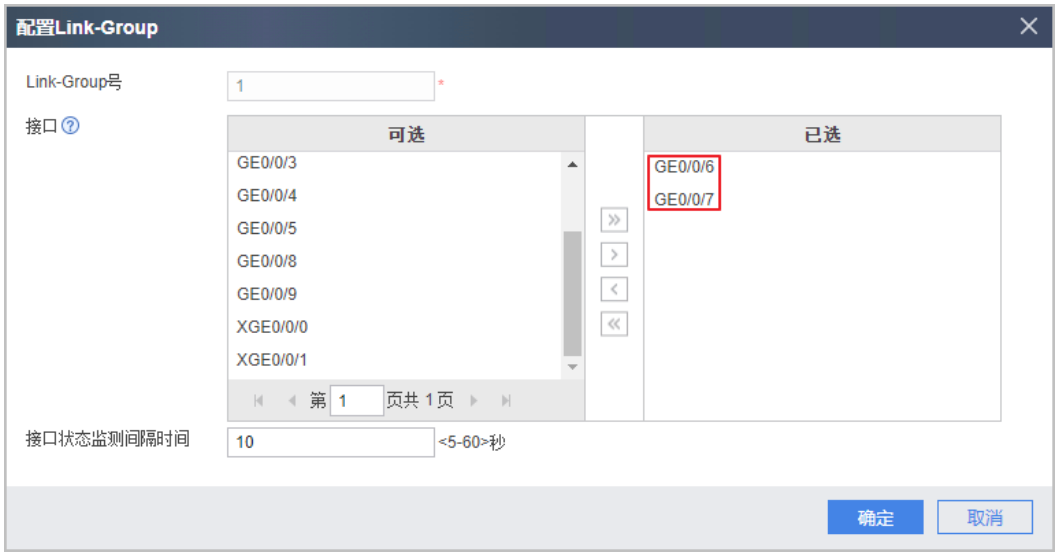


d. 选择“系统 > 高可靠性 > Link-Group”。

e. 配置Link-Group，添加GE0/0/7、GE0/0/6。

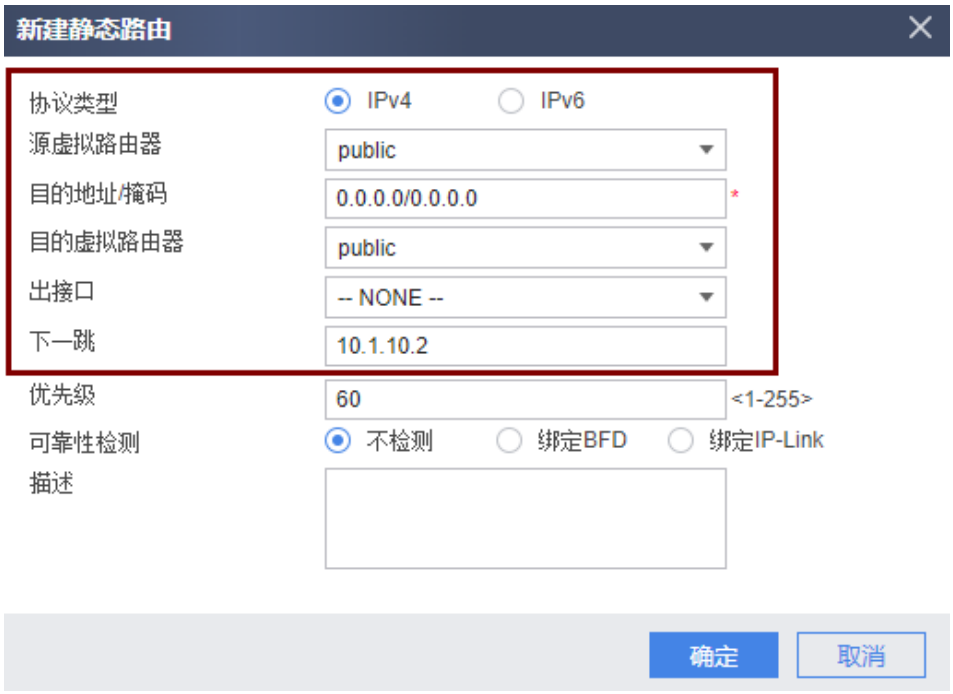
 版权所有 © 华为技术有限公司

图 1-12 配置 Link-Group



2. 配置路由。
   a. 选择“网络 > 路由 > 静态路由”。
   b. 配置数据流量出场景的静态路由。

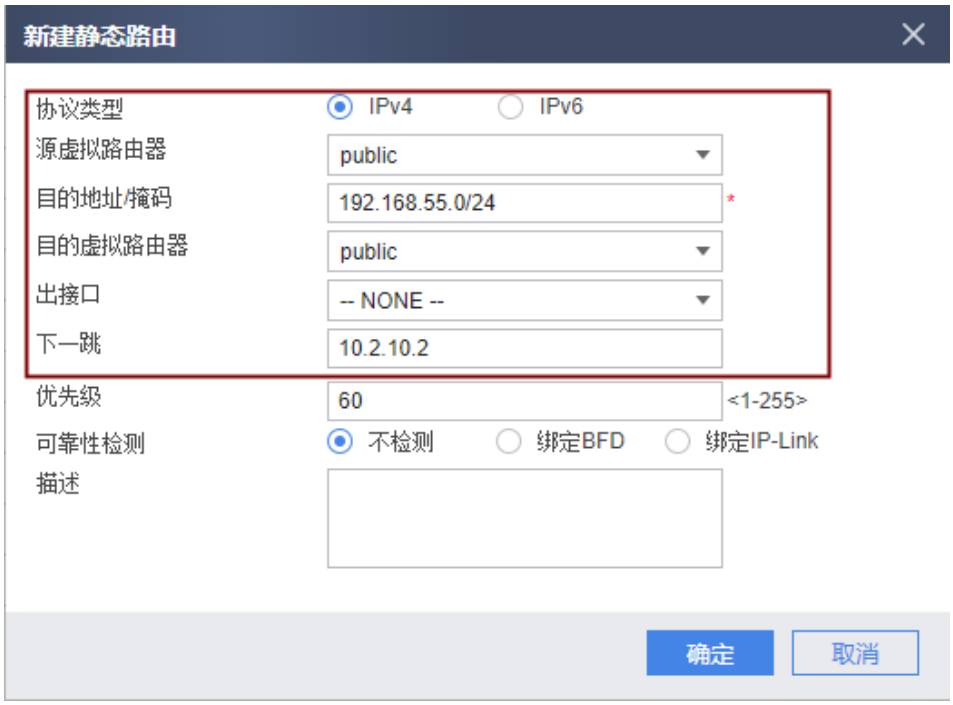
图 1-13 配置静态路由



   c. 配置数据流量入场景的静态路由。
   目的地址/掩码需要覆盖租户内网资产IP地址所在网段，如果涉及多个网段，则需要配置多条入场景的静态路由。本示例以配置区域1网段静态路由为例。

版权所有 © 华为技术有限公司

图 1-14 配置静态需求



3. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

图 1-15 配置系统时间

4. 配置业务参数（边界防护与响应服务）。
   a. 加载License。

      说明

      如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

      i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。
      ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。
   c. 确认安全策略已成功下发。

版权所有 © 华为技术有限公司

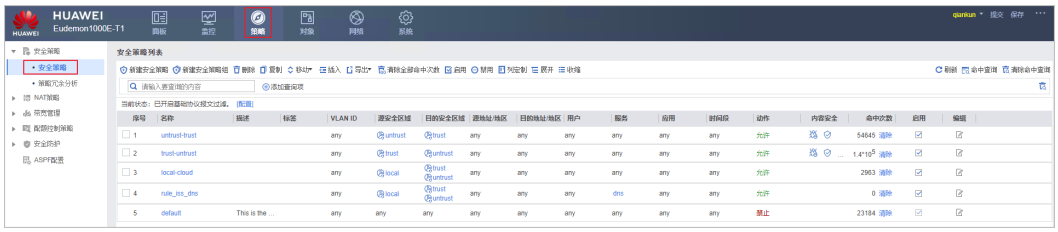
设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

安全策略下发后，如图1-16所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

说明

如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

图 1-16 安全策略



d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-17 特征库升级

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-18 保存配置

1.2.7 结果验证

步骤1 验证设备上线是否成功、业务套餐是否激活成功。

1. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。

   设备状态为“正常”表示设备已上线成功。

版权所有 © 华为技术有限公司

2. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。
   套餐状态为“正常”表示套餐已激活成功。

步骤2 验证边界防护与响应服务是否正常。

1. 检查黑名单是否能够正常下发。
   a. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”，在右上角菜单栏选择“黑白名单”。
   b. 在“黑名单 > IP黑名单”页签中创建并部署一个黑名单。
   c. 登录设备的标准界面**https://192.168.0.1:8443/**。
      - Eudemon1000E-T1：在“策略 > 安全防护 > 黑名单”中检查是否存在下发的黑名单。

      如果存在则表示黑名单能够正常下发。

      说明

      - 请获取一个当前没有业务使用的IP地址作为黑名单，否则可能会影响当前业务。
      - 验证后请务必在“黑名单 > IP黑名单”页签中删除刚创建的黑名单。
2. 验证云端是否能够正常接收设备的威胁日志。
   a. 等待一段时间后，登录设备的标准界面**https://192.168.0.1:8443/**，在“监控 > 日志 > 威胁日志”中查看是否存在威胁日志，如果存在表示设备已产生威胁日志。
   b. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。在右上角菜单栏选择“威胁事件”，查看是否存在威胁事件，如果存在则表示云端能够正常接收设备的威胁日志。

----结束

1.3 企业边界天关旁路镜像流状态检测

1.3.1 组网需求

适用产品和版本

设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本	-

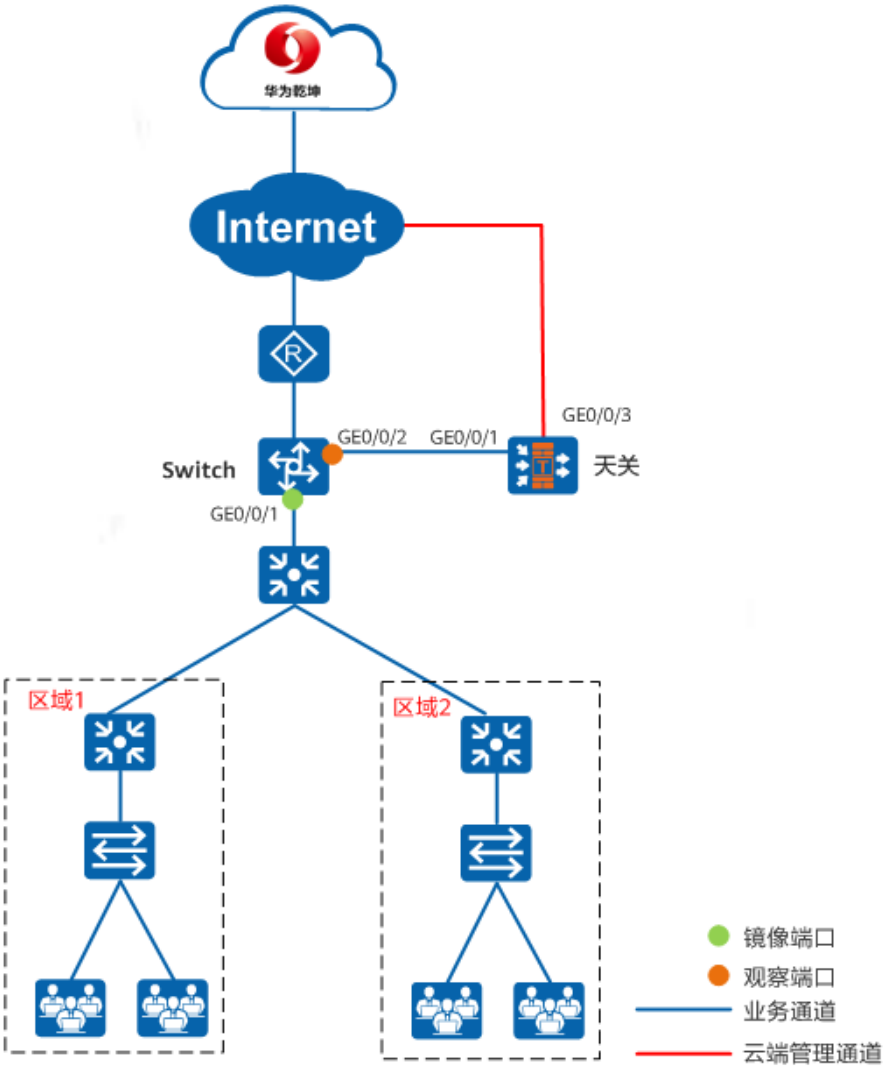
组网需求说明

如**图1-19**所示，在某企业网络出口，核心交换机Switch上行通过路由器访问外网，天关旁挂于Switch。华为乾坤对业务流量提供安全状态检测功能。

下图以Eudemon1000E-T1为例，配置天关上的二层接口GE0/0/1为旁路检测模式，与Switch的观察端口直连，并使用GE0/0/3上报云端。

版权所有 © 华为技术有限公司

图 1-19 方案组网



约束或注意事项

- 本场景中天关设备仅提供安全状态检测的功能，不对威胁事件进行自动阻断，云端配置的黑名单也不会生效。
- 本场景中天关设备旁挂的核心交换机需要支持镜像功能。
- 交换机上需要将镜像端口入方向和出方向的报文都镜像到观察端口，即双向镜像。

1.3.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

版权所有 © 华为技术有限公司

配置思路

1. 登录华为乾坤控制台，根据租户内网资产IP地址配置全局白名单，提升安全状态检测的准确性。
2. 配置交换机：
   a. 配置Switch的GigabitEthernet0/0/2为观察端口，该端口直连天关，Switch将通过镜像将流量上送到天关进行检测。
   b. 配置Switch的GigabitEthernet0/0/1为镜像端口，开启端口镜像功能。
3. 配置天关：
   a. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   b. 配置检测接口GE0/0/1为旁路检测模式，该二层接口与Switch的观察端口直连。
   c. 配置边界防护与响应服务的业务参数。
   d. 将GE0/0/1和对应VLAN都加入trust安全域，并配置旁路检测所需要的安全策略。

1.3.3 数据规划

项目	数据	说明
租户内网资产IP地址	● 区域1地址：192.168.55.0-192.168.55.255 ● 区域2地址：172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5	请向租户获取，此处为示例。
交换机	GigabitEthernet0/0/2	观察端口。
	GigabitEthernet0/0/1	镜像端口。
天关	GE0/0/1	流量检测端口。
	GE0/0/3：172.16.10.10/24	云端管理接口，IP地址请向租户获取，此处为示例。

1.3.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

说明

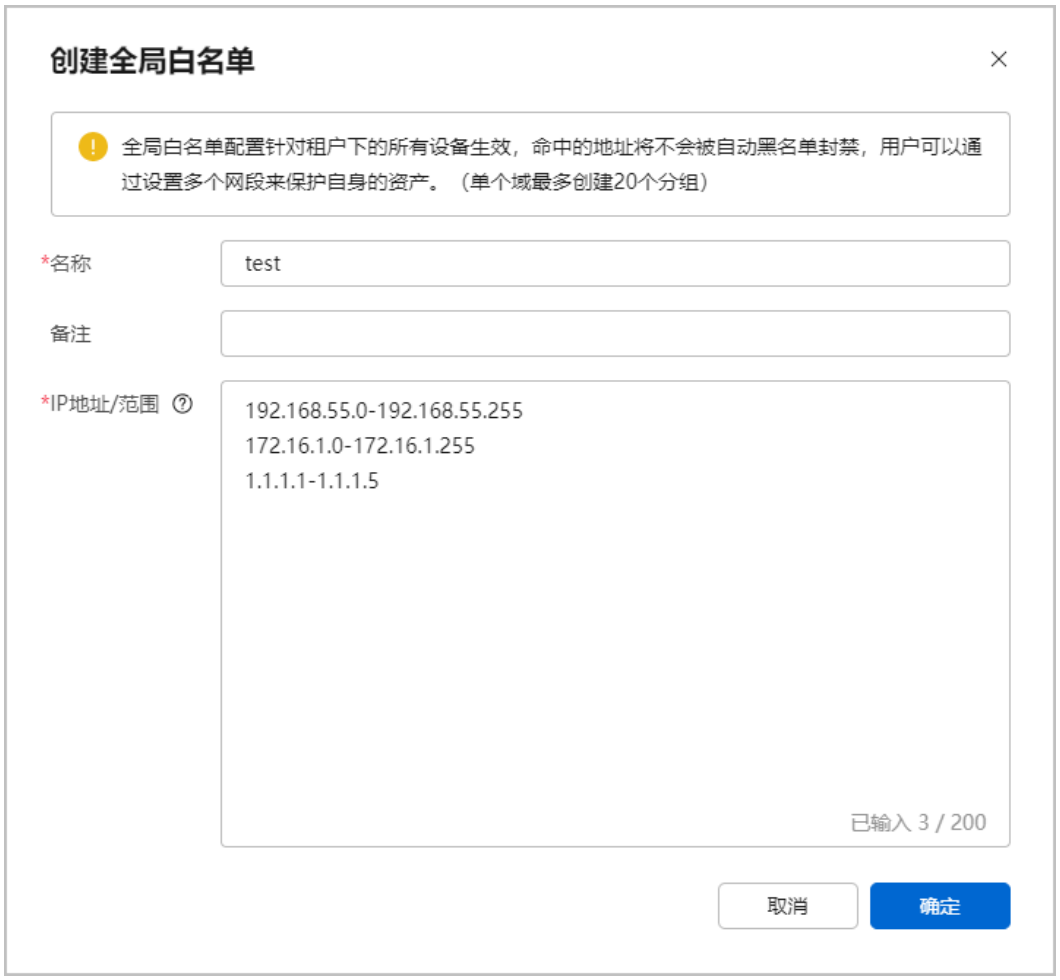
已购买边界防护与响应服务时需要配置全局白名单。

版权所有 © 华为技术有限公司

操作步骤

1. 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。
2. 在“全局地址管理 > 全局白名单”页签中，单击“ + ”，按照下图所示配置全局白名单。

图 1-20 创建全局白名单



1.3.5 配置交换机

操作步骤

1. 配置观察端口。

   配置Switch的GigabitEthernet0/0/2为观察端口，该端口直连天关，Switch将通过镜像将流量上送到天关进行检测。

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname Switch
   [Switch] observe-port 1 interface gigabitEthernet 0/0/2
   ```

2. 配置镜像端口。

   配置Switch的GigabitEthernet0/0/1为镜像端口，开启端口镜像功能。

   ```
   [Switch] interface gigabitEthernet 0/0/1
   [Switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 both
   [Switch-GigabitEthernet0/0/1] quit
   ```


版权所有 © 华为技术有限公司

1.3.6 配置天关（Eudemon1000E-T1）

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置云端管理接口。

   GE0/0/3默认为二层接口，请按照如下方式配置成三层接口。

   a. 选择“网络 > 接口”。

   b. 单击GE0/0/3对应的，按照如下参数配置接口。

安全区域	untrust
模式	路由
IPv4	
IP地址	172.16.10.10/24

   c. 配置云端管理接口的静态路由。

      i. 选择“网络 > 路由 > 静态路由”。

      ii. 单击“静态路由列表”区域下的“新建”，添加静态路由。下一跳配置为网关地址。

图 1-21 配置静态路由

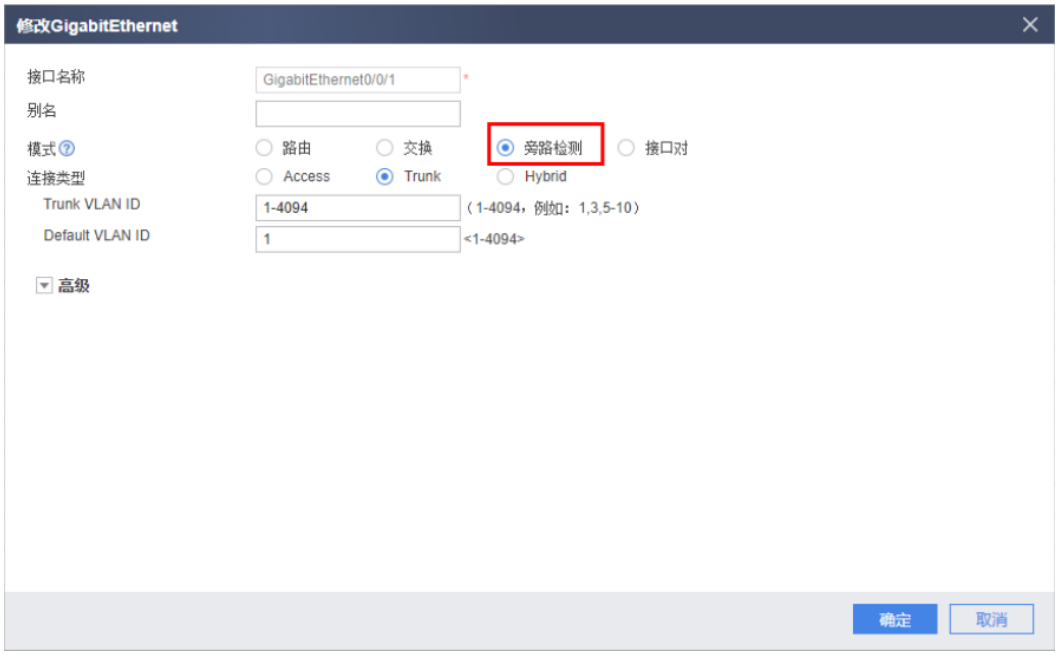
3. 配置检测接口GE0/0/1为旁路检测模式，该二层接口与Switch的观察端口直连。

   a. 选择“网络 > 接口”。

版权所有 © 华为技术有限公司

b. 单击GE0/0/1对应的，按照下图所示配置接口，注意“模式”需要选择“旁路检测”。

图 1-22 配置接口



4. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

图 1-23 配置系统时间

5. 配置业务参数（边界防护与响应服务）。

a. 加载License。

说明

如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。

ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。

 版权所有 © 华为技术有限公司

c. 确认安全策略已成功下发。

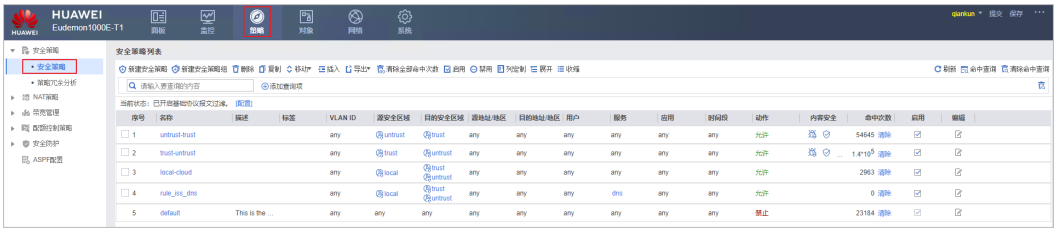
设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

安全策略下发后，如图1-24所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

说明

如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

图 1-24 安全策略

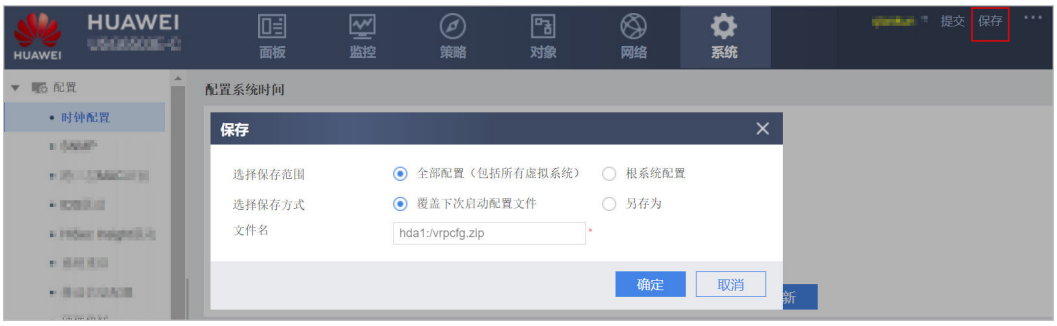


d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-25 特征库升级

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-26 保存配置

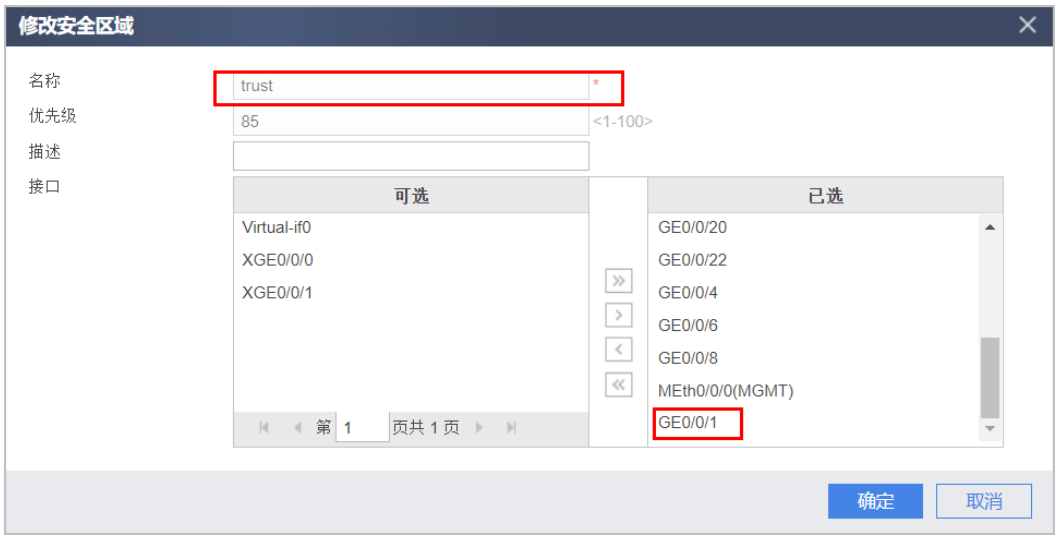


6. 配置旁路检测所需要的安全策略。

a. 选择“网络 > 安全区域”。将GE0/0/1加入trust安全区域。

 版权所有 © 华为技术有限公司

图 1-27 修改安全区域



b. 选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置名称为“trust-trust”的安全策略，源安全区域为trust，目的安全区域为trust，反病毒采用新建的AV_default，入侵防御采用新建的IPS_default，动作为“允许”。

图 1-28 配置安全策略

1.3.7 结果验证

1. 验证设备上线是否成功、业务套餐是否激活成功。

版权所有 © 华为技术有限公司

a. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。

设备状态为“正常”表示设备已上线成功。

b. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。

套餐状态为“正常”表示套餐已激活成功。

2. 验证云端是否能够正常接收设备的威胁日志。

a. 等待一段时间后，登录设备的标准界面**https://192.168.0.1:8443/**，在“监控 > 日志 > 威胁日志”中查看是否存在威胁日志，如果存在表示设备已产生威胁日志。

b. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。在右上角菜单栏选择“威胁事件”，查看是否存在威胁事件，如果存在则表示云端能够正常接收设备的威胁日志。

1.4 企业边界天关旁挂直路检测场景

1.4.1 组网需求

适用产品和版本

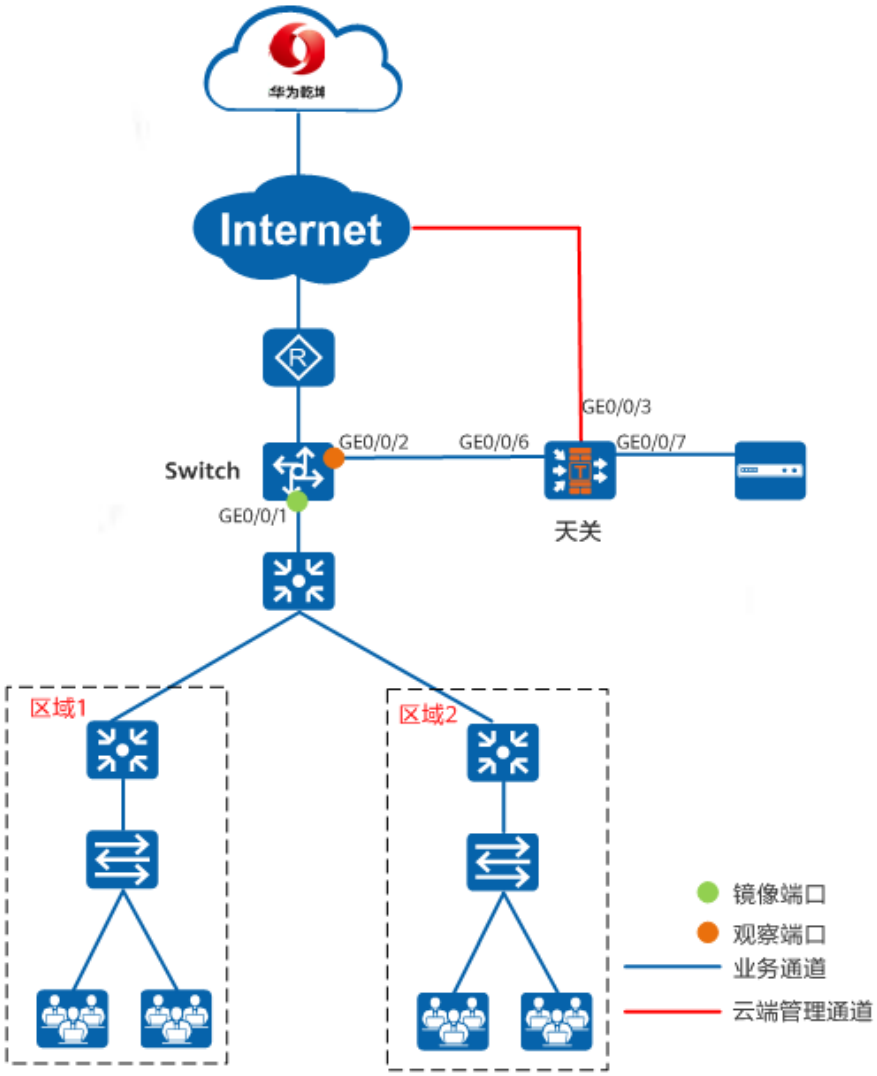
设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本	-

组网需求说明

在某企业网络出口，核心交换机Switch上行通过路由器访问外网，天关在企业边界只做旁挂直路检测场景。华为乾坤对业务流量提供安全状态检测功能。

版权所有 © 华为技术有限公司

图 1-29 方案组网



约束或注意事项

- 本场景中天关设备仅提供安全状态检测的功能，不对威胁事件进行自动阻断，云端配置的黑名单也不会生效。
- 本场景中天关设备旁挂的核心交换机需要支持镜像功能。
- 交换机上需要将镜像端口入方向和出方向的报文都镜像到观察端口，即双向镜像。

1.4.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

版权所有 © 华为技术有限公司

配置思路

1. 登录**华为乾坤云服务控制台**，根据租户内网资产IP地址配置全局白名单，提升安全状态检测的准确性。
2. 配置交换机：
   a. 配置Switch的GigabitEthernet0/0/2为观察端口，该端口直连天关，Switch将通过镜像将流量上送到天关进行检测。
   b. 配置Switch的GigabitEthernet0/0/1为镜像端口，开启端口镜像功能。
3. 配置天关：
   a. 配置云端管理接口，用于天关于云端对接，包括设备向云端注册、接收云端下发配置等。
   b. 配置GE0/0/7和GE0/0/6为为接口对模式，GE0/0/6与Switch的观察端口直连。
   c. 配置边界防护与响应服务业务参数。

1.4.3 数据规划

项目	数据	说明
租户内网资产IP地址	• 区域1地址：192.168.55.0-192.168.55.255 • 区域2地址：172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5	请向租户获取，此处为示例。
交换机	GigabitEthernet0/0/2	观察端口。
	GigabitEthernet0/0/1	镜像端口。
天关	• USG6603F-C – 转发镜像流量Bypass接口对：GE0/0/6和GE0/0/7 – 云端管理接口GE0/0/3：172.16.10.10/24 – 漏洞扫描和云日志审计接口GE0/0/2：192.168.56.10/24 • Eudemon1000E-T1 – 转发镜像流量接口对：GE0/0/6和GE0/0/7 – 云端管理接口GE0/0/3：172.16.10.10/24	请向租户获取，此处为示例。

版权所有 © 华为技术有限公司

1.4.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

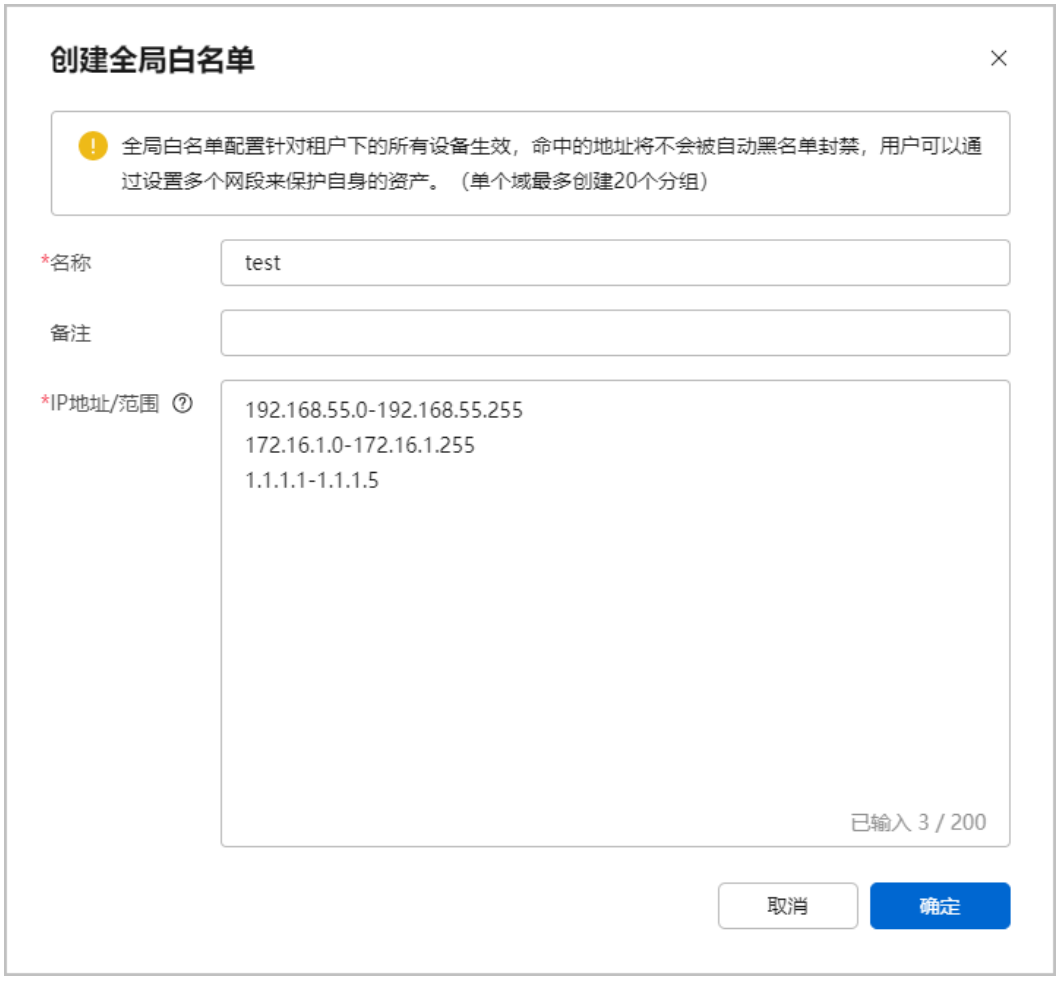
说明

已购买边界防护与响应服务时需要配置全局白名单。

操作步骤

1. 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。
2. 在“全局地址管理 > 全局白名单”页签中，单击“ + ”，按照下图所示配置全局白名单。

图 1-30 创建全局白名单



版权所有 © 华为技术有限公司

1.4.5 配置交换机

操作步骤

1. 配置Switch的GigabitEthernet0/0/2为观察端口，该端口直连天关，Switch将通过镜像将流量上送到天关进行检测。
```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] observe-port 1 interface gigabitEthernet 0/0/2
```
2. 配置Switch的GigabitEthernet0/0/1为镜像端口，开启端口镜像功能。
```
[Switch] interface gigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] port-mirroring to observe-port 1 both
[Switch-GigabitEthernet0/0/1] quit
```

1.4.6 配置天关（Eudemon1000E-T1）

操作步骤

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置云端管理接口。

   GE0/0/3默认为二层接口，请按照如下方式配置成三层接口。

   a. 选择“网络 > 接口”。

   b. 单击GE0/0/3对应的，按照如下参数配置接口。

安全区域	untrust
模式	路由
IPv4	
IP地址	172.16.10.10/24

   c. 配置云端管理接口的静态路由。

      i. 选择“网络 > 路由 > 静态路由”。

      ii. 单击“静态路由列表”区域下的“新建”，添加静态路由。下一跳配置为网关地址。

版权所有 © 华为技术有限公司

图 1-31 配置静态路由

3. 配置业务接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/6，按如下参数配置，单击“确定”。

安全区域	trust
模式	接口对

   c. 参考上述步骤按如下参数配置GE0/0/7接口。

安全区域	untrust
模式	接口对

4. 配置业务接口对。
   a. 选择“网络 > 接口对”。
   b. 单击“新建”，按如下参数配置，单击“确定”。

名称	interface_bypass1
工作模式	不同口进出
成员	
接口一	GE0/0/6
接口二	GE0/0/7

版权所有 © 华为技术有限公司

允许的VLAN	1-4094
接口对状态同步	不开启

5. 配置业务参数（边界防护与响应服务）。

   a. 加载License。

   说明

   如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

   i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。

   ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。

   c. 确认安全策略已成功下发。

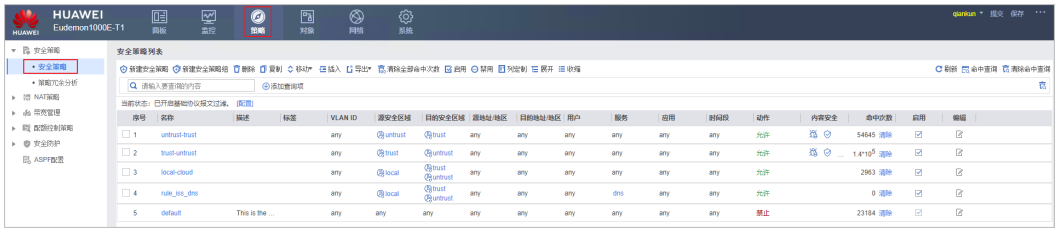
   设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

   安全策略下发后，如图1-32所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

   说明

   如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

图 1-32 安全策略



   d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-33 特征库升级

   e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

版权所有 © 华为技术有限公司

图 1-34 保存配置

1.4.7 结果验证

步骤1 验证设备上线是否成功、业务套餐是否激活成功。

1. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。

   设备状态为“正常”表示设备已上线成功。

2. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。

   套餐状态为“正常”表示套餐已激活成功。

步骤2 验证边界防护与响应服务是否正常。

1. 检查黑名单是否能够正常下发。

   a. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”，在右上角菜单栏选择“黑白名单”。

   b. 在“黑名单 > IP黑名单”页签中创建并部署一个黑名单。

   c. 登录设备的标准界面**https://192.168.0.1:8443/**。

      - Eudemon1000E-T1：在“策略 > 安全防护 > 黑名单”中检查是否存在下发的黑名单。

   如果存在则表示黑名单能够正常下发。

   说明

   - 请获取一个当前没有业务使用的IP地址作为黑名单，否则可能会影响当前业务。
   - 验证后请务必在“黑名单 > IP黑名单”页签中删除刚创建的黑名单。

2. 验证云端是否能够正常接收设备的威胁日志。

   a. 等待一段时间后，登录设备的标准界面**https://192.168.0.1:8443/**，在“监控 > 日志 > 威胁日志”中查看是否存在威胁日志，如果存在表示设备已产生威胁日志。

   b. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。在右上角菜单栏选择“威胁事件”，查看是否存在威胁事件，如果存在则表示云端能够正常接收设备的威胁日志。

----结束

版权所有 © 华为技术有限公司

1.5 企业内部存在 NAT 转换场景

1.5.1 组网需求

适用产品和版本

设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本	-

组网需求说明

本方案适用于客户内网中存在NAT设备的场景。

如果客户内网中存在NAT设备，内网资产使用NAT后地址访问外部区域，导致天关检测到威胁事件的源地址都是NAT后地址，进而无法识别失陷主机的真实地址。

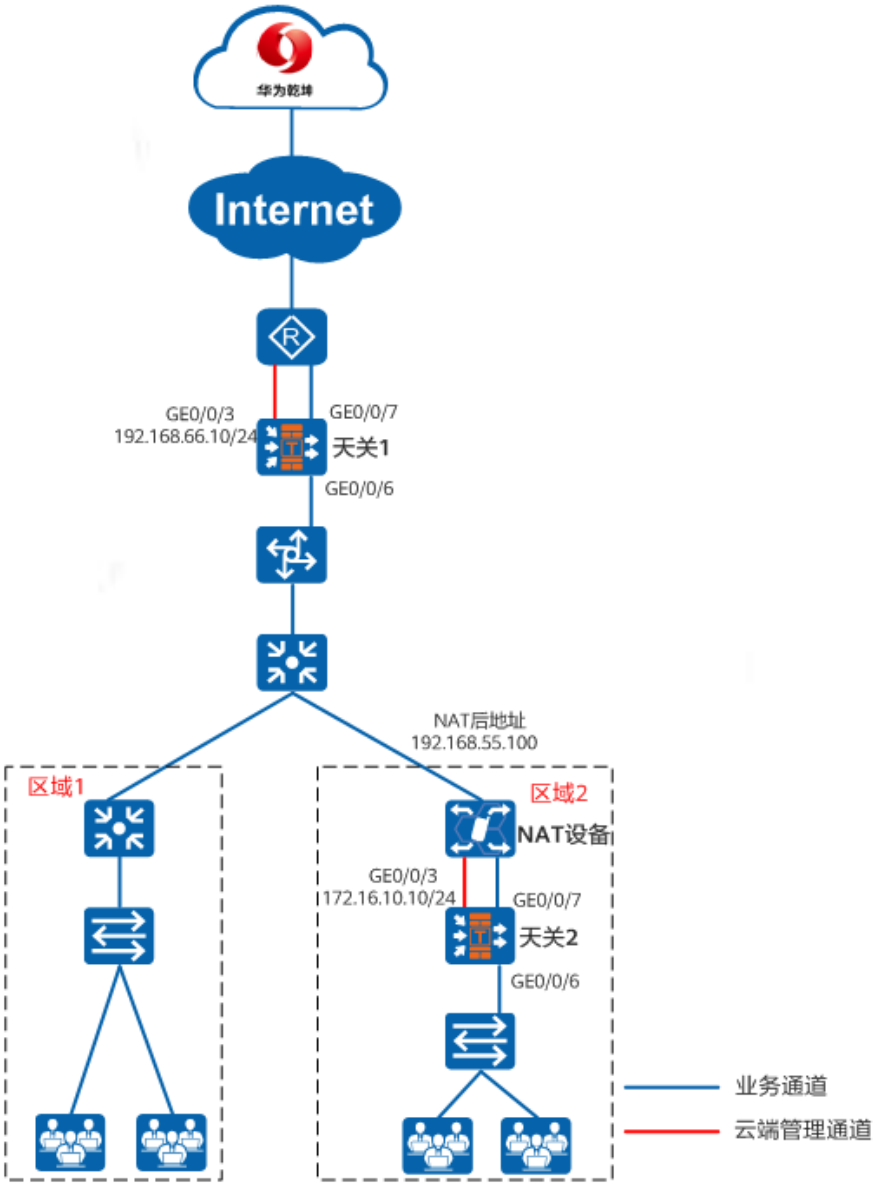
为解决上述问题，采用如下图所示方案。

- 在NAT设备前部署天关2，用于检测区域2的威胁事件，云端通过天关2的威胁日志识别区域2的失陷主机。
- 在出口网关前部署天关1，用于检测非NAT区域（区域1）的威胁事件。
- 在天关1上将区域2NAT后的地址配置为白名单，保证天关1不检测区域2发出的流量，防止NAT后地址被误封禁，同时缓解天关1的检测性能压力。

下图以Eudemon1000E-T1的GE0/0/6和GE0/0/7为例，用于转发内外网的业务流量，同时使用三层接口GE0/0/3与云端对接。

版权所有 © 华为技术有限公司

图 1-35 方案组网



约束或注意事项

- 请按照本章介绍的步骤配置，在天关1开启安全检测前，必须先在天关1上将区域2NAT后的地址192.168.55.100配置为白名单，保证天关1不检测区域2发出的流量，防止NAT后地址被误封禁。
- Eudemon1000E-T1接口使用限制：
  - Eudemon1000E-T1不支持硬件Bypass功能。
  - 默认情况下，接口编号相邻的接口两两组成二层接口对。
  - 奇数编号接口用于连接上行设备，偶数编号接口用于连接下行局域网设备

 版权所有 © 华为技术有限公司

1.5.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

配置思路

1. 登录华为乾坤控制台，配置全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。
2. 登录天关2，主要配置一下内容：
   a. 配置业务接口对，用于转发内外网业务流量。
   b. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   c. 配置边界防护与响应服务业务参数。
3. 登录天关1，主要配置以下内容：
   a. 配置业务接口对，用于转发内外网业务流量。
   b. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   c. 配置设备白名单，将区域2NAT后的地址192.168.55.100配置为白名单，保证天关1不检测区域2发出的流量。
   d. 配置边界防护与响应服务业务参数。

1.5.3 数据规划

项目	数据	说明
租户内网资产IP地址	● 区域1地址：192.168.55.0-192.168.55.255 ● 区域2地址：172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5	请向租户获取，此处为示例。
转发业务流量接口（Bypass接口对）	● Eudemon1000E-T1 – 天关1：GE0/0/7和GE0/0/6 – 天关2：GE0/0/7和GE0/0/6	-
区域2NAT后地址	192.168.55.100	区域2中所有资产使用该NAT后地址访问其他区域（外网或区域1）。

版权所有 © 华为技术有限公司

项目	数据	说明
云端管理接口	• 天关1GE0/0/3：192.168.66.10/24 • 天关2GE0/0/3：172.16.10.10/24	请向租户获取，此处为示例。

1.5.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

说明

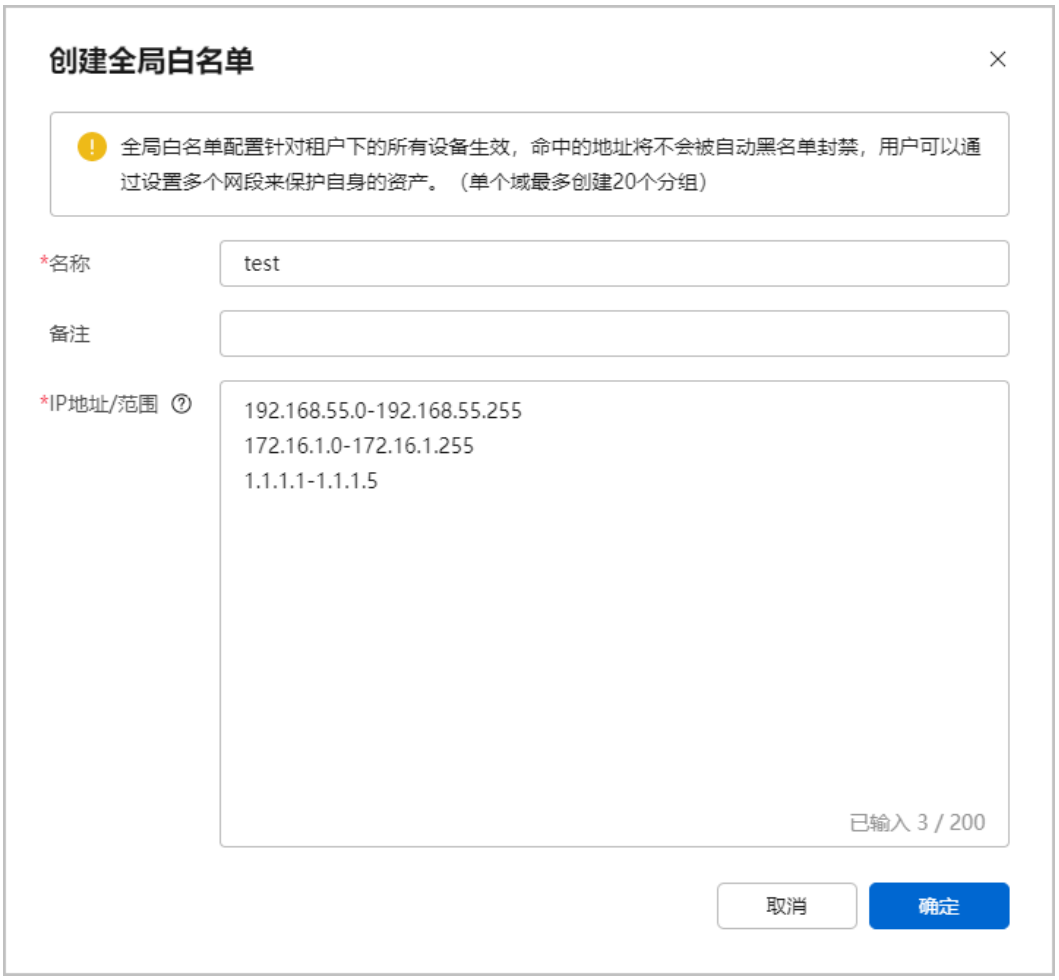
已购买边界防护与响应服务时需要配置全局白名单。

操作步骤

1. 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。
2. 在“全局地址管理 > 全局白名单”页签中，单击“ + ”，按照下图所示配置全局白名单。

版权所有 © 华为技术有限公司

图 1-36 创建全局白名单



1.5.5 配置天关（Eudemon1000E-T1）

背景信息

请按照如下顺序先配置天关2，再配置天关1。

配置天关 2

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置业务接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/6，按如下参数配置，单击“确定”。

安全区域	trust
模式	接口对

   c. 参考上述步骤按如下参数配置GE0/0/7接口。

版权所有 © 华为技术有限公司

安全区域	untrust
模式	接口对

3. 配置业务接口对。
   a. 选择“网络 > 接口对”。
   b. 单击“新建”，按如下参数配置，单击“确定”。

名称	interface_bypass1
工作模式	不同口进出
成员	
接口一	GE0/0/6
接口二	GE0/0/7
允许的VLAN	1-4094
接口对状态同步	不开启

4. 配置云端管理接口。
   GE0/0/3默认为二层接口，请按照如下方式配置成三层接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/3对应的，按照如下参数配置接口。

安全区域	untrust
模式	路由
IPv4	
IP地址	172.16.10.10/24

   c. 配置云端管理接口的静态路由。
      i. 选择“网络 > 路由 > 静态路由”。
      ii. 单击“静态路由列表”区域下的“新建”，添加静态路由。下一跳配置为网关地址。

 版权所有 © 华为技术有限公司

图 1-37 配置静态路由

5. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

图 1-38 配置系统时间

6. 配置业务参数（边界防护与响应服务）。
   a. 加载License。

      说明

      如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

      i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。
      ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。

版权所有 © 华为技术有限公司

c. 确认安全策略已成功下发。

设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

安全策略下发后，如图1-39所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

说明

如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

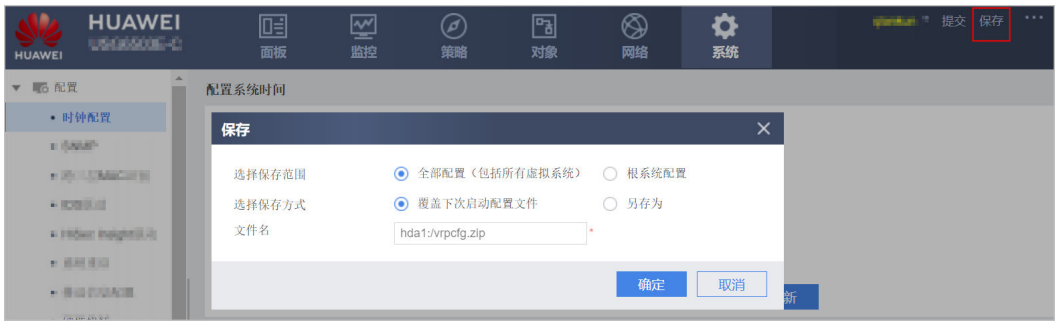
图 1-39 安全策略

d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-40 特征库升级

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-41 保存配置



配置天关 1

1. 参照步骤1，登录天关1。
2. 参照步骤2和步骤3，配置业务接口对。

版权所有 © 华为技术有限公司

3. 参照**步骤4**，根据数据规划配置云端管理接口。
4. 参照**步骤5**，配置设备系统时间。
5. 登录华为乾坤控制台，将区域2NAT后的地址192.168.55.100配置为白名单，并下发给天关1。
   a. 选择“ ≡ > 我的服务 > 边界防护与响应 > 黑白名单”。
   b. 在“白名单”页签中，单击“创建”，按照下图所示配置白名单。

图 1-42 配置白名单

6. 参照**步骤6**，配置边界防护与响应服务业务参数。

1.5.6 结果验证

1. 验证设备上线是否成功、业务套餐是否激活成功。
   a. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。
      设备状态为“正常”表示设备已上线成功。
   b. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。
      套餐状态为“正常”表示套餐已激活成功。

版权所有 © 华为技术有限公司

2. 验证边界防护与响应服务是否正常。

   华为乾坤控制台可以检测到源地址为172.16.1.0-172.16.1.255、1.1.1.1-1.1.1.5的失陷主机，检测不到源地址为192.168.55.100的失陷主机，表示边界边界防护与响应服务已正常运行。

1.6 企业内部存在 DNS 服务器场景

1.6.1 组网需求

适用产品和版本

设备	版本	备注
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本	-

组网需求说明

本方案适用企业内网有DNS服务器的场景。

该场景下，企业内网主机使用DNS服务器代理后的IP地址访问外部区域，出口天关1检测到威胁事件的源地址都是DNS服务器代理后的IP地址，非真实的内网IP地址，进而导致客户无法对失陷主机做对应处理。

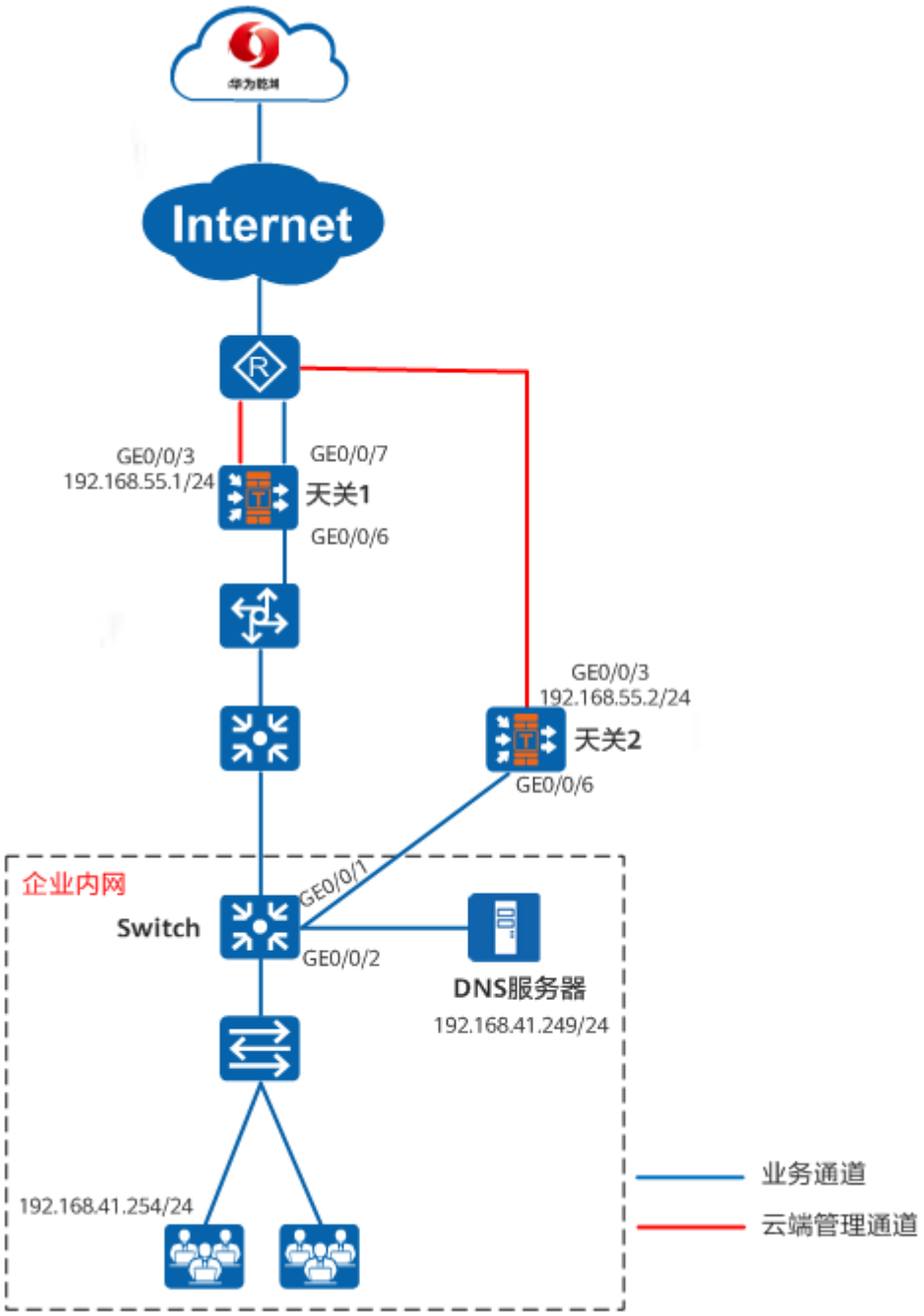
针对上述问题，采用如下方案，如图1-43所示。增加天关2，将用户访问DNS服务器的流量镜像到天关2，并把检测日志上送到华为乾坤，华为乾坤根据天关2的威胁日志识别真正的失陷主机。

说明

下图以Eudemon1000E-T1的GE0/0/7和GE0/0/6为例，组成业务接口对，用于转发内外网的业务流量，同时使用三层接口GE0/0/3与云端对接。

版权所有 © 华为技术有限公司

图 1-43 方案组网



约束或注意事项

- 对交换机的要求：
  天关2对应的交换机需支持源+目的协议的镜像，建议只引流DNS流量。
- Eudemon1000E-T1接口使用限制：
  - Eudemon1000E-T1不支持硬件Bypass功能。
  - 奇数编号接口用于连接上行设备，偶数编号接口用于连接下行局域网设备。
  - 默认情况下，接口编号相邻的接口两两组成二层接口对。

版权所有 © 华为技术有限公司

1.6.2 配置思路

前提条件

- 已购买相应的服务。
- 除天关外的其他设备已完成网络连接，确保通信正常。

配置思路

1. 登录华为乾坤控制台，配置全局白名单，增加租户的全部内网地址段，保证对内网流量的检测。
2. 配置交换机到DNS服务器的流量为镜像流量（回程流量不需要检测），并且保证镜像流量可以到达天关2镜像口。
3. 配置天关1。
   a. 配置业务接口对，用于转发内外网业务流量。
   b. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   c. 配置边界防护与响应服务业务参数。
4. 配置天关2。
   a. 配置镜像流量接收口为旁路检测模式。
   b. 配置云端管理接口，用于天关与云端对接，包括设备向云端注册、接收云端下发配置等。
   c. 配置边界防护与响应服务业务参数。

1.6.3 数据规划

表 1-1 数据规划

项目		数据	说明
租户内网资产IP地址		192.168.41.0-192.168.41.255	请向租户获取，此处仅为示例。
天关1	转发业务流量接口	GE0/0/7和GE0/0/6	-
	云端管理接口	GE0/0/3：192.168.55.1/24	-
天关2	镜像流量接收口（旁路检测模式）	GE0/0/6	此处请使用偶数端口。
	云端管理接口	GE0/0/3：192.168.55.2/24	-
交换机	端口规划	• 观察端口：GigabitEthernet0/0/1 • 镜像端口：GigabitEthernet0/0/2	-

版权所有 © 华为技术有限公司

1.6.4 配置全局白名单

背景信息

将租户全部的内网资产IP地址添加到全局白名单，防止租户内网资产IP地址被云端（包括云端自动下发、云端安全服务人员）错误下发黑名单。

说明

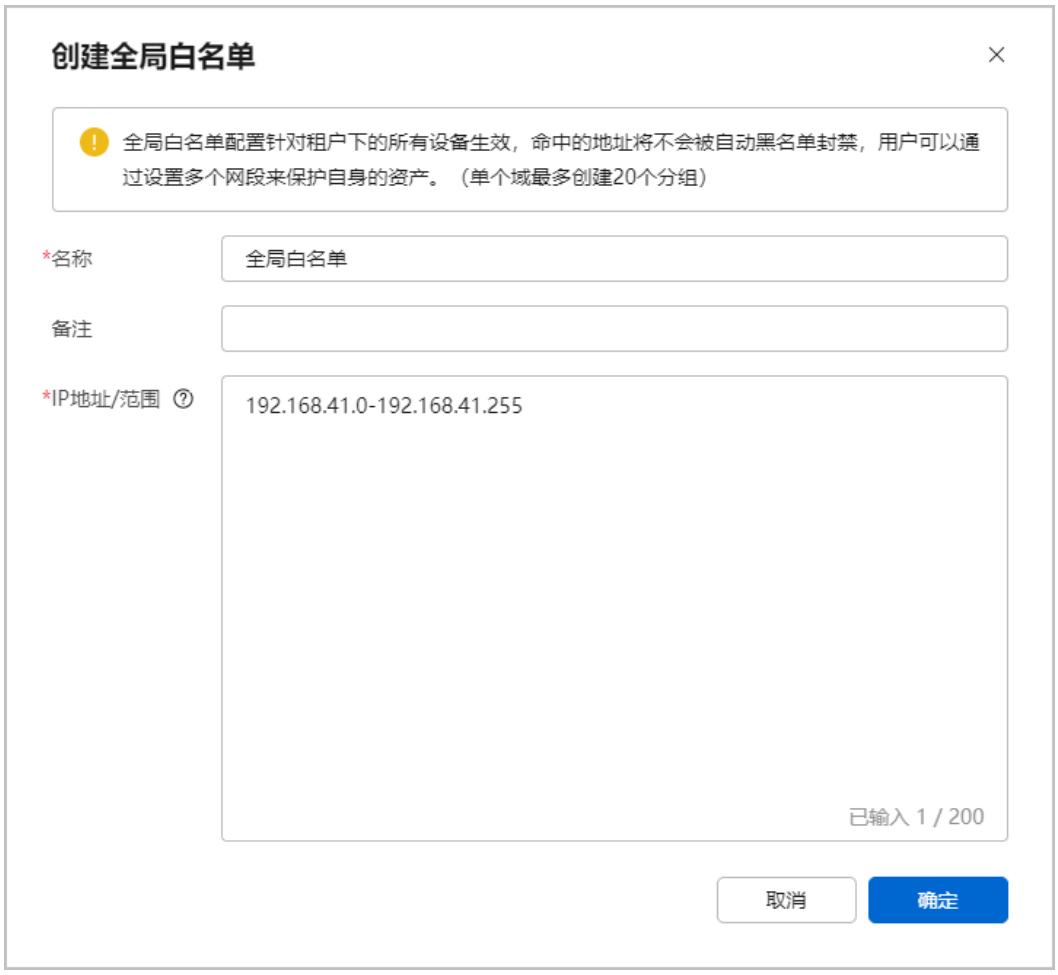
已购买边界防护与响应服务时需要配置全局白名单。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应 > 服务配置 > 地址安全域管理”。

步骤2 在“全局白名单”页签中，单击“创建”，根据数据规划配置全局白名单。

图 1-44 配置全局白名单



----结束

 版权所有 © 华为技术有限公司

1.6.5 配置交换机

操作步骤

步骤1 配置接口GigabitEthernet0/0/1为本地观察端口。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] observe-port 1 interface gigabitEthernet 0/0/1
```

步骤2 配置接口GigabitEthernet0/0/2为流量镜像端口，并将其出方向绑定到本地观察端口。

```
[Switch] interface gigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] port-mirroring to observe-port 1 outbound
```

----结束

1.6.6 配置天关（Eudemon1000E-T1）

配置天关 1

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置业务接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/6，按如下参数配置，单击“确定”。

安全区域	trust
模式	接口对

   c. 参考上述步骤按如下参数配置GE0/0/7接口。

安全区域	untrust
模式	接口对

3. 配置业务接口对。
   a. 选择“网络 > 接口对”。
   b. 单击“新建”，按如下参数配置，单击“确定”。

名称	interface_bypass1
工作模式	不同口进出
成员	
接口一	GE0/0/6
接口二	GE0/0/7
允许的VLAN	1-4094
接口对状态同步	不开启

版权所有 © 华为技术有限公司

4. 配置云端管理接口。
   GE0/0/3默认为二层接口，请按照如下方式配置成三层接口。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/3对应的，按照如下参数配置接口。

安全区域	untrust
模式	路由
IPv4	
IP地址	172.16.10.10/24

   c. 配置云端管理接口的静态路由。
      i. 选择“网络 > 路由 > 静态路由”。
      ii. 单击“静态路由列表”区域下的“新建”，添加静态路由。下一跳配置为网关地址。

图 1-45 配置静态路由

5. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

版权所有 © 华为技术有限公司

图 1-46 配置系统时间

6. 配置业务参数（边界防护与响应服务）。
   a. 加载License。

      说明

      如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

      i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。
      ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。
   c. 确认安全策略已成功下发。

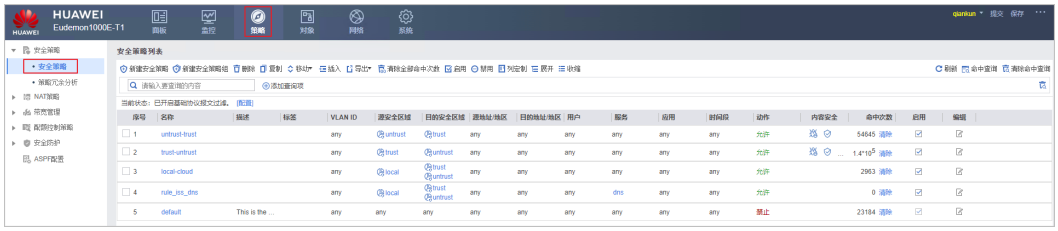
      设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

      安全策略下发后，如图1-47所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

      说明

      如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

图 1-47 安全策略



   d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

版权所有 © 华为技术有限公司

图 1-48 特征库升级

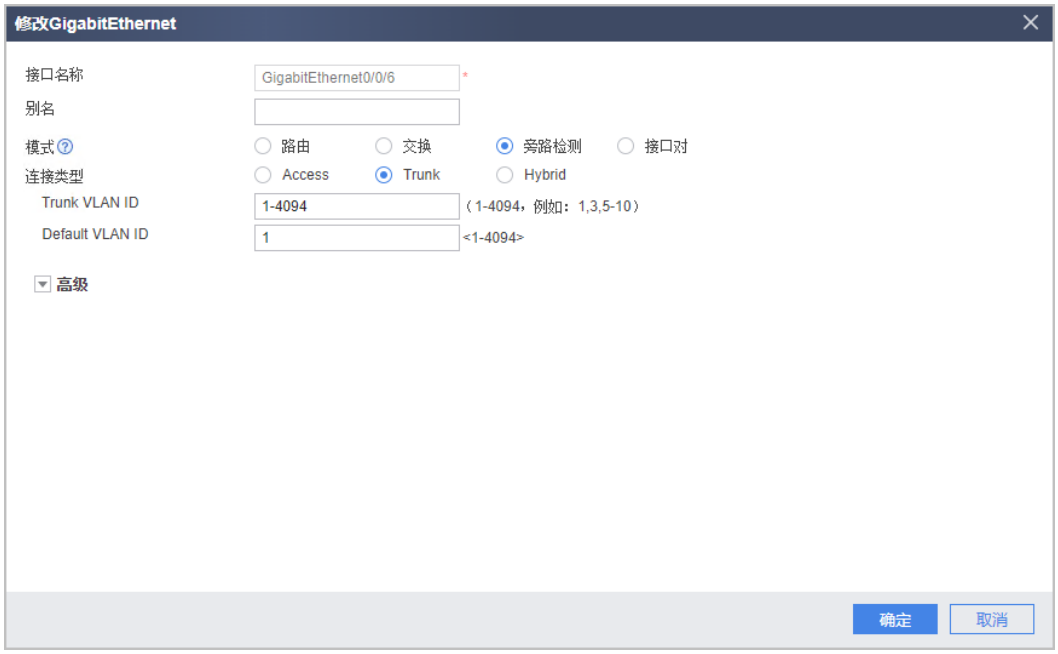
e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-49 保存配置

配置天关 2

1. 参见**步骤1**，登录天关2。
2. 配置镜像流量接收口GE0/0/6为旁路检测模式。
   a. 选择“网络 > 接口”。
   b. 单击GE0/0/6对应，按照下图所示配置接口。

图 1-50 配置接口



版权所有 © 华为技术有限公司

3. 参照**步骤4**，配置云端管理接口。
4. 参照**步骤5**，配置设备系统时间。
5. 配置业务参数（边界防护与响应服务）。
   a. 加载License。

      说明

      如果设备为V600R007C20SPC500之前的版本，需要执行本步骤。

      i. 选择“系统 > License管理”，“License激活方式”设置为“本地手动激活”。
      ii. 单击“浏览”，选择本地PC中的的License文件，并单击“激活”。

   b. 选择“策略 > 安全策略 > 安全策略”，检查default策略的动作是否为“允许”，如果不是，单击策略名称default进入修改安全策略界面，将动作修改为“允许”。
   c. 配置安全策略。

      天关2上需要配置名称为“local-cloud”、“rule_iss_dns”和“trust-trust”的安全策略。

      i. 配置名称为“local-cloud”、“rule_iss_dns”的安全策略。

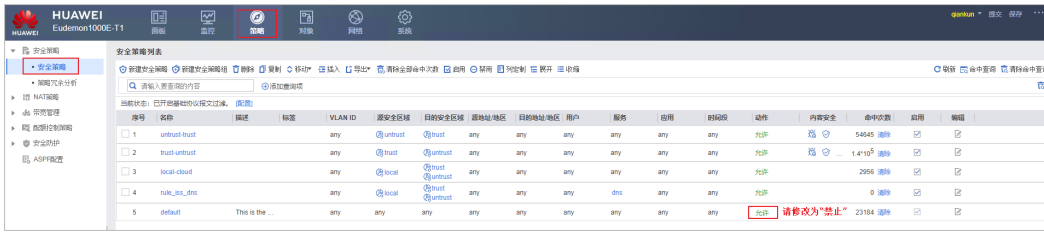
         设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

         安全策略下发后，如**图1-51**所示。共有5条安全策略，其中default安全策略建议改回**禁止**，默认安全需要。

         说明

         如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

         图 1-51 安全策略

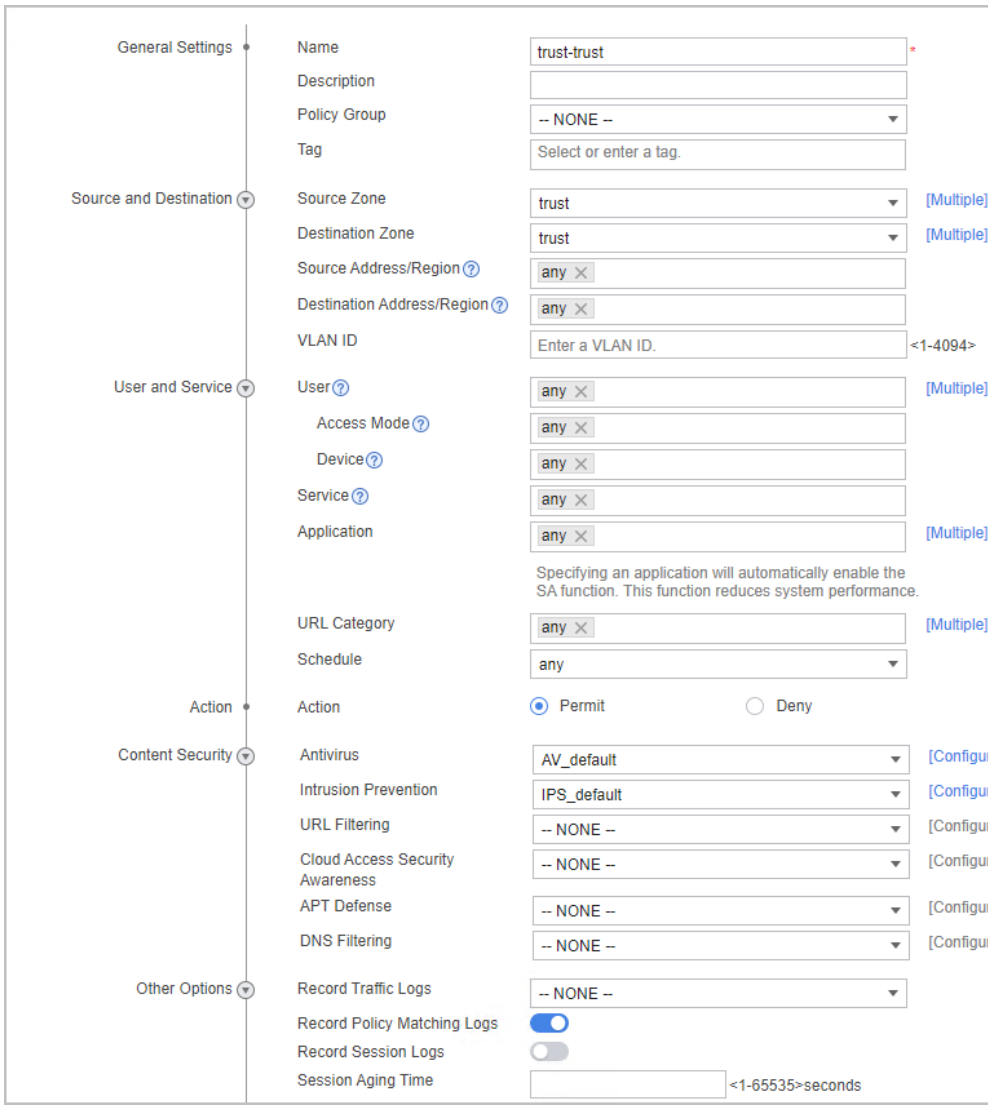
      ii. 配置名称为“trust-trust”的安全策略。

         1) 选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”。
         2) 配置名称为“trust-trust”的安全策略，源安全区域为“trust”，目的安全区域为“trust”，反病毒采用新建的AV_default，入侵防御采用新建的IPS_default，动作为“允许”。

 版权所有 © 华为技术有限公司

图 1-52 配置安全策略

 版权所有 © 华为技术有限公司



d. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-53 特征库升级

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

版权所有 © 华为技术有限公司

图 1-54 保存配置

1.6.7 结果验证

1. 验证设备上线是否成功、业务套餐是否激活成功。
   a. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。

      设备状态为“正常”表示设备已上线成功。
   b. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。

      套餐状态为“正常”表示套餐已激活成功。
2. 验证边界防护与响应服务是否正常。
   a. 在华为乾坤控制台上可以检测到源地址为内网地址的威胁事件，如192.168.41.254。
   b. 在租户内网设备上能够ping通公网域名。

1.7 企业边界防火墙单机组网（三层）

1.7.1 组网需求

适用产品和版本

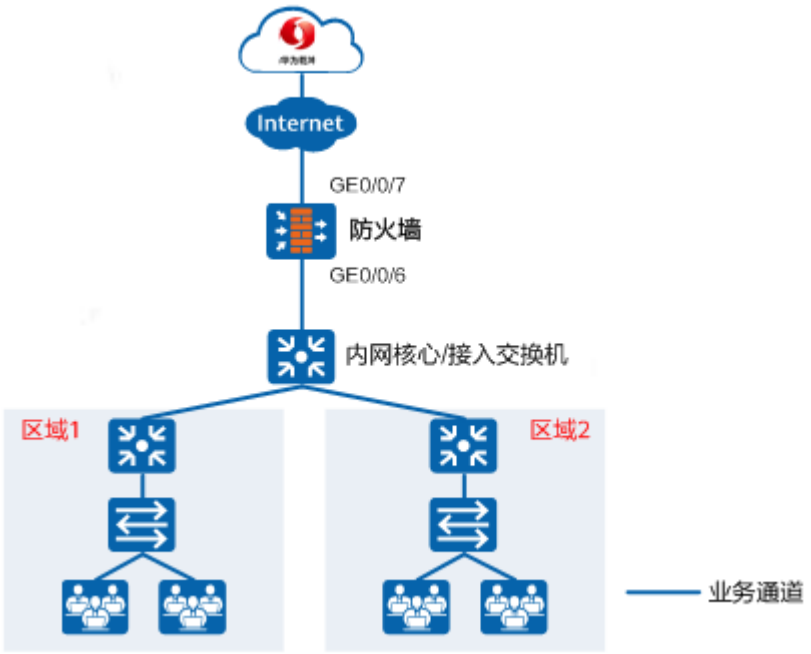
设备	版本
Eudemon1000E-T1	边界防护与响应服务：V600R007C20SPC602及其后续版本

组网需求说明

防火墙部署在企业出口位置。根据客户需求，防火墙可以兼任出口网关或NAT功能。

版权所有 © 华为技术有限公司

图 1-55 三层组网方案



约束或注意事项

- Eudemon1000E-T1接口使用限制：
  - Eudemon1000E-T1系统软件已自带云服务功能，故不需要另外加载云服务组件包。

1.7.2 配置思路

前提条件

- 已购买相应的服务。
- 除防火墙外的其他设备已完成网络连接，确保通信正常。

配置思路

登录防火墙，主要配置以下内容。

1. 配置公网地址和内网地址。
2. （可选）配置静态路由。在配置公网地址时采用了静态IP的方式，且没有配置默认网关，此场景下需要配置静态路由。
3. 配置NAT策略（easy-ip方式），以便内网用户可以直接使用防火墙的公网IP地址来访问Internet。
4. （可选）配置DHCP参数，如果客户需要防火墙作为DHCP服务器，为内网交换机/PC分配IP地址。
5. 配置防火墙与云平台对接。
6. 配置边界防护与响应服务业务参数。

版权所有 © 华为技术有限公司

1.7.3 数据规划

IP 地址规划

表 1-2 IP 地址规划

接口	IP地址获取方式	IP地址示例	备注
上行接口 GE0/0/7	**静态IP地址**	IP地址：1.1.1.1	IP地址的获取方式支持静态IP、DHCP和PPPoE。请根据实际情况进行选择。 IP地址、DNS和PPPoE的拨号信息等需要向租户获取。
		子网掩码：255.255.255.0	
		默认网关：1.1.1.254	
		首选DNS：2.2.2.2	
		（可选）备用DNS：2.2.3.3	
	DHCP方式	防火墙作为DHCP客户端，由DHCP服务器为防火墙分配IP地址和DNS地址。	
	PPPoE方式	通过拨号向PPPoE Server（运营商设备）拨号获得IP地址、DNS地址。	
下行接口 GE0/0/6	**静态IP地址**	IP地址：10.1.1.1	业务接口，漏洞扫描服务和云日志审计服务共用此接口。
		子网掩码：255.255.255.0	

DHCP 服务器规划（可选）

如果客户需要防火墙作为DHCP服务器，为内网交换机/PC分配IP地址。那么请参考如下内容完成数据规划。

表 1-3 DHCP 服务器规划

作为DHCP服务器的接口	可分配IP地址范围	子网掩码	默认网关	DNS服务器
GE0/0/6	10.1.1.1-10.1.1.253	255.255.255.0	10.1.1.254	首选DNS：2.2.2.2 （可选）备用DNS：2.2.3.3

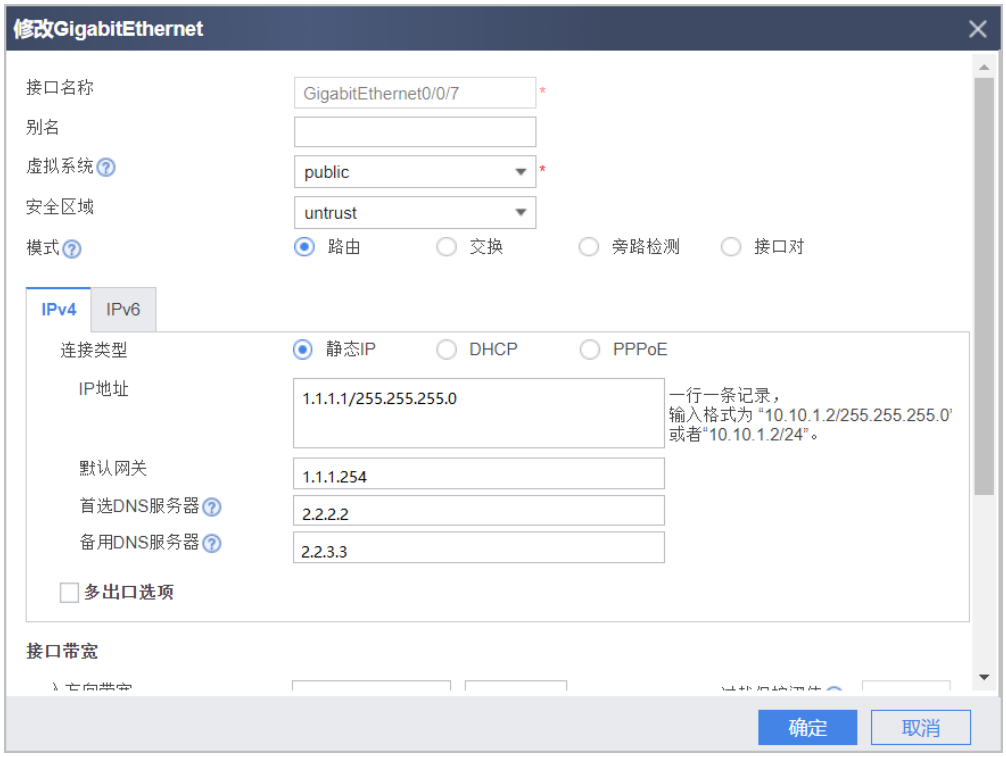
版权所有 © 华为技术有限公司

1.7.4 配置防火墙

操作步骤

1. 在管理PC上配置网口的IP地址为192.168.0.2（可以是192.168.0.2～192.168.0.254中的任何一个），子网掩码为255.255.255.0，然后打开Web浏览器访问设备的标准界面**https://192.168.0.1:8443/**。
2. 配置公网地址。
   a. 选择“网络 > 接口”，选择连接Internet的网络接口，假设为GE0/0/7。
   b. 设置“模式”为“路由”，“安全区域”选择“untrust”，“连接类型”和“IP地址”请根据实际IP地址的获取方式进行配置。

图 1-56 静态 IP 配置方式



版权所有 © 华为技术有限公司

图 1-57 DHCP 配置方式

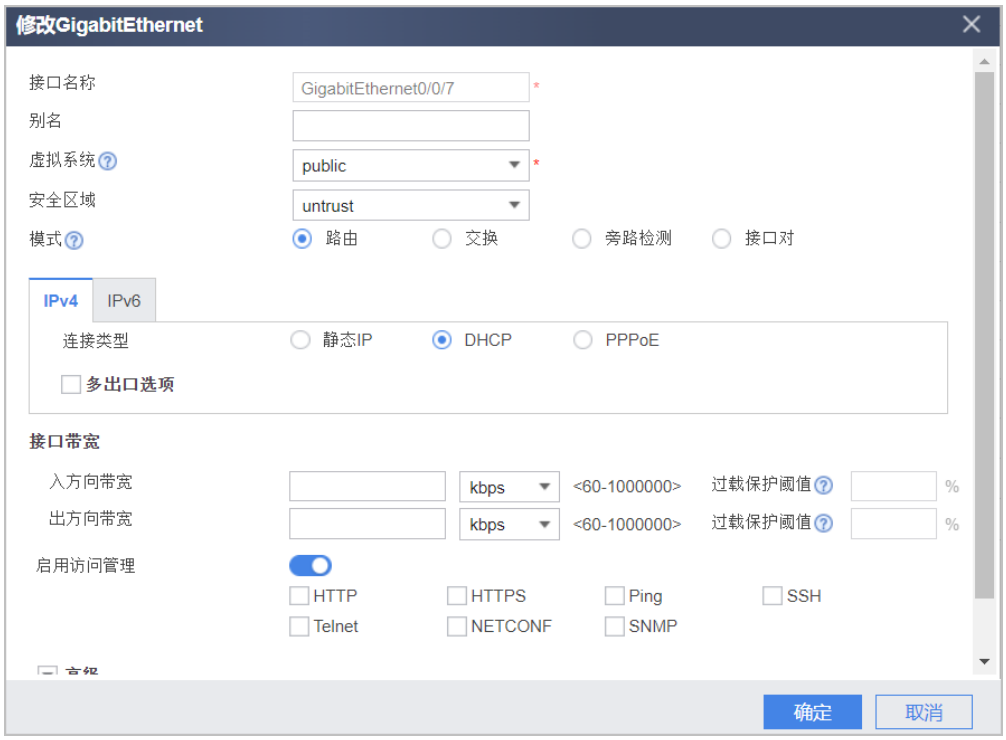
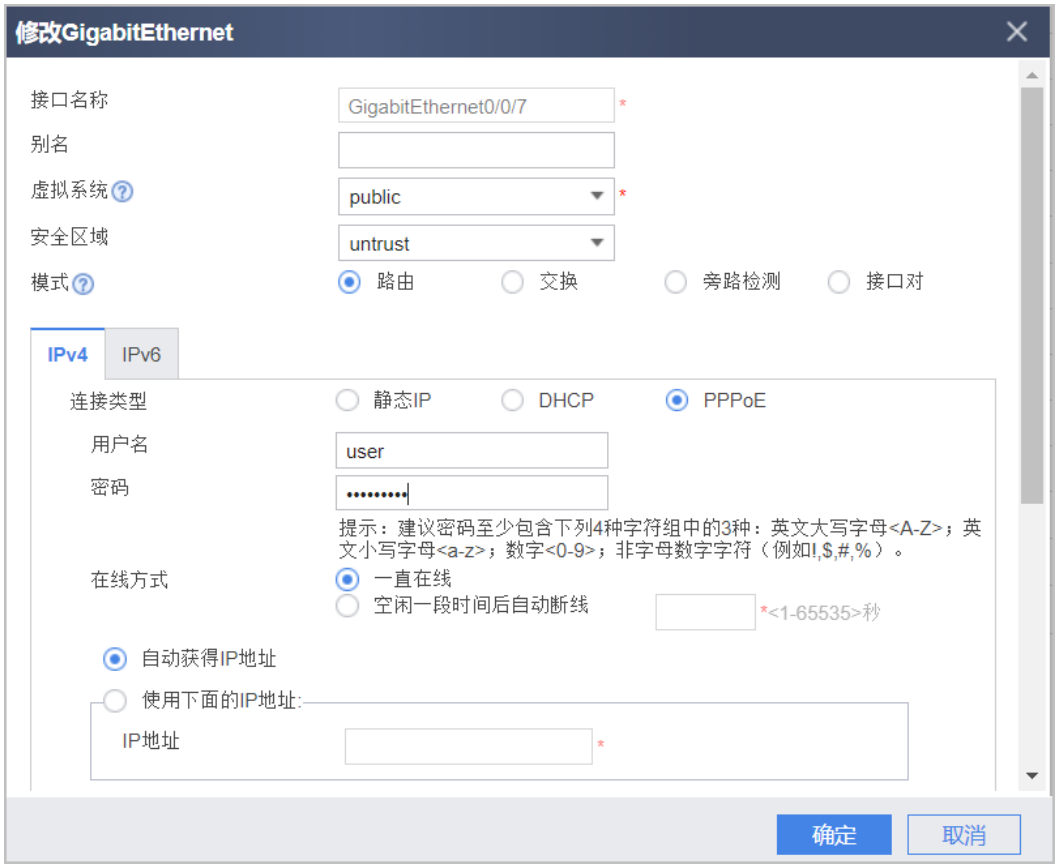


图 1-58 PPPoE 配置方式



c. 单击“确定”，完成配置。

 版权所有 © 华为技术有限公司

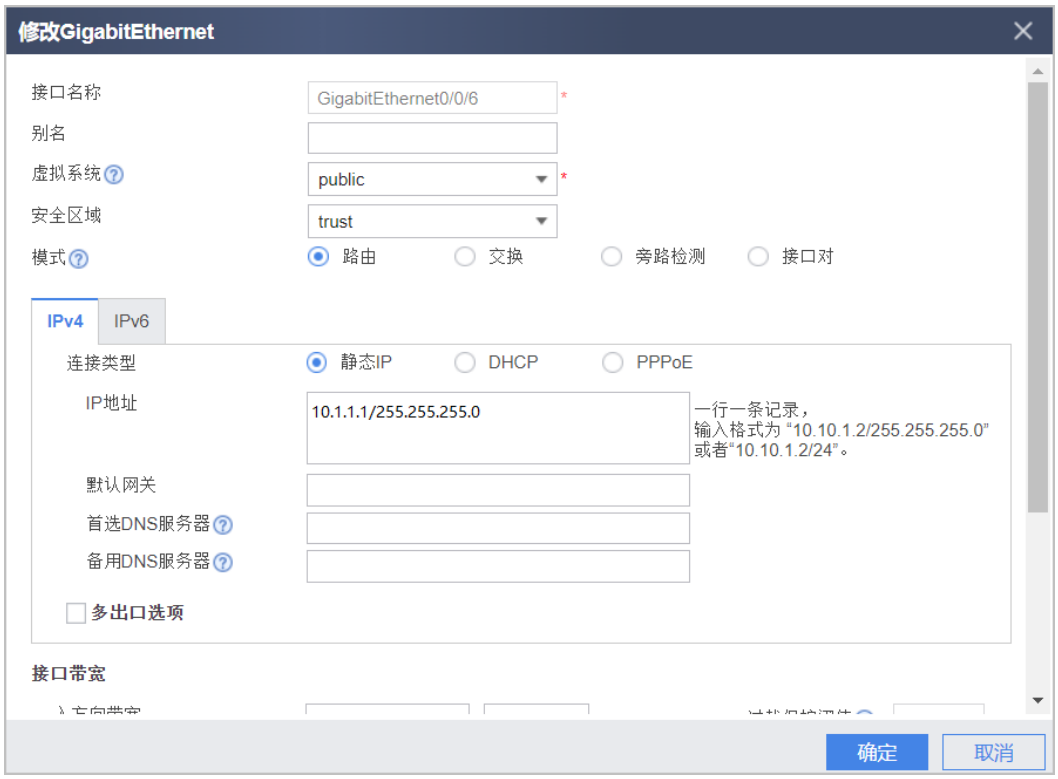
3. 配置内网地址。

   a. 选择“网络 > 接口”，选择内网核心/接入交换机的网络接口，假设为GE0/0/6。

图 1-59 选择接口

   b. 设置“模式”为“路由”，“安全区域”选择“trust”，“连接类型”和“IP地址”请根据实际IP地址的获取方式进行配置。

图 1-60 配置接口



版权所有 © 华为技术有限公司

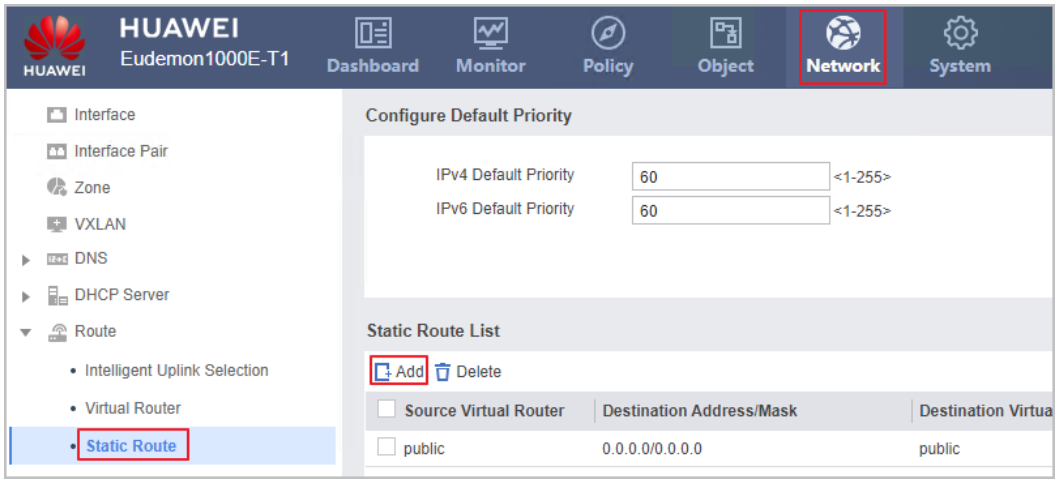
c. 单击“确定”，完成配置。

4. （可选）配置静态路由。

在步骤2时如果采用了静态IP的方式，且没有配置默认网关，此场景下需要配置静态路由。其他场景不需要配置静态路由，如：静态IP方式（配置了默认网关）、DHCP或PPPoE的方式。

a. 选择“网络 > 路由 > 静态路由”，单击“新建”。

图 1-61 新建静态路由



b. 设置“目的地址/掩码”为“0.0.0.0/0.0.0.0”，“出接口”为上行接口（如：GE0/0/7），“下一跳”配置为网关地址，请向租户获取该地址。

 版权所有 © 华为技术有限公司

图 1-62 配置静态路由

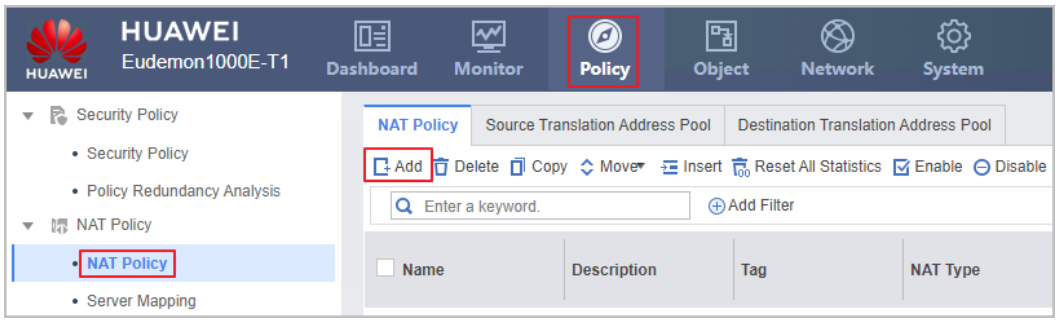
c. 单击“确定”，完成配置。

5. 配置出接口方式的源NAT策略（easy-ip方式），以便内网用户可以使用防火墙的公网IP地址来访问Internet。

a. 选择“策略 > NAT策略 > NAT策略”，在“NAT策略”页签中，单击“新建”。

图 1-63 新建 NAT 策略

 版权所有 © 华为技术有限公司



b. 按照如下参数配置NAT策略，其中“源地址”请根据实际情况选择。

图 1-64 配置 NAT 策略

c. 单击“确定”，完成配置。

6. （可选）配置DHCP。

如果客户需要防火墙作为DHCP服务器，为内网交换机/PC分配IP地址，这种情况下需要配置DHCP。

a. 选择“网络 > DHCP服务器 > 服务”，单击“新建”。

版权所有 © 华为技术有限公司

图 1-65 新建 DHCP 服务

b. 请根据**DHCP服务器规划（可选）**，配置DHCP。

说明

若“DNS服务”配置为“使用系统的DNS设置”，则在边界防护与响应服务部署之后，需要手动创建一条trust到local的安全策略，并放通dns服务，具体配置参见**7.b**。

图 1-66 配置 DHCP

c. 单击“确定”，完成配置。

7. 配置业务参数（边界防护与响应服务）。

a. 确认安全策略已成功下发。

设备上线后，云端会部署套餐，需要2分钟左右，部署成功后安全策略会自动下发。

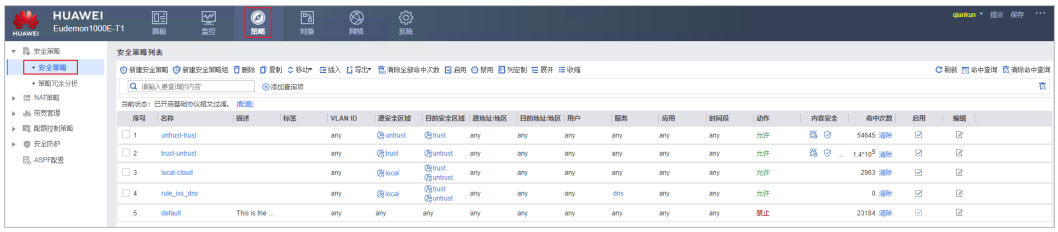
安全策略下发后，如**图1-67**所示。共有5条安全策略，其中default安全策略被自动修改为**禁止**。

说明

如果设备上只有“default”和“rule_iss_dns”安全策略，或只有“default”安全策略时，由云端自动下发安全策略。

版权所有 © 华为技术有限公司

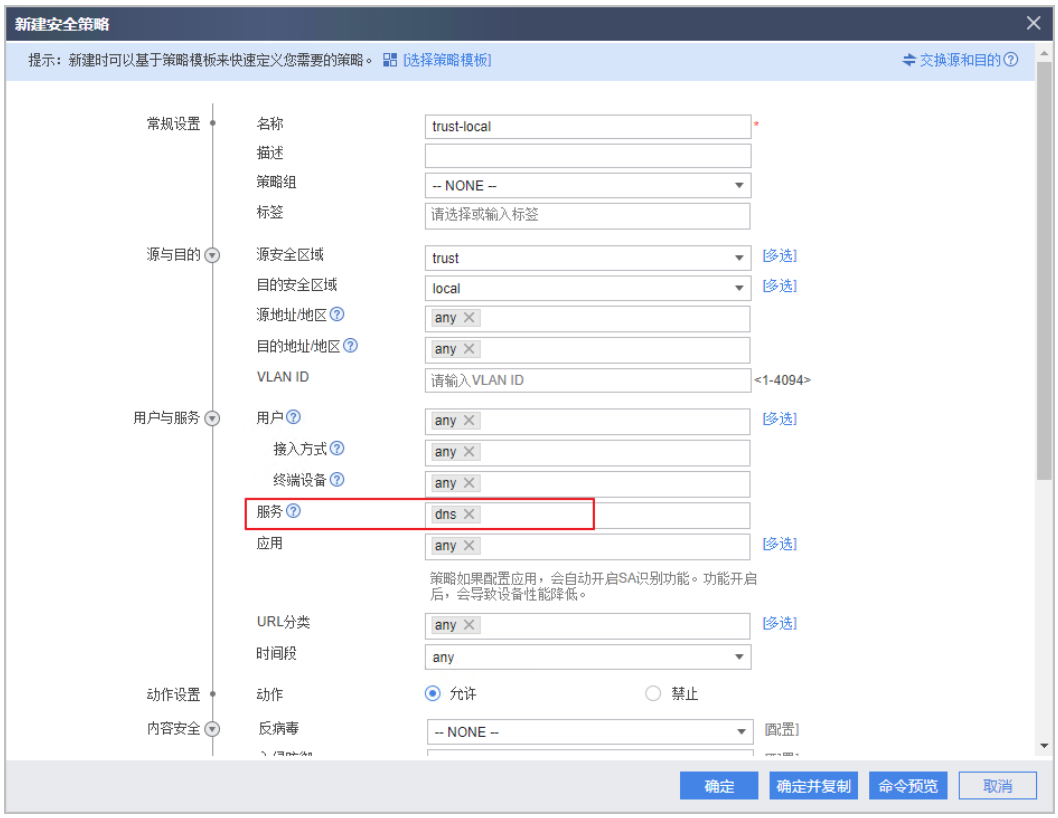
图 1-67 安全策略



b. （可选）配置trust到local的安全策略并放通dns服务。

在6.b中“DNS服务”配置为“使用系统的DNS设置”时，此处需要手动创建一条trust到local的安全策略并放通dns服务。

图 1-68 配置安全策略



c. 选择“系统 > 升级中心”，检查“入侵防御特征库”和“反病毒特征库”是否在线升级成功，升级需要10分钟左右，请耐心等待。如果不成功，请单击“立即升级”。

图 1-69 特征库升级

 版权所有 © 华为技术有限公司

d. 选择“系统 > 配置 > 时钟配置”，检查设备系统时间是否与当前时间一致，如果不一致，请调整设备系统时间，以保证云端能够精确掌握威胁事件的发生时间。

图 1-70 配置系统时间

e. 单击右上角“保存”按钮，在系统显示界面单击“确定”，保存配置以避免设备重启后配置丢失。

图 1-71 保存配置

1.7.5 结果验证

1. 验证设备上线是否成功、业务套餐是否激活成功。
   a. 登录华为乾坤控制台，右上方菜单栏选择“资源中心 > 设备管理 > 设备”，查看设备状态。
      设备状态为“正常”表示设备已上线成功。
   b. 登录华为乾坤控制台，单击右上角帐号选择“订单中心 > 我的套餐”查看套餐状态。
      套餐状态为“正常”表示套餐已激活成功。
2. 验证边界防护与响应服务是否正常。
   a. 检查黑名单是否能够正常下发。
      i. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”，在右上角菜单栏选择“黑白名单”。
      ii. 在“黑名单 > IP黑名单”页签中创建并部署一个黑名单。
      iii. 登录设备的标准界面**https://192.168.0.1:8443/**。
         - Eudemon1000E-T1：在“策略 > 安全防护 > 黑名单”中检查是否存在下发的黑名单。

版权所有 © 华为技术有限公司

如果存在则表示黑名单能够正常下发。

说明

- 请获取一个当前没有业务使用的IP地址作为黑名单，否则可能会影响当前业务。
- 验证后请务必在“黑名单 > IP黑名单”页签中删除刚创建的黑名单。

b. 验证云端是否能够正常接收设备的威胁日志。

i. 等待一段时间后，登录设备的标准界面**https://192.168.0.1:8443/**，在“监控 > 日志 > 威胁日志”中查看是否存在威胁日志，如果存在表示设备已产生威胁日志。

ii. 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。在右上角菜单栏选择“威胁事件”，查看是否存在威胁事件，如果存在则表示云端能够正常接收设备的威胁日志。

版权所有 © 华为技术有限公司

2 边界防护与响应

2.1 产品介绍

2.1.1 什么是边界防护与响应

边界防护与响应服务使用天关为租户的本地网络提供边界防护，并基于天关提供的日志进行智能分析和处置，持续保护企业内网安全。华为乾坤通过集成告警自动确认、威胁分析等检测模型，智能识别租户本地网络的潜在威胁并完成自动化处置，从而帮助租户简化本地运维，提升安全防护实效。

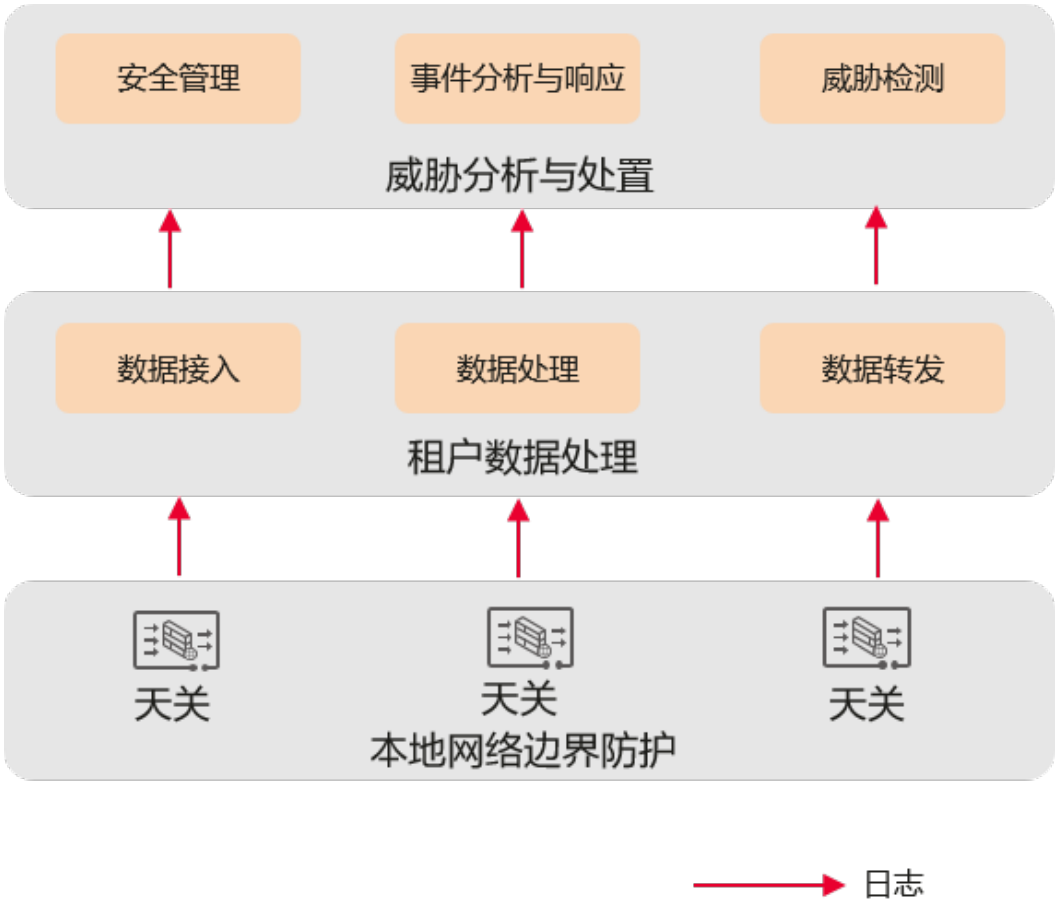
逻辑架构

如图2-1所示，边界防护与响应由三个部分组成。

- 本地网络边界防护：部署在租户网络边界的天关提供入侵防御、反病毒、DNS过滤等能力，守护本地网络边界安全。
- 租户数据处理：华为乾坤的数据接入中心模块对天关侧的日志进行相关处理，并将各业务数据进行持久化存储。
- 威胁分析与处置：华为乾坤的威胁分析与处置模块获取各业务数据后，通过威胁检测、事件分析与响应、安全管理三个子模块协同工作共同完成自动化分析和安全响应。具体分析过程请参见图2-2。

版权所有 © 华为技术有限公司

图 2-1 逻辑架构



威胁分析与处置

如图2-2所示，威胁分析与处置中心模块获取各业务数据后，通过威胁检测、事件分析响应、安全管理三个模块协同工作共同完成自动化分析和安全响应。

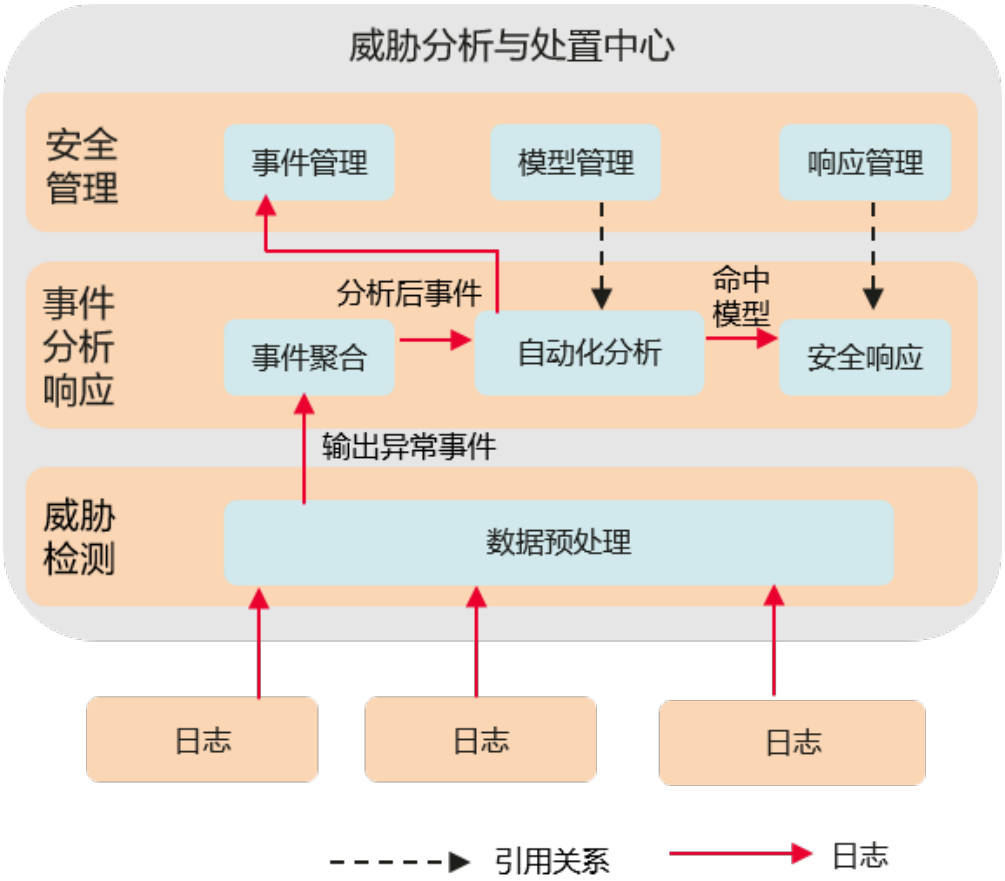
- 威胁检测：针对获取的日志，直接进行格式、字段等预处理后输出异常事件。
- 事件分析响应：对输出的异常事件依次进行聚合分析、自动化分析、安全响应。

  针对输出的异常事件根据对应的聚合策略进行聚合分析，然后基于自动化分析模型对聚合后的事件进行自动化分析判定。对于命中分析模型的事件，由安全响应执行自动响应动作，在自动化分析的基础上，分析后的事件（包括命中或未命中事件）由安全专家进一步分析处置。
- 安全管理：为华为乾坤安全专家提供事件可视化Portal、事件人工处置能力，日常管理能力、安全响应管理能力等。

  安全专家可以通过事件管理查看自动化分析后的事件；通过模型管理及时配置和调整自动化分析模型；通过响应管理完成黑白名单的日常维护工作。

版权所有 © 华为技术有限公司

图 2-2 威胁分析与处置



2.1.2 功能特性

本地网络边界防护

天关部署在租户网络边界，通过入侵防御、反病毒、DNS过滤等技术守护本地安全，租户订购边界防护与响应服务后，天关可以执行以下防护动作：

- 对流量进行入侵防御检测，全方位防御各种威胁行为。
- 对流量进行反病毒处理，有效避免病毒文件引起的数据破坏、权限更改和系统崩溃等情况的发生。
- 对流量进行DNS过滤，全面控制域名访问。

租户数据安全处理

- 数据授权：在用户授权前提下，本地天关仅提供用户授权范围内的数据。
- 加密传输：本地天关采用HTTPS或TLS协议将日志提供到云服务平台。
- 加密保存：使用华为公司密钥管理中心（KMC）加密组件对数据进行加密，加密后存储在华为乾坤。
- 处理原则：仅供云服务平台运营专家进行威胁分析和溯源。
- 信息隔离：每个客户都有自己的服务账号，基于账号接收分析报表和短信，不同客户间信息隔离。

版权所有 © 华为技术有限公司

自动化分析

华为乾坤基于分析模型对威胁事件进行分析判定，并根据判定结果执行不同的处置。租户可依靠华为乾坤的自动化分析能力和安全专家简化本地运维，提升防护实效。

自动化分析以后，可以有如下几种处置方式：

- 事件命中误报模型，则此事件状态变更为误报。
- 事件命中告警自动确认模型、威胁分析等模型，则自动化分析将请求安全响应执行相应的处置。
- 在自动化分析的基础上，安全专家进一步分析处置事件。

安全响应

提供安全事件的响应闭环能力，主要包括下发黑名单、发送告警两种安全响应动作，租户可利用华为乾坤的安全响应能力有效提高安全事件的闭环效率。

针对以下场景提供下发黑名单、发送告警两种安全响应动作：

- 自动化分析判定后可以自动处置的事件，自动化分析将请求安全响应下发黑名单或发送告警。
- 自动化分析判定后需要安全专家处置的事件，安全专家分析后可通过Portal页面的事件管理菜单人工下发黑名单或发送告警。
- 租户在租户门户中下发黑名单。

安全专家精准分析

华为乾坤安全专家整合安全能力，快速准确识别复杂威胁：

- 现网对抗经验固化到华为乾坤，不断增强华为乾坤安全能力。
- 最新漏洞分析、华为乾坤智能签名生产，快速应对新型威胁。
- 安全专家针对发现的每一条安全告警进行统一分析，运用华为乾坤各种安全能力，解决最新“疑难杂症”。

2.1.3 产品优势

跨服务联动

对监测结果向下转存储OBS满足合规，向上同步态势感知形成可视化运营。

准确识别威胁

基于误报模型、告警自动确认模型、威胁分析等智能分析模型，同时结合华为乾坤安全专家团队的现网经验，对数据进行关联分析，快速准确发现威胁。

自动化威胁响应

发现威胁时，执行自动化处置流程自动下发黑名单、发送告警等动作闭环威胁事件，并通过邮件、短信等方式通知用户，有效提高威胁事件的闭环效率。

版权所有 © 华为技术有限公司

2.1.4 应用场景

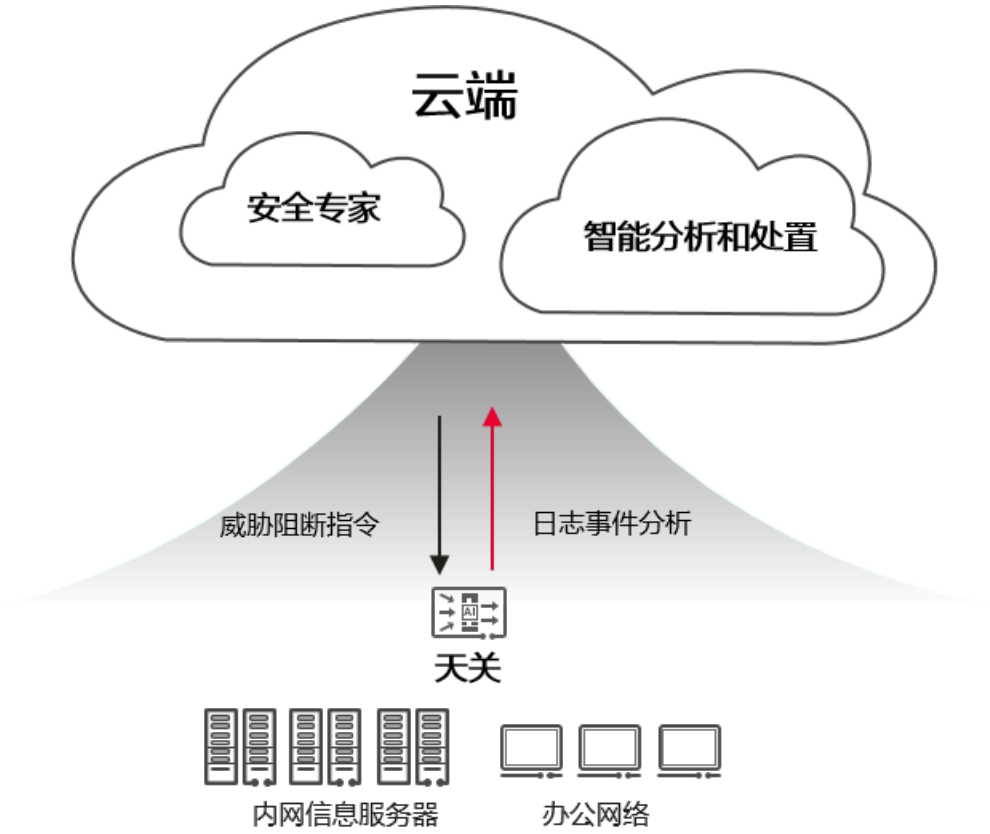
中小型企业互联网出口场景

中小型企业只有很少或者没有安全投资，没有专门的网络安全负责人，也买不起驻场服务。即使购买了最基本的安全设备，通常也会因为没有专业安全运维人员而无法发挥作用。此类型企业的安全防护能力几乎是一片空白，只要一个普通的病毒就可能导致整个信息系统不可用。随着网络安全形势日趋严峻，已严重影响到日常业务运营，因此网络安全建设也成为此类型企业必须面对的课题。

此类型企业安全建设的主要诉求包括：

- 由于没有人力投入安全运维，因此不想购买多种安全设备。
- 安全预算非常有限，买不起驻场服务，希望将“网络安全建设”外包出去，获得基本的安全能力，在保证内网与外网能够互通的同时，不影响日常业务运营。

图 2-3 中小型企业互联网出口场景



采用边界防护与响应服务可以实现：

- 仅需在企业互联网出口部署一台天关，通过华为乾坤自动向天关下发入侵防御、反病毒基本防御能力，能够有效拦截外网威胁和避免病毒文件感染，在保证内网与外网能够互通的同时，不影响日常业务运营。
- 只需少量的投资，即可购买云服务安全能力并获得安全专家服务和智能处置能力，将“网络安全建设”外包给华为乾坤，大幅减少本地运维工作量。

版权所有 © 华为技术有限公司

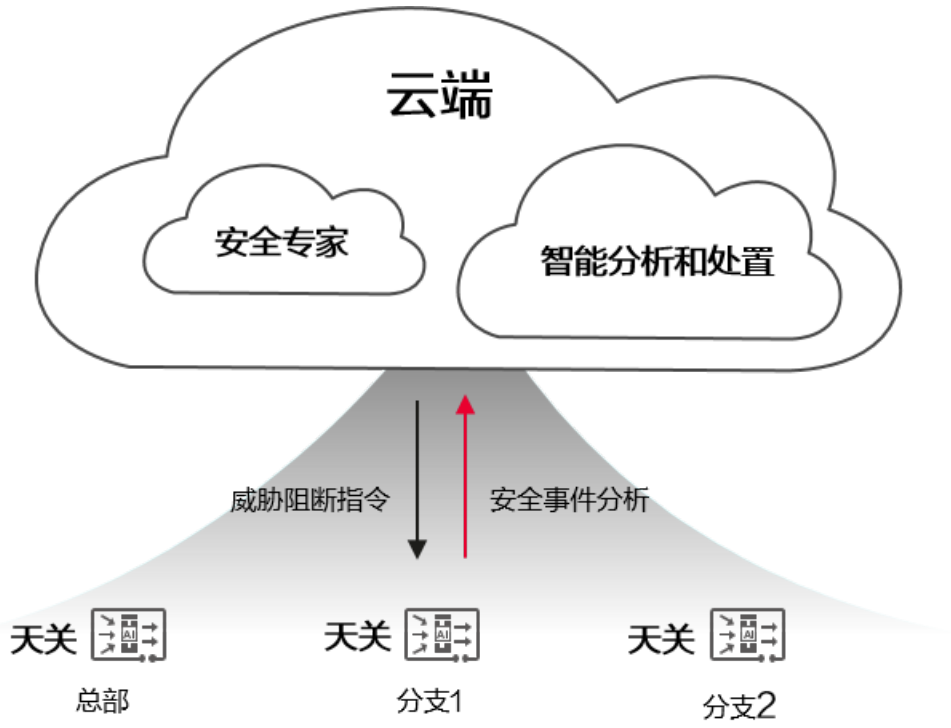
大型企业集团多分支互联场景

大型企业集团业务一般遍及全国，在全国多省市设有分支，且分支之间业务来往频繁。此类型企业一般在集团总部设有小型的网络安全部门，安全投资主要依赖安全厂商或集成商进行建设，从厂商或服务商购买驻场服务。由于驻场服务人员的能力有限、分支基本没有专门的安全运维人力、分支之间互联网数据传输频繁等原因，导致集团整体的安全状况堪忧，可能轻易就被普通水平的黑客攻陷。

此类型企业安全建设的主要诉求包括：

- 简化本地运维：受限于安全运维人力成本，无法为每个分支派驻安全运维人力或购买驻场服务，即使为分支购买了驻场服务，由于驻场服务人员的能力有限，也难以达成安全效果。
- 实现统一防护：能够对分支机构网络防护全部覆盖，可以统筹分析全集团的安全事件，并统一响应、及时阻断威胁，同时集团总部能够及时了解每个分支的安全状况。

图 2-4 大型企业集团多分支互联场景



采用边界防护与响应服务可以实现：

- 利用华为乾坤的智能分析和处置能力提升自动运维效率，自动拦截威胁，华为乾坤安全专家资源7*24小时在线服务，解决复杂网络安全问题，有效简化本地运维。
- 通过在每个分支的互联网边界处部署一台天关作为安全防御节点，结合华为乾坤的安全服务实现对所有分支网络的统一防护。
- 借助华为乾坤对安全事件的统筹分析，及时自动响应阻断威胁，并将安全告警通过邮件发送至总部安全管理员，总部安全管理员可针对性进行应急响应，解决严重的失陷主机事件。总部安全管理员借助全局安全服务周报、月报了解整体的网络安全态势，把握全集团的网络安全动态。

版权所有 © 华为技术有限公司

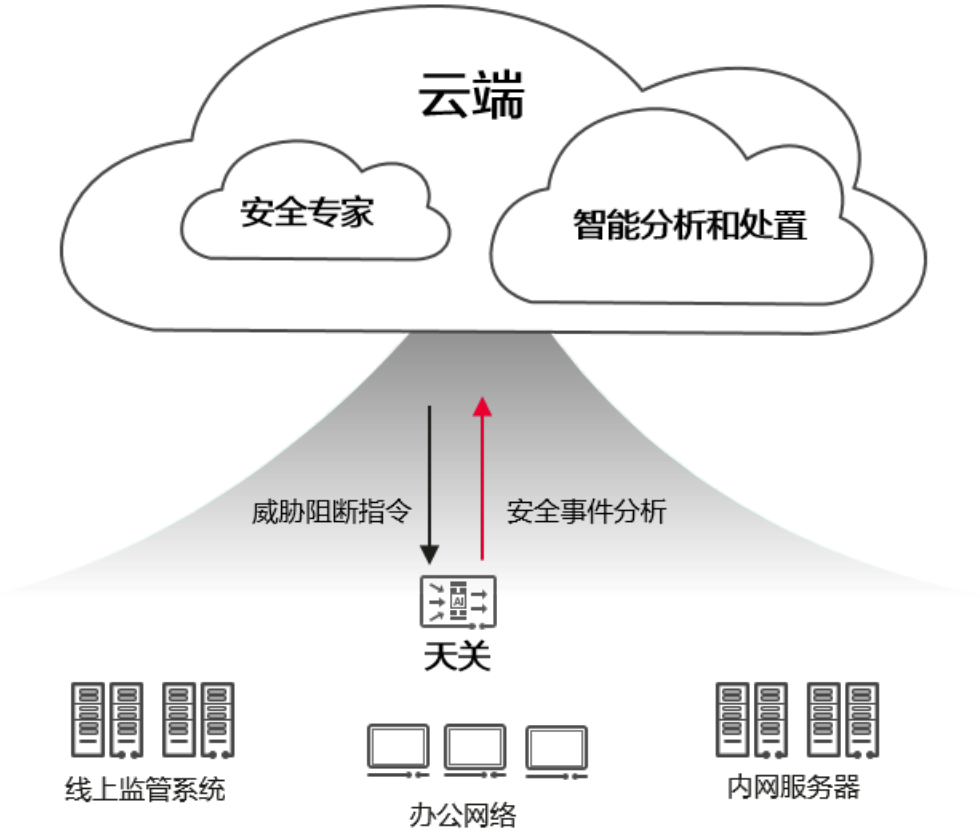
行业安全监管建设场景

在政府、医疗、教育等行业，上级行政主管部门对下级单位提出了较高的网络安全要求，但下级单位由于安全预算有限、技术能力储备不足等问题较难实现完善的网络安全建设。同时，上级主管部门无法有效监管网络安全要求是否落到实处，也无法督促下级单位针对不满足项及时进行整改。

此类型单位安全建设的主要诉求包括：

- 下级单位在安全预算有限的前提下，满足上级主管部门的网络安全要求。
- 上级主管部门能够对下级单位进行有效监管，对不满足项可以及时督促整改。

图 2-5 行业安全监管建设场景



采用边界防护与响应服务可以实现：

- 只需少量的投资，即可购买云服务安全能力并获得安全专家服务和智能处置能力。
- 借助华为乾坤对威胁事件进行统一分析，统一响应及时阻断，同时借助华为乾坤安全专家解决疑难问题，弥补下级单位技术能力储备不足的问题。
- 华为乾坤向下级单位发送安全告警和邮件报告的同时，也向上级主管部门发送全局安全检测报告，全面展示下级单位的安全状况，安全事件处置是否及时等，实现对下级单位的有效监管、及时督促。

版权所有 © 华为技术有限公司

2.2 服务开通

2.2.1 开通商用服务

2.2.1.1 租户身份开通

2.2.1.1.1 注册华为乾坤帐号

说明

- 华为乾坤控制台是使用华为乾坤的界面，登录前需要先注册华为乾坤帐号。
- 如果您已有华为乾坤MSP（渠道服务商）创建的租户帐号，可跳过本节内容。

步骤1 访问华为乾坤控制台。

步骤2 在登录页面单击“立即注册”。

根据界面提示完成帐号注册。

----结束

2.2.1.1.2 开通服务套餐

背景信息

线下购买云服务License后，在华为乾坤激活线下订单。本服务配套的天关型号，如**表1 天关型号**所示。

表 2-1 天关型号

设备型号	激活方式
Eudemon1000E-T1	请参见**操作步骤**。

操作步骤

1. 使用租户帐号登录华为乾坤控制台。
2. 在界面右上方单击“订单”，选择“我的套餐”页签。
3. 单击“开通服务”，选择“根据SN激活”，输入设备的SN，单击“开通”。

版权所有 © 华为技术有限公司

图 2-6 输入 SN

4. （可选）在“开通服务”页面，单击“添加授权”。

   如果华为工程师已在ESDP系统中激活License，则此界面会显示已激活的授权ID，此时无需执行本步骤。

图 2-7 开通服务

5. （可选）在“添加授权”页面，根据提示输入授权ID，单击“确定”。

   如果华为工程师已在ESDP系统中激活License，则无需执行本步骤。

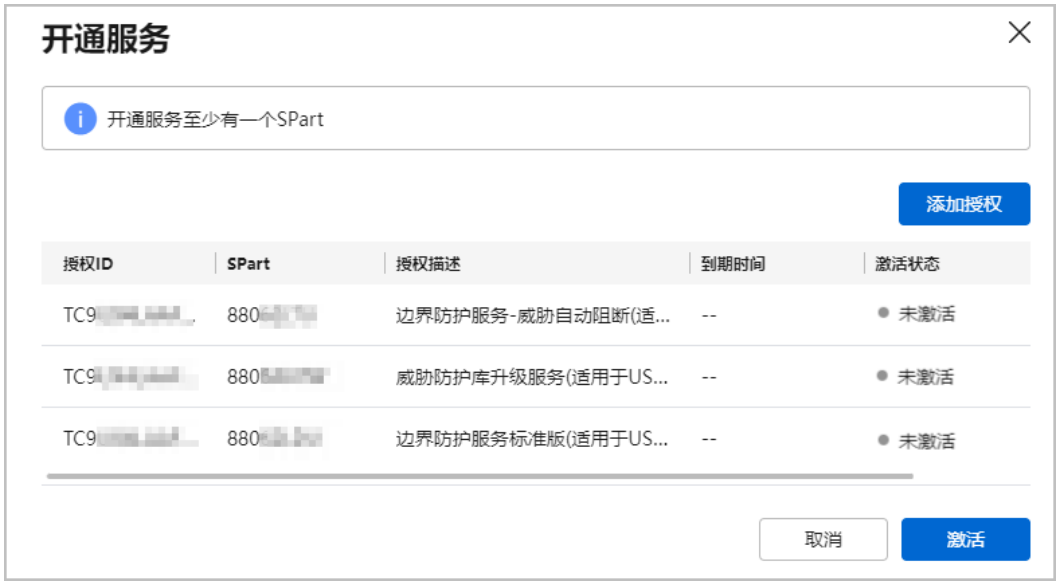
   如果没有激活License，则需要添加授权ID，边界防护与响应服务相关的授权ID包括边界防护服务标准版授权ID、边界防护服务专业版授权ID、边界防护服务-威胁自动阻断授权ID、威胁防护库升级服务授权ID。请根据实际购买的授权ID填写。

版权所有 © 华为技术有限公司

图 2-8 添加授权

6. 在“开通服务”页面，单击“激活”。

图 2-9 开通服务



7. 开通成功后，在界面右上方选择“资源中心 > 设备管理 > 设备”，在显示界面中可以查看到设备处于未注册状态。

2.2.1.2 MSP 身份开通

2.2.1.2.1 MSP 代建租户

操作步骤

步骤1 以MSP帐号登录华为乾坤控制台。

步骤2 单击控制台页面右上方“租户”，进入租户管理页面。

步骤3 创建租户帐号。

1. 选择“自建租户”，单击租户列表右上角“创建”。
2. 填写租户信息后单击“下一步”。

版权所有 © 华为技术有限公司

图 2-10 自建租户信息

说明

- 创建租户时，授权MSP开关默认为“否”不开启，开启后需要选择委托时间以及勾选风险告知协议。
- 创建租户时，屏蔽本MSP信息开关默认为“否”不开启，开启后租户不感知当前MSP信息。
- 默认自动委托当前新建租户的公共角色。租户创建完成后，租户因新购买的服务而产生的服务类角色都不会自动委托给MSP。

3. 设置租户管理员信息，单击“完成”。

版权所有 © 华为技术有限公司

图 2-11 自建租户管理员信息

----结束

2.2.1.2.2 委托 MSP 管理

背景信息

用户根据自身实际情况，选择合适的MSP（服务渠道商）进行代维授权。通过MSP进行日常运维，可以降低企业人力投入成本。

操作步骤

步骤1 使用租户帐号登录华为乾坤控制台。

步骤2 单击控制台页面右上角帐号，选择“委托”进入委托界面。

步骤3 单击“创建”，根据**表 委托参数**设置参数。

版权所有 © 华为技术有限公司

图 2-12 委托 MSP 页面

表 2-2 委托参数

参数	说明
受托方标识	• 如果当前租户帐号由MSP创建，界面默认填充对应MSP的标识。 • 如果当前租户帐号是自注册，请向被委托的MSP获取唯一标识码（MSP帐号界面右侧唯一ID）。
委托列表	可以委托给MSP代维的服务列表及对应的执行权限。 • 当委托角色选择为“边界防护与响应管理员”时，MSP对业务有操作权限。 • 当委托角色选择为“边界防护与响应审计员”时，MSP对业务仅有查看权限。 • 当委托角色选择为“边界防护与响应开放接口操作员”时，MSP对开放接口业务有使用权限。 默认全部选择，单击服务卡片上的“自定义角色”可以选择委托的角色。
委托到期时间	选择委托到期时间，到达该时间后，本次委托将自动结束。
说明	委托说明，此处填写的内容将在MSP的审批流程中显示。

步骤4 单击“确定”。

步骤5 在弹出的授权清单界面，确认风险，勾选“我已阅读代操作授权风险告知协议并明确该操作的风险”，单击“确定”。

在MSP审批同意后，将与MSP建立委托关系。

----结束

版权所有 © 华为技术有限公司

2.2.1.2.3 开通服务套餐

背景信息

线下购买云服务License后，在华为乾坤激活线下订单。本服务配套的天关型号，如**表1 天关型号**所示。

表 2-3 天关型号

设备型号	激活方式
Eudemon1000E-T1	请参见**操作步骤**。

操作步骤

1. 使用租户帐号登录华为乾坤控制台。
2. 在界面右上方单击“订单”，选择“我的套餐”页签。
3. 单击“开通服务”，选择“根据SN激活”，输入设备的SN，单击“开通”。

图 2-13 输入 SN

4. （可选）在“开通服务”页面，单击“添加授权”。
   如果华为工程师已在ESDP系统中激活License，则此界面会显示已激活的授权ID，此时无需执行本步骤。

版权所有 © 华为技术有限公司

图 2-14 开通服务

5. （可选）在“添加授权”页面，根据提示输入授权ID，单击“确定”。

   如果华为工程师已在ESDP系统中激活License，则无需执行本步骤。

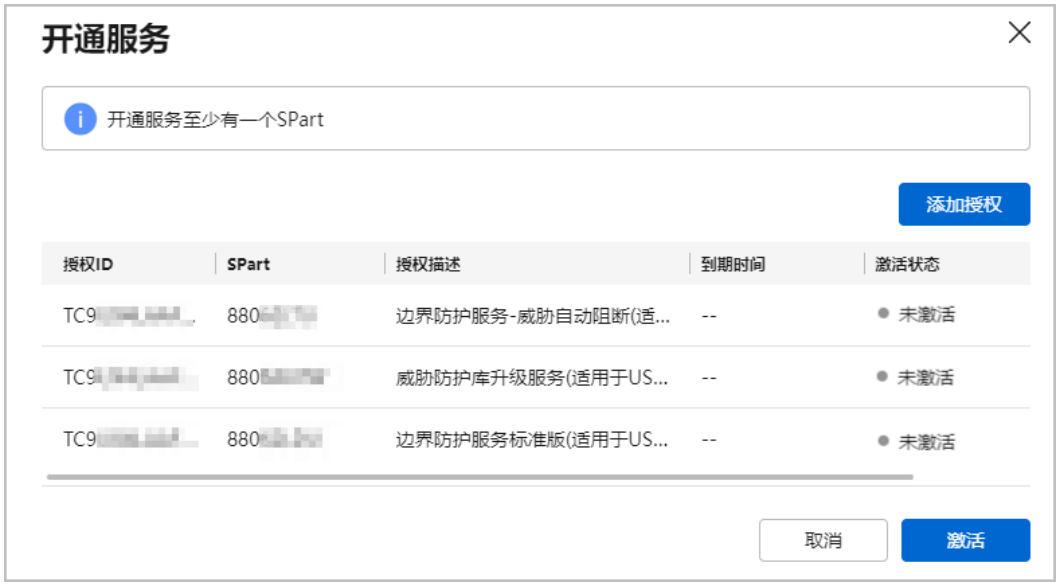
   如果没有激活License，则需要添加授权ID，边界防护与响应服务相关的授权ID包括边界防护服务标准版授权ID、边界防护服务专业版授权ID、边界防护服务-威胁自动阻断授权ID、威胁防护库升级服务授权ID。请根据实际购买的授权ID填写。

图 2-15 添加授权

6. 在“开通服务”页面，单击“激活”。

版权所有 © 华为技术有限公司

图 2-16 开通服务



7. 开通成功后，在界面右上方选择“资源中心 > 设备管理 > 设备”，在显示界面中可以查看到设备处于未注册状态。

2.3 部署指南

2.3.1 配置天关上线

边界防护与响应服务需要在客户侧部署天关才能正常使用。本服务配套的天关型号，如表2-4所示。

表 2-4 天关型号

设备型号	支持版本	推荐版本
Eudemon1000E-T1	V600R007C20SPC602及之后版本	V600R007C20SPC602

2.3.2 配置设备安全域

背景信息

华为乾坤需要识别攻击的发出区域、到达区域属于的安全域类型用于分析威胁事件。

华为乾坤提供以下几种类型的安全域：

- 信任域：用户信任的安全区域，通常用来定义用户的内部网络，华为乾坤不会对该区域发起的“威胁流量”进行封禁。
- 混合域：介于信任域和非信任域之间安全区域，属于一个特殊的网络，华为乾坤不会对该区域发起的“威胁流量”进行封禁。
- 非信任域：属于用户不信任的安全区域，通常用来定义Internet等不安全的网络，华为乾坤会自动封禁从该区域发起的“威胁流量”。

版权所有 © 华为技术有限公司

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 地址安全域管理”。

步骤3 在“设备安全域管理”区域中单击“创建”，将untrust区域添加到非信任域。

图 2-17 创建安全域

步骤4 （可选）将trust区域添加到信任域。华为乾坤默认已将trust区域添加到信任域中，如果trust区域被删除，请执行本步骤添加。

图 2-18 创建安全域

添加完成后，系统显示如下图所示。

版权所有 © 华为技术有限公司

图 2-19 设备安全域

----结束

2.3.3 配置全局白名单

背景信息

将租户全部的内网资产IP地址和对外提供服务的地址段，都添加到全局白名单，防止上述IP地址被华为乾坤（包括华为乾坤自动下发、华为乾坤安全服务人员）错误下发黑名单。

操作步骤

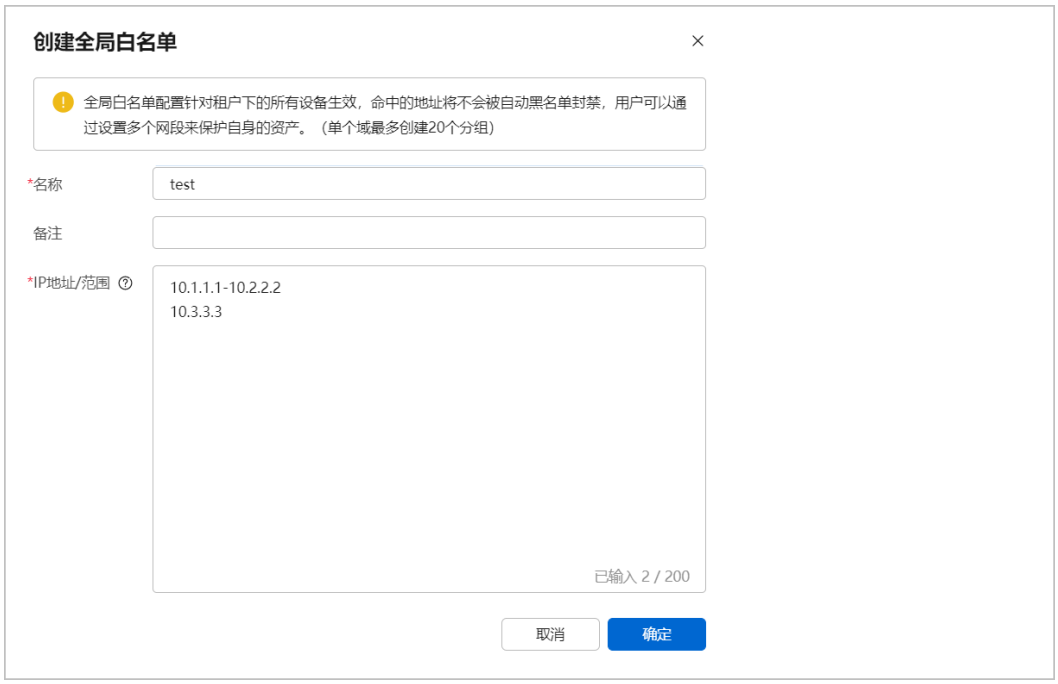
步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 地址安全域管理”。

步骤3 在“全局地址管理 > 全局白名单”区域配置全局白名单。

版权所有 © 华为技术有限公司

图 2-20 新建全局白名单



----结束

2.3.4 黑白名单授权

背景信息

只有在授予黑名单管理权限后，华为乾坤才可以对租户的设备自动执行下发黑名单操作。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ☰ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 授权管理”。

步骤3 按照界面提示完成操作。

----结束

2.3.5 订阅告警与报告

背景信息

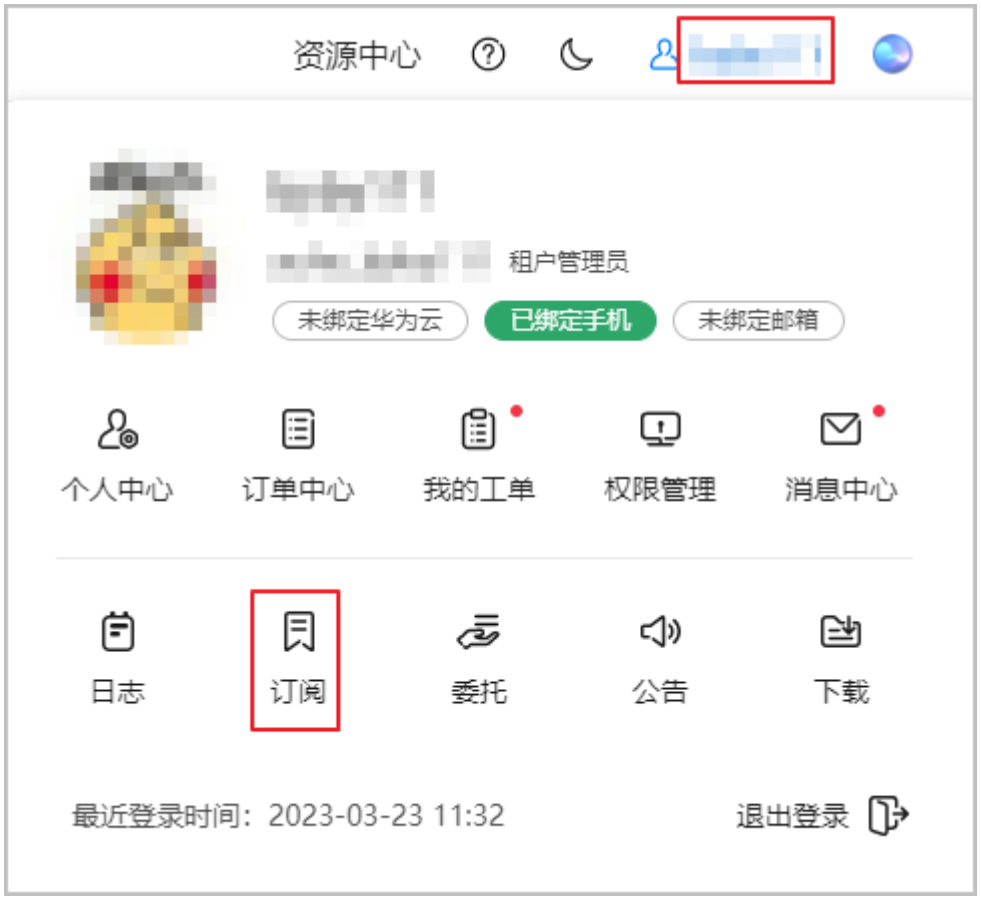
订阅后华为乾坤将以短信、邮件的方式向用户发送告警和安全报表。

操作步骤

步骤1 登录华为乾坤控制台，单击右上角帐号，选择“订阅”。

版权所有 © 华为技术有限公司

图 2-21 订阅



步骤2 根据界面提示按“订阅人”增加订阅。

图 2-22 按订阅人增加订阅

----结束

2.3.6 查看威胁事件

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“威胁事件”，可以查看到已经上报到华为乾坤的威胁事件，此时说明华为乾坤能够正常接收设备的威胁日志。

版权所有 © 华为技术有限公司

步骤3 查看后即可在华为乾坤云服务控制台处理安全事件，具体操作请参见《用户指南》中的“处置威胁事件”章节。

----结束

2.4 用户指南

2.4.1 查看网络安全状态

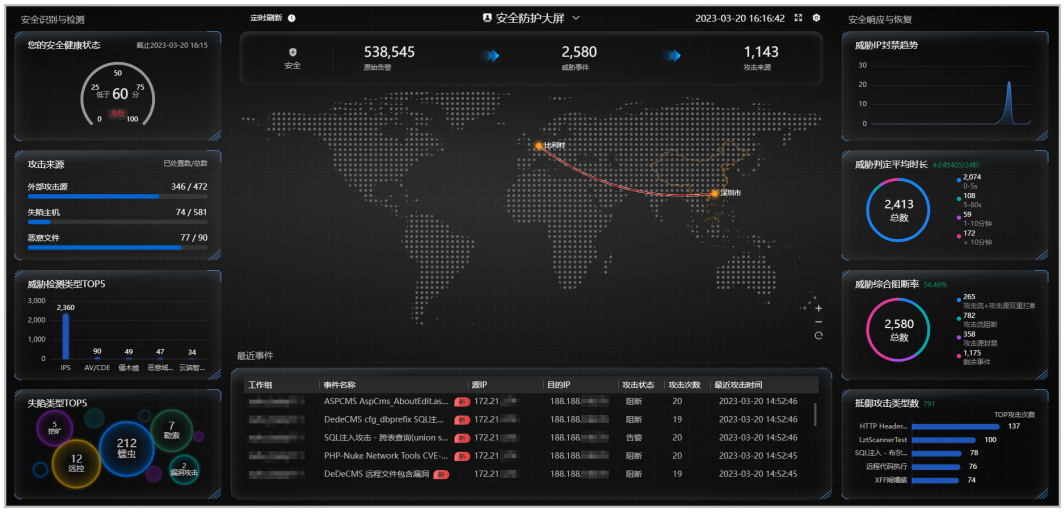
2.4.1.1 查看安全防护大屏

背景信息

安全防护大屏展示了安全识别与检测、安全响应与恢复和最近事件三块内容，包括失陷类型TOP5、威胁检测类型TOP5、攻击来源、系统健康状态、威胁判定平均时长、威胁综合阻断率、抵御攻击类型数量、威胁IP封禁趋势、最近事件等基础功能模块。智能识别网络安全状态，7*24小时实时监测、及时告警、主动处置，让企业网络更简单、更安全。

安全防护大屏根据用户开通的边界防护与响应服务套餐类别，提供差异化的功能模块选择。基础功能模块适用于开通任一套餐的用户；标注了“专业版”标签的功能模块，仅适用于开通**专业版**套餐的用户。功能模块套餐匹配及数据呈现，请参见**表2-5**。

图 2-23 安全防护大屏



操作步骤

步骤1 登录华为乾坤控制台，选择“大屏 > 安全防护大屏”。

说明

若只购买开通了华为乾坤安全相关服务，则默认进入安全防护大屏，无需选择。

步骤2 （可选）对安全防护大屏进行设置：

版权所有 © 华为技术有限公司

- 单击 按钮，可设置定时刷新的间隔周期。开启定时刷新功能后，页面将持续保持登录状态，达到会话超时时间也不会自动登出。
- 单击 按钮，可支持全屏查看。
- 单击 按钮，可自定义大屏名称，可选择需要展示的模块。

表 2-5 安全防护大屏模块说明

适用套餐	模块	说明
标准版、标准版+自动阻断、专业版	您的系统健康状态	安全相关服务在使用时，实时检测系统安全问题，根据评分规则得出系统的健康等级。
	攻击来源	展示已处置的外部攻击源、失陷主机、恶意文件数量与总数的对比。
	威胁检测类型TOP5	展示数量排名TOP5的威胁事件类型。
	失陷类型TOP5	展示数量排名TOP5的失陷主机类型。
	安全事件	展示各类安全事件数量 – 原始告警：华为乾坤根据天关提供的威胁日志识别的原始事件。 – 威胁事件：华为乾坤利用自动化模型分析和业务运营人员人工处置后，将原始事件聚合为威胁事件。 – 攻击来源：华为乾坤进一步智能处置后，将威胁事件分为外部攻击源、失陷主机和恶意文件三种类型，您可以在此处查看尚未处理的事件数量。
	攻击地图	动态呈现最新威胁事件源到端的攻击方向及地域分布。
	最近事件	按时间顺序由近到远呈现威胁事件相关信息。
	威胁IP封禁趋势	展示近30天封禁的攻击源IP数量变化趋势。
	抵御攻击类型数	展示数量排名TOP5已抵御的攻击类型。
	威胁判定平均时长	华为乾坤根据天关提供的威胁日志，进行分析后判断是否识别为威胁事件，展示其平均检测时长。

版权所有 © 华为技术有限公司

适用套餐	模块	说明
	威胁综合阻断率	展示威胁事件阻断情况。 – 攻击流+攻击源双重拦截：天关的安全防御策略识别到并已拦截和华为乾坤已执行下发黑名单操作的威胁事件。 – 攻击流阻断：天关的安全防御策略识别到并已拦截的威胁事件。 – 攻击源封禁：华为乾坤已执行下发黑名单操作的威胁事件。 – 剩余事件：未处理的威胁事件。
专业版	恶意文件类型TOP5	展示按文件类型（exe、zip等）划分，数量排名TOP5的恶意文件类型。
	主机恶意文件数TOP5	展示单终端存在恶意文件数量排名TOP5的主机IP。
	攻击源地理位置TOP5	展示攻击源数量排名TOP5的国家或区域。
	威胁事件严重级别分布	展示不同严重级别威胁事件数量的饼状分布。
	专项类型趋势	展示近30天外部攻击源、失陷主机、恶意文件的数量变化趋势。
	专项类型处置状态	展示外部攻击源、失陷主机、恶意文件的处置状态（未处置、已封禁、已忽略、人工处置）。

----结束

2.4.1.2 查看服务首页

背景信息

边界防护与响应服务首页支持查看服务整体运行状况，包括“本地设备，实时防护”、“云端分析，智能判定”、“风险溯源，深度清理”三大模块。同时还呈现了TOP抵御攻击类型、威胁综合阻断率、近30天威胁事件趋势、近30天黑名单趋势等统计信息。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 查看边界防护与响应服务首页。

版权所有 © 华为技术有限公司

图 2-24 边界防护与响应服务首页

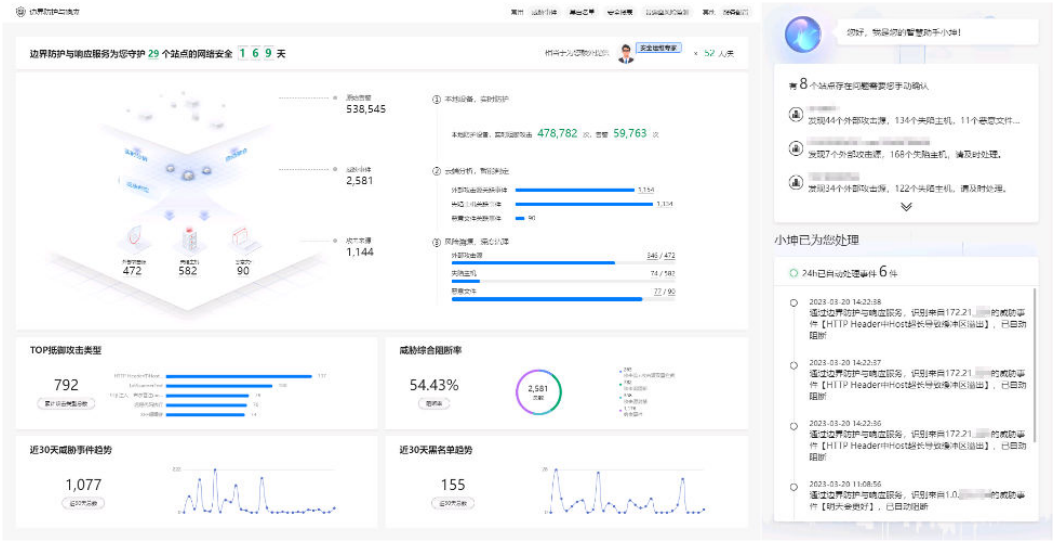


表 2-6 边界防护与响应服务首页介绍

板块	模块	说明
服务价值呈现	边界防护与响应服务为您守护X个站点的网络安全X天	展示站点数量、已使用服务的时间和换算的人效，单击站点数字可以查看站点列表。
	概览	展示安全事件整体概况。 ● 原始告警：华为乾坤根据天关提供的威胁日志识别的原始事件。 ● 威胁事件：华为乾坤利用自动化模型分析和业务运营人员人工处置后，将原始事件聚合为威胁事件。您可以在此处单击事件数字查看尚未处理的威胁事件列表 ● 攻击来源：华为乾坤进一步智能处置后，将威胁事件分为外部攻击源、失陷主机和恶意文件三种类型。
	TOP抵御攻击类型	展示数量排名TOP5已抵御的攻击类型。
	威胁综合阻断率	展示威胁事件阻断情况。 ● 攻击流+攻击源双重拦截：天关的安全防御策略识别到并已拦截和华为乾坤已执行下发黑名单操作的威胁事件。 ● 攻击流阻断：天关的安全防御策略识别到并已拦截的威胁事件。 ● 攻击源封禁：华为乾坤已执行下发黑名单操作的威胁事件。 ● 剩余事件：未处理的威胁事件。

版权所有 © 华为技术有限公司

板块	模块	说明
	近30天威胁事件趋势	展示近30天威胁事件数量的变化趋势。
	近30天黑名单趋势	展示近30天黑名单下发数量的变化趋势。
小坤智能助手	健康状态评估	• 以站点维度，提供处置威胁事件的快捷入口。
	小坤已为您处理	华为乾坤对异常事件自动处理，保障用户业务正常运行。 展示近24小时此类事件的数量和概要。

----结束

2.4.2 快速配置

背景信息

为正常使用边界防护与响应服务，除设备上线外，用户还需在华为乾坤添加多项配置。为简化开局流程，降低学习成本，边界防护与响应服务提供快速配置指引，用户可以根据提示，在相应页面完成对应配置。

初始配置

当用户首次登录到华为乾坤后，边界防护与响应服务将自动弹出初始配置的提示界面，用户需要完成以下配置项：

- **地址安全域管理**：完善安全域，帮助用户更好地管理信任网段、隔离威胁网段。
- **授权管理**：授予相关权限，安全专家将会替代本地运维，实现防护过程自动化，分钟级响应处置威胁攻击，保障用户的网络使用安全。
- 更多配置
  - 威胁自动阻断配置：对于华为乾坤自动下发的黑名单，用户可以自定义封禁时长。
  - 自定义签名配置：用户可以选择是否开启IPS自定义签名功能。授权后，华为乾坤将向设备下发自定义签名，自定义签名可以依据客户不同业务，实现灵活处理，提升威胁防御能力。自定义签名将由华为乾坤统一验证、配置、下发，请勿直接在设备上配置自定义签名，以免与华为乾坤下发的签名冲突。

    对于业务运营人员而言，在紧急情况下可针对多用户进行评估后下发IPS自定义签名，IPS自定义签名可作为网络补丁，对已产生的攻击进行拦截；对于用户而言，IPS自定义签名可用于拦截私有或定制的流量。

    如需使用此功能，请将授权按钮置为“已授权”状态。

    图 2-25 自定义签名配置

版权所有 © 华为技术有限公司

- 订阅设置：边界防护与响应服务提供紧急事件的短信、邮件告警功能，同时定期发送安全周报、月报至用户邮箱，用户可以通过订阅开启相关功能，具体操作请参见《租户操作指南》中“**订阅管理**”章节。

建议用户按照推荐步骤完成初始配置，以获得更好的服务使用体验。如果用户选择暂时跳过初始配置，后续使用服务过程中期望继续配置，可以单击右上角菜单栏的“初始配置”进入初始配置流程。

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 按照提示完成初始配置。

说明

用户在完成初始配置后，如果需要对各配置项进行修改，可以单击右上角菜单栏的“服务配置”进入服务配置流程。

----结束

2.4.3 处置威胁事件

2.4.3.1 事件概览

背景信息

华为乾坤识别出威胁事件后，经过进一步智能处置，将威胁事件分为外部攻击源、失陷主机和恶意文件三种类型。

威胁事件页面默认显示近30天的数据。租户可以单击右上角的威胁周期页签，指定页面显示某个特定时间段内的数据。当租户选定“更多”页签时，页面将显示近3个月的数据。

说明

租户在使用服务期间，数据留存的最长期限为3个月，超过3个月的数据将丢弃。

某些特殊场景下的威胁事件，会在参数列打上对应标签：

- 攻击成功的威胁事件在“事件名称”栏打上“攻击成功”标签。
- 采用旁路模式上线的设备检测到的威胁事件，“攻击状态”栏将打上“旁路”标签。旁路模式的设备无法对流量进行阻断。

威胁事件支持“按事件类型”和“按站点”查看。两种方式呈现维度不同，但涉及的威胁事件相同。如果没有特殊说明，以下章节对外部攻击源、失陷主机、恶意文件的详细介绍均以“按事件类型”查看为例。

高等级租户享有对自身及下级租户威胁事件的查看、处置权限。

操作步骤

“按事件类型”查看时，威胁事件页面由事件概览、外部攻击源、失陷主机、恶意文件几个模块组成。

 版权所有 © 华为技术有限公司

图 2-26 按事件类型查看

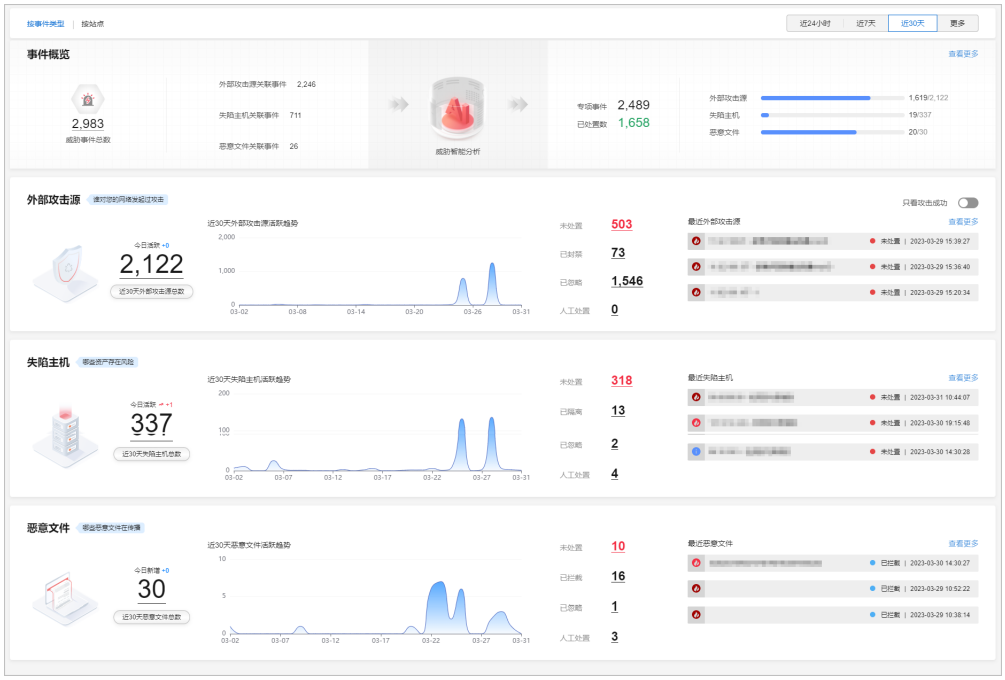


表 2-7 按事件类型查看

模块	说明
事件概览	展示威胁事件相关信息，包含事件总数、自动阻断的事件总数和占比。蓝色线条标识已处置（包含自动处置和人工处置）的威胁事件，灰色线条标识剩余未处置的威胁事件，您可以将鼠标悬浮于线条上查看详细信息。
外部攻击源	展示外部攻击源相关信息，单击“查看更多”可进入外部攻击源详情页面。 外部攻击源的详细介绍请参见**外部攻击源**。
失陷主机	展示失陷主机相关信息，单击“查看更多”可进入失陷主机详情页面。 失陷主机的相关介绍请参见**失陷主机**。
恶意文件	展示恶意文件相关信息，单击“查看更多”可进入恶意文件详情页面。 恶意文件的相关介绍请参见**恶意文件**。

“按站点”查看时，威胁事件页面以站点维度显示各站点下的威胁事件，单击“站点详情”可以查看站点模型。

站点是基于地理信息的设备集合，是设备分域的最小单位，是网络、安全质量评估的对象。租户可以将同一范围内的设备添加到同一站点中，在平台统一监测和管理。

华为乾坤根据天关在不归属于任何站点期间内提供的威胁日志，进行聚合后得出的威胁事件，将会被纳入“未知站点”。

版权所有 © 华为技术有限公司

图 2-27 按站点查看

2.4.3.2 外部攻击源

前提条件

已完成**黑白名单授权**。

背景信息

华为乾坤根据天关提供的日志判断威胁事件的发出区域、到达区域，如果威胁事件的发出区域位于非信任域或混合域，则此威胁事件被识别为外部攻击源。

针对外部攻击源，华为乾坤有如下几种处置方式：

- 华为乾坤智能分析后成功下发IP黑名单，其状态显示为“已封禁”。
- 华为乾坤智能分析后无法下发IP黑名单，由业务运营人员进一步分析后手动成功下发IP黑名单，其状态显示为“已封禁”。
- 华为乾坤智能分析和业务运营人员根据现有信息无法处置时，需要租户进行人工处置，其状态显示为“未处置”。

租户需要对“未处置”的外部攻击源进行处置，处置方法包括封禁攻击源和标记状态（已人工处置、已忽略）。

购买如下版本时，才能使用华为乾坤自动下发IP黑名单和业务运营人员分析功能。

- 同时购买边界防护与响应服务**标准版**+自动阻断
- 边界防护与响应服务**专业版**
- 边界防护与响应服务**高级版**
- 边界防护与响应服务**试用版**

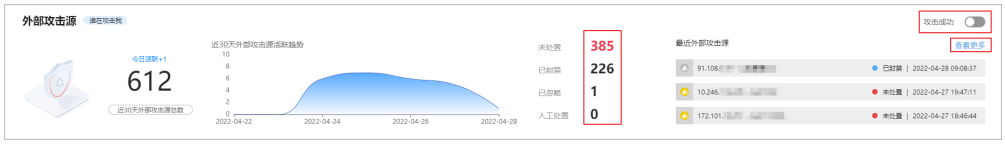
操作步骤

步骤1 登录华为乾坤控制台，选择“ ☰ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“威胁事件”。

步骤3 查看外部攻击源概览，单击数据或“查看更多”进入对应处理页面。

图 2-28 外部攻击源概览



版权所有 © 华为技术有限公司

步骤4 针对未处置的外部攻击执行处置操作，包括以下几种处置方法。

- 封禁攻击源

  当确认此IP地址为外部攻击源地址，此时可在操作列单击“封禁攻击源”下发IP黑名单。

  华为乾坤向天关下发IP黑名单后，由天关对黑名单IP执行封禁操作，来自黑名单IP的请求和去往黑名单IP的请求都会被阻断。

  说明

  设备存在绑定热备场景。当两台设备均已成功上线并绑定热备，主设备无法正常工作时，备设备会在短时间内进行替代，完全实现主设备功能。以事件维度进行封禁攻击源操作时，会对绑定热备的两台设备同时下发IP黑名单，在历史IP黑名单中显示两条记录。

  图 2-29 封禁攻击源

- 标记状态
  - 已人工处置

    租户根据具体的事件采取人工处置，比如根据事件的源、目的地址查找目标主机，并对目标主机执行病毒查杀。处置完成后，在操作列将外部攻击标记为“已人工处置”。
  - 忽略

    租户经过排查后发现事件无需处理或者是误报时，在操作列将外部攻击标记为“忽略”。后续就无需再关注此事件。

说明

如果您不知如何处置，或者处置后未能有效解决，请求助对应MSSP安全云服务商或渠道商。

----结束

后续处理

- 外部攻击源的攻击源IP前显示攻击源IP所在国家国旗，鼠标悬停在国旗上可显示国名。您可以单击外部攻击源列表中的攻击源IP，查看此外部攻击源详情页面。

  您可以在高级搜索中设置筛选条件，单击“导出”，导出符合筛选条件的外部攻击源列表（Excel格式文件）；或勾选预导出的外部攻击源，单击“导出”，导出选中的外部攻击源列表。

版权所有 © 华为技术有限公司

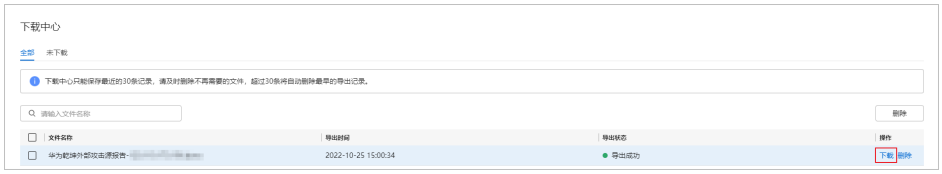
图 2-30 外部攻击源列表

- 外部攻击源详情页面包含处置建议、操作记录、外部攻击源分析、关联威胁事件列表等信息。
  - 您可以单击“导出详情”，导出包含外部攻击源详细信息的Word格式文件。

    图 2-31 外部攻击源详情页面

    导出完成后，请单击右上角帐号，选择“下载中心”，下载对应文件。

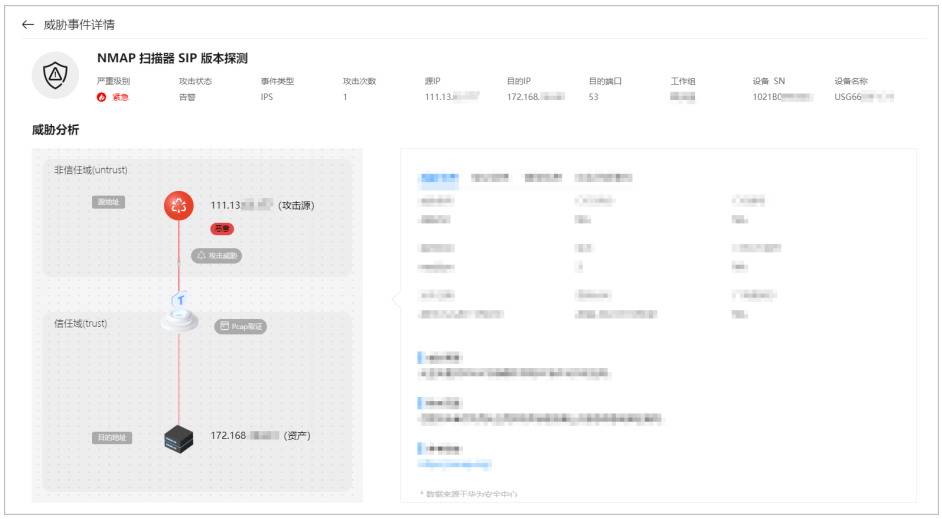
    图 2-32 下载中心

  - 您可以单击外部攻击源详情页面中关联威胁事件列表中的事件名称，查看此事件的详情页面。

版权所有 © 华为技术有限公司

图 2-33 事件详情页面



说明

外部攻击源详情页面可能涉及公网地址，仅用于事件信息展示以帮助用户了解威胁事件，服务不会主动发起与这些公网地址的连接。

2.4.3.3 失陷主机

前提条件

已完成**黑白名单授权**。

背景信息

华为乾坤根据天关提供的日志判断威胁事件的发出区域、到达区域，如果威胁事件的发出区域位于信任域，则此威胁事件被识别为失陷主机。

根据失陷类型的不同，业务运营人员可以为失陷主机打上“勒索”、“挖矿”、“蠕虫”、“远控”、“漏洞攻击”、“不安全配置”等标签，暂未识别失陷类型的归入“其他”。

为了不影响租户内部主机的业务，针对失陷主机，华为乾坤（包括自动下发和业务运营人员下发）有如下几种处置方式：

- 对于恶意域名检测类型的事件，华为乾坤智能分析后成功下发域名黑名单的，其状态显示为“已隔离”，同时发送短信和邮件通知用户。用户再次访问域名黑名单中的域名时，设备会上报告警日志。
- 对于恶意域名检测类型的事件，华为乾坤智能分析后没有成功下发域名黑名单的，或其他类型的事件，华为乾坤向租户发送短信和邮件告警，同时将失陷主机的状态置为“未处置”。

已发送短信或邮件告警的失陷主机在威胁事件列表中显示 标记。租户需要进一步确认和处置，处置方法包括隔离主机和标记状态（已人工处置、忽略）。

USG6603F-C天关、USG6000F防火墙不支持下发域名黑名单功能。USG6000E-C天关、USG6000E防火墙支持自动下发域名黑名单功能，且同时满足如下条件时，才能正常使用自动下发域名黑名单功能。

版权所有 © 华为技术有限公司

- 购买边界防护与响应服务**试用版**、边界防护与响应服务**高级版**或同时购买边界防护与响应服务**标准版**+自动阻断。
- 设备上存在名称为“trust-untrust”的安全策略。
- 设备上存在名称为“huawei_qiankun_dns”的DNS过滤配置文件（此配置文件在设备上线过程中由华为乾坤自动下发，且默认动作为告警）。

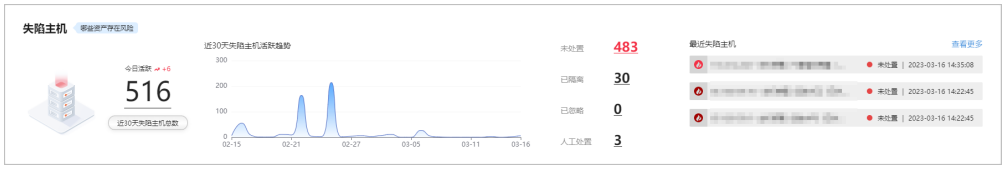
操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“威胁事件”。

步骤3 查看失陷主机概览，并单击数据或“查看更多”进入相应处理页面。

图 2-34 失陷主机概览



步骤4 针对未处置的失陷主机事件执行处置操作，包括以下几种处置方法。

- 隔离主机

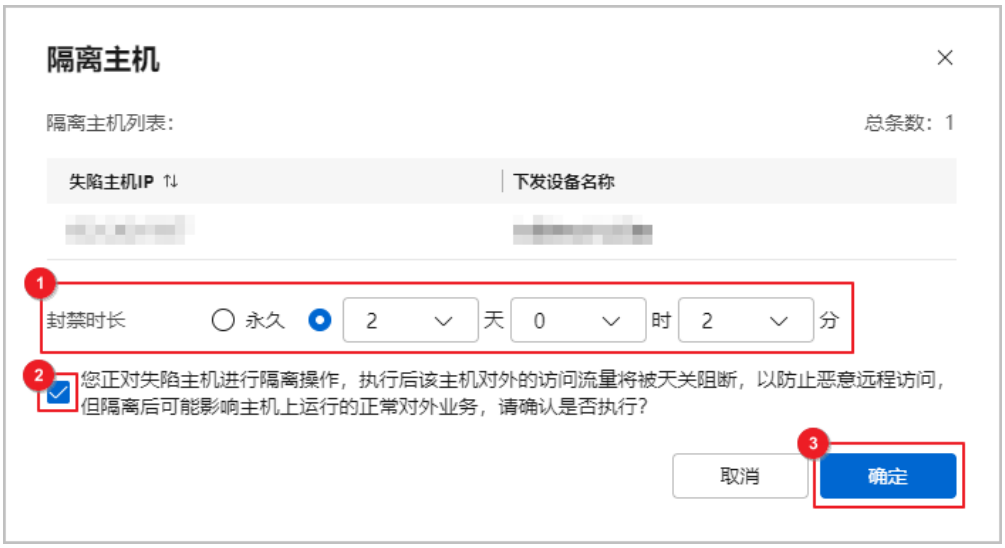
  当确认此失陷主机上无业务运行，或者隔离后不影响正常业务，此时可在操作列单击“隔离主机”下发IP黑名单。

  华为乾坤向天关下发IP黑名单后，由天关对黑名单IP执行隔离操作，来自黑名单IP的请求和去往黑名单IP的请求都会被阻断。

  说明

  设备存在绑定热备场景。当两台设备均已成功上线并绑定热备，主设备无法正常工作时，备设备会在短时间内进行替代，完全实现主设备功能。以事件维度进行隔离主机操作时，会对绑定热备的两台设备同时下发IP黑名单，在历史IP黑名单中显示两条记录。

图 2-35 隔离主机



 版权所有 © 华为技术有限公司

- 标记状态
  - 已人工处置

    租户根据具体的事件采取人工处置，比如对失陷主机执行病毒查杀，并确认此主机已无安全风险后，在操作列将失陷主机标记为“已人工处置”。
  - 忽略

    租户经过排查后发现失陷主机无需处理或者是误报时，在操作列将失陷主机标记为“忽略”。后续就无需再关注此事件。

说明

- 处置建议中可能包含处置手册下载链接，可供您参考。
- 如果您不知如何处置，或者处置后未能有效解决，请求助对应MSSP安全云服务商或渠道商。

----结束

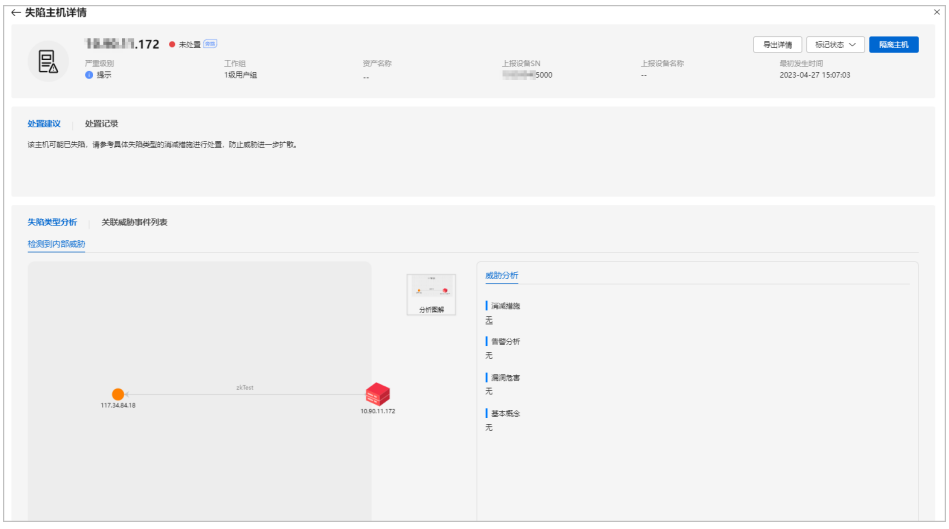
后续处理

- 您可以单击失陷主机列表中的失陷主机IP，查看此失陷主机详情页面。

图 2-36 失陷主机列表

- 失陷主机详情页面包含处置建议、操作记录、失陷类型分析和关联威胁事件列表等信息。
  - 您可以单击“导出详情”，导出包含失陷主机详细信息的Word格式文件。

图 2-37 失陷主机详情页面



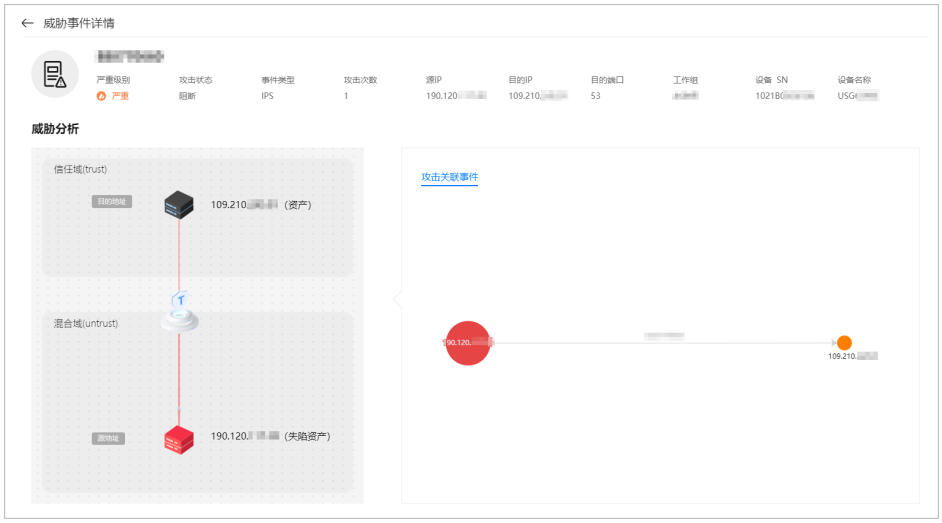
导出完成后，请单击右上角帐号，选择“下载中心”，下载对应文件。

版权所有 © 华为技术有限公司

图 2-38 下载中心

- 您可以单击失陷主机详情页面中关联威胁事件列表中的事件名称，查看此事件的详情页面。

图 2-39 事件详情页面



说明

失陷主机详情页面可能涉及公网地址，仅用于事件信息展示以帮助用户了解威胁事件，服务不会主动发起与这些公网地址的连接。

2.4.3.4 恶意文件

背景信息

华为乾坤根据天关提供的日志判断威胁事件的威胁类型，如果威胁事件的威胁类型为AV/CDE，则此威胁事件被识别为恶意文件。

针对恶意文件，有如下几种处置方式：

- 华为乾坤智能分析后成功下发IP黑名单，其状态显示为“已拦截”。
- 天关检测到恶意文件时已拦截，其状态显示为“已拦截”。
- 华为乾坤智能分析后向租户发送短信和邮件告警，其状态显示为“未处置”。
- 华为乾坤智能分析后根据现有信息无法处置，或者天关未拦截时，其状态显示为“未处置”。

租户需要对“未处置”的恶意文件进行处置，处置后将其状态标记为已人工处置或已忽略。

操作步骤

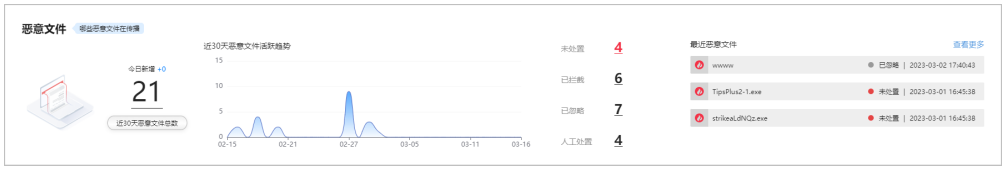
步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

 版权所有 © 华为技术有限公司

步骤2 在右上角菜单栏选择“威胁事件”。

步骤3 查看恶意文件概览，并单击数据或“查看更多”进入相应处理页面。

图 2-40 恶意文件概览



步骤4 针对未处置的恶意文件标记状态。

- 已人工处置

  租户根据具体的事件采取人工处置，比如根据事件的源、目的地址、文件名等查找并清除恶意文件。

  确认风险主机中已清除恶意文件后，在操作列将事件标记为“已人工处置”。

- 忽略

  租户经过排查后发现为误报或无需处理时，在操作列将事件标记为“忽略”。后续就不用再关注此事件。

说明

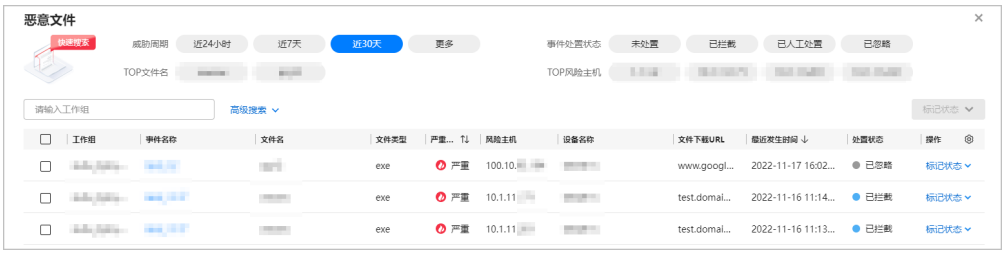
如果您不知如何处置，或者处置后未能有效解决，请求助对应MSSP安全云服务商或渠道商。

----结束

后续处理

- 您可以单击恶意文件列表中的事件名称，查看此恶意文件详情页面。

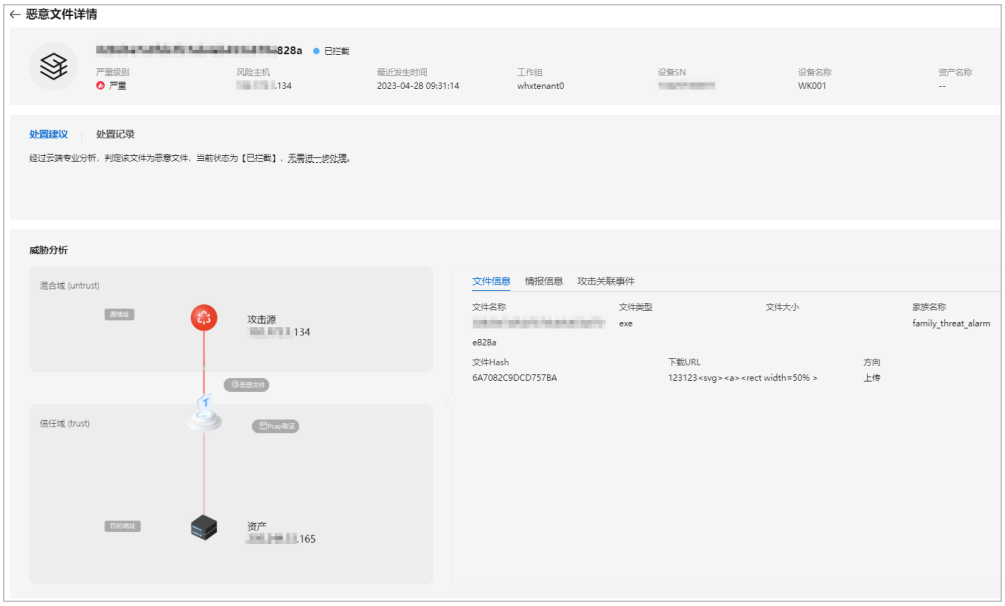
图 2-41 恶意文件列表



- 恶意文件详情页面包含处置建议、处置记录、威胁分析等。

版权所有 © 华为技术有限公司

图 2-42 恶意文件详情页面



说明

恶意文件详情界面中的事件名称以及恶意文件详情可能涉及公网地址，仅用于事件信息展示以帮助用户了解威胁事件，服务不会主动发起与这些公网地址的连接。

2.4.4 管理黑白名单

2.4.4.1 一键清除指定设备的 IP 黑名单

背景信息

对于已被下发IP黑名单的设备，如果存在业务异常，可以一键清除该设备的所有IP黑名单配置，以确保业务快速恢复。

注意

一键清除指定设备的所有IP黑名单，天关将失去防护能力，企业网络可能会遭到攻击，请谨慎操作。

高等级租户享有对自身及下级租户的IP黑名单的删除权限。

操作步骤

步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“黑白名单”。

步骤3 选择“黑名单 > IP黑名单”页签，单击“设备黑名单清除”。

步骤4 清除设备黑名单。

版权所有 © 华为技术有限公司

图 2-43 设备黑名单清除

----结束

2.4.4.2 手工创建 IP 黑白名单

背景信息

- IP黑名单是一种阻断措施，华为乾坤将IP黑名单下发给设备后，设备会丢弃命中IP黑名单的报文。

  从威胁事件维度看，下发IP黑名单有如下几种方式。

  - 外部攻击源：包括华为乾坤自动下发、业务运营人员下发、用户执行“封禁攻击源”下发。
  - 失陷主机：用户可以执行“隔离主机”下发。

  此外，用户还可以根据实际的网络环境或业务需要，从设备维度（针对某设备）手动下发IP黑名单，作为上述IP黑名单下发的补充手段，以提高安全防护的灵活性。
- IP白名单是一种放通措施，华为乾坤将IP白名单下发给设备后，设备会放通命中IP白名单的报文。

高等级租户享有对自身及下级租户的IP黑白名单的创建、修改权限。

说明

用户手动下发黑白名单时，如果设备黑白名单数量超规格，则会提示下发失败。

华为乾坤自动下发黑名单时，如果设备黑名单数量超过规格，华为乾坤将滚动删除之前自动下发的黑名单，以保证本次下发成功。当剩余的黑名单都由用户手动下发时，华为乾坤自动下发也会失败。

操作步骤

步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“黑白名单”。

版权所有 © 华为技术有限公司

步骤3 此处以创建IP黑名单为例，创建IP白名单与之类似。

选择“黑名单 > IP黑名单”页签，单击“创建”。

图 2-44 创建黑名单

参数	参数说明
选择设备	选择需要下发IP黑名单的设备。
源/目的	选择源IP地址或者目的IP地址，支持源、目的IP地址同时下发。

版权所有 © 华为技术有限公司

参数	参数说明
IP地址	阻断或放通的具体IP地址。 IP黑名单不支持下发D类保留地址：224.0.0.0-239.255.255.255。
协议	选择IP协议：ANY、TCP、UDP、ICMP
端口	未配置则默认所有端口。
封禁时长	未配置则默认为永久。

步骤4 单击“确定”，将IP黑名单部署到指定设备。

说明

设备存在绑定热备场景。当两台设备均已成功上线并绑定热备，主设备无法正常工作时，备设备会在短时间内进行替代，完全实现主设备功能。以设备维度下发IP黑名单时，并不会对备设备同步下发IP黑名单，历史IP黑名单记录中只会添加一条记录。

----结束

2.4.4.3 快速查看 IP 黑白名单

背景信息

IP黑白名单管理是边界防护的重要环节，相比传统复杂的安全检测方式，IP黑白名单可以直接、有效地阻断恶意攻击，从而节省天关系统资源，降低负载。

IP黑白名单主要来源于以下几种情况：

- 华为乾坤对威胁事件进行分析后，由华为乾坤自动下发的IP黑名单。
- 华为乾坤业务运营人员处理后确认为攻击，由业务运营人员下发IP黑名单。
- 租户在控制台手动创建并下发的IP黑白名单。

IP黑白名单包括以下几种状态：

- 已生效：IP黑白名单保存在华为乾坤，已经成功下发到天关设备，并已经生效。
- 部署中：IP黑白名单保存在华为乾坤，但未下发到天关设备。
- 部署失败：已部署下发指令，但由于其他原因导致下发失败。

高等级租户享有对自身及下级租户的IP黑白名单的查看权限。

操作步骤

步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“黑白名单”。

步骤3 此处以查看设备IP黑名单为例。

选择“黑名单 > IP黑名单”页签，单击“最近修改时间”栏的按钮，支持按照最近修改时间顺序或逆序查看。

版权所有 © 华为技术有限公司

图 2-45 查看设备 IP 黑名单

表 2-8 IP 黑名单列表关键参数说明

参数	说明
是否全局白名单	如果源/目的IP在全局白名单中，IP黑名单无法从华为乾坤自动下发（包括自动下发、业务运营人员下发），仅可由租户、MSP手动创建并下发。
创建者	• 租户：适用于租户在华为乾坤手动下发IP黑名单场景。 • 受托方：适用于MSP在华为乾坤手动下发IP黑名单场景。 • 系统：适用于华为乾坤自动下发或业务运营人员下发IP黑名单场景。 • 三方接口：适用于运营商场景。

----结束

后续处理

- 查看历史IP黑名单

  历史IP黑名单包含已生效和已失效的黑名单，您可以通过“黑白名单 > 黑名单 > IP黑名单 > 历史IP黑名单”查看。

- 修改IP黑/白名单

  您可以选中某个IP黑/白名单，单击操作栏的“修改”，对IP黑/白名单策略进行重新配置。

- 删除IP黑/白名单

  您可以选中某个IP黑/白名单，单击操作栏的“删除”，删除指定IP黑/白名单。

2.4.4.4 手工创建域名黑名单

背景信息

域名黑名单是一种阻断措施，华为乾坤将域名黑名单下发给设备后，内部资产将不能访问黑名单中的恶意域名。

一般情况下，华为乾坤对威胁事件进行智能分析后，自动下发域名黑名单。此外，用户还可以根据实际的网络环境或业务需要，从设备维度（针对某设备）手动下发域名黑名单，作为上述域名黑名单下发的补充手段，以提高安全防护的灵活性。

高等级租户享有对自身及下级租户的域名黑名单的创建、修改、删除权限。

版权所有 © 华为技术有限公司

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“黑白名单”。

步骤3 选择“黑名单 > 域名黑名单”页签，单击“创建”。

域名支持正则匹配，具体规则请将鼠标悬停在图标上查看。

图 2-46 创建域名黑名单

步骤4 单击“确定”，将域名黑名单部署到指定设备。

说明

域名黑名单不会立即下发到设备的DNS过滤配置文件。华为乾坤每分钟批量下发一次，默认有效期为永久。

----结束

2.4.4.5 快速查看域名黑名单

背景信息

域名黑名单管理是边界防护的重要环节，通过安全策略关联DNS过滤配置文件，可以有效避免内部资产对恶意域名的持续访问。

域名黑名单主要来源于以下几种情况：

- 华为乾坤对威胁事件进行智能分析后，由华为乾坤自动下发。

版权所有 © 华为技术有限公司

- 租户在控制台手动创建并下发域名黑名单。

域名黑名单包括以下几种状态：

- 已生效：域名黑名单保存在华为乾坤，已经成功下发到天关设备，并已经生效。
- 部署中：域名黑名单保存在华为乾坤，但未下发到天关设备。
- 部署失败：已部署下发指令，但由于其他原因导致下发失败。

高等级租户享有对自身及下级租户的域名黑名单的查看权限。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“黑白名单”。

步骤3 选择“黑名单 > 域名黑名单”页签，查看域名黑名单列表。

----结束

后续处理

- 删除域名黑名单
  您可以选中某个域名黑名单，单击操作栏的“删除”，删除指定域名黑名单。

2.4.5 查看安全报表

前提条件

已通过订阅管理绑定邮箱，具体操作请参见《租户操作指南》中“**订阅管理**”章节

背景信息

华为乾坤为帮助租户了解某个时段内网络安全状态的变化趋势，提供安全报表查询功能。

租户可以在安全报表界面查看安全报表，华为乾坤将在每周一或每个月的第一天，生成上周或上个月的安全报表。在“帐户 > 订阅”中订阅“边界防护安全报表”后，租户还能通过绑定邮箱接收安全周报或月报。

目前支持的报表类型包含常规报表和自定义报表。

- 常规报表：分为周报和月报两种类型。一级租户支持查看当前工作组下各个租户的个体报表和所有租户的汇总报表，非一级租户仅支持查看个体报表。
- 自定义报表：业务运营人员或MSP可以指定自定义周期生成报表。自定义报表不支持常规订阅，仅可由业务运营人员或MSP主动推送，并于记录生成后定时删除。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“安全报表”。

 版权所有 © 华为技术有限公司

步骤3 选择任一报表，单击“预览”。

图 2-47 安全报表列表

步骤4 查看安全报表。

表 2-9 安全报表介绍

模块	说明
网络安全概览	展示原始告警、威胁事件、专项风险的统计数据。
威胁事件	威胁事件是系统基于原始安全告警，通过关联分析、专家模型、人工智能等自动化研判技术，自动识别出的真实安全攻击事件。 展示其活跃趋势、严重级别统计、响应状态统计、威胁类型、目标地址、详情等相关信息。
专项风险 | 外部攻击源	外部攻击源是系统通过威胁事件自动分析研判后，识别的外部攻击者地址，及时处置可降低来自外部的入侵威胁。 展示其数量趋势、严重级别统计、威胁状态统计、攻击源地理位置、攻击类型、详情等相关信息。
专项风险 | 失陷主机	失陷主机是系统通过对威胁事件自动分析研判后，识别的内部风险资产地址，包括挖矿、远控、勒索、内部攻击威胁等失陷类型。 展示其活跃趋势、严重级别统计、威胁状态统计、恶意行为、失陷类型、详情等相关信息。
专项风险 | 恶意文件	恶意文件是系统通过对威胁事件自动分析研判后，识别出的恶意程序文件，包括木马、蠕虫、挖矿、勒索、广告等文件类型，系统会自动检测并拦截高风险的恶意文件。 展示其数量趋势、严重级别统计、威胁状态统计、文件类型、风险主机、详情等相关信息。

----结束

后续处理

- 您可以在安全报表预览页面单击“PDF导出”，下载PDF版安全报表到本地。
- 了解安全状态变化趋势后，您可以参考**处置威胁事件**进行处置。

说明

如果您不知如何处置，或者处置后未能有效解决，请求助对应MSSP安全云服务商或渠道商。

版权所有 © 华为技术有限公司

2.4.6 地址安全域管理

2.4.6.1 监测安全域状态

背景信息

天关的奇数编号接口（属于untrust区域）用于连接上行设备，偶数编号接口（属于trust区域）用于连接下行局域网设备，如果上下行连接错误，将影响华为乾坤威胁事件通知及展示。

华为乾坤根据过去24小时聚合的IPS事件和CDE事件，判断天关上下行接口连线接反的概率，例如CDE事件的概率为100%，则表示根据CDE事件判断，天关上下行接口连线100%接反。

华为乾坤将判断的结果提供给业务运营人员，业务运营人员根据IPS事件和CDE事件综合判断是否接反，如果确认接反，则在此界面提示用户存在设备安全域接反的情况。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 地址安全域管理”。

步骤3 在“设备安全域管理”区域，查看设备卡片。

说明

如果租户在此界面看到存在设备安全域接反的提示，表示天关线缆连接错误，租户需要交换本地天关上下行接口的连线。

图 2-48 存在设备安全域接反

----结束

2.4.6.2 配置全局白名单

背景信息

如果某些资产上运行的业务非常重要，或者用户确定某些资产不存在安全风险，则可以将这些资产的IP地址配置到全局白名单中，以防止这些资产的IP地址被错误下发IP黑名单。

版权所有 © 华为技术有限公司

某资产的IP地址被配置为全局白名单后，华为乾坤（包括自动下发、业务运营人员下发）不能将此IP地址当做IP黑名单下发给天关。用户在华为乾坤通过**封禁攻击源**、**隔离主机**或**配置IP黑名单策略**将此IP地址当作IP黑名单下发时，华为乾坤将提示用户是否要继续下发，租户根据实际情况选择是否需要继续下发。

操作步骤

步骤1 登录华为乾坤控制台，选择“ > 我的服务 > 边界防护与响应”。

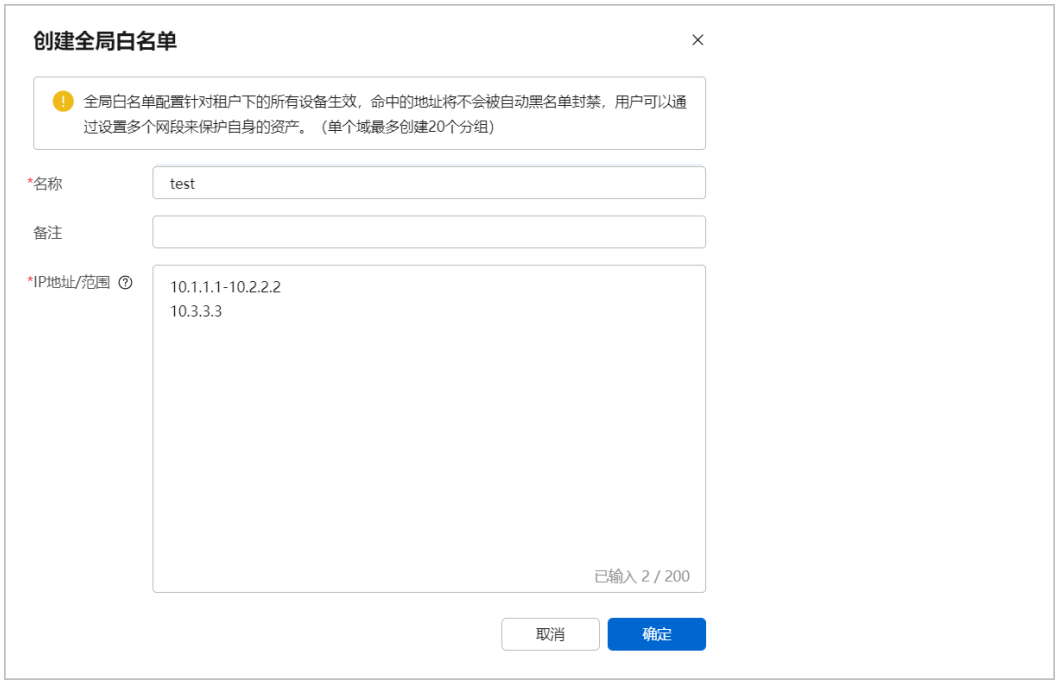
步骤2 在右上角菜单栏选择“服务配置 > 地址安全域管理”。

步骤3 在“全局地址管理 > 全局白名单”区域配置全局白名单。

说明

- “IP地址/范围”的输入规则请将鼠标悬停在图标上查看。
- 全局白名单支持名称自定义，用户可以根据业务需求，灵活设置多个全局白名单（单个域最多创建20个），但多个全局白名单中的网段不能重叠。

图 2-49 新建全局白名单



----结束

后续处理

- 您可以单击全局地址管理中的全局白名单，修改已有配置。
- 您可以单击全局地址管理中已有全局白名单的图标，删除已有配置。

版权所有 © 华为技术有限公司

2.4.6.3 配置不可信内网地址

背景信息

华为乾坤（包括自动下发、业务运营人员下发）发现内网地址存在风险时，默认不会将这些IP地址当作IP黑名单下发给天关。如果某些内网地址具有较高安全风险，且用户允许将其加入IP黑名单，则可以将这些内网地址配置到“不可信内网地址”中。

华为乾坤在发现存在风险的内网地址时，会与“不可信内网地址”中设置的内网地址进行匹配，如果匹配成功，就会将此IP地址当作IP黑名单下发给天关。如果未在“不可信内网地址”中找到该地址，则不会将其当作IP黑名单下发给天关。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右侧菜单栏选择“服务配置 > 地址安全域管理”。

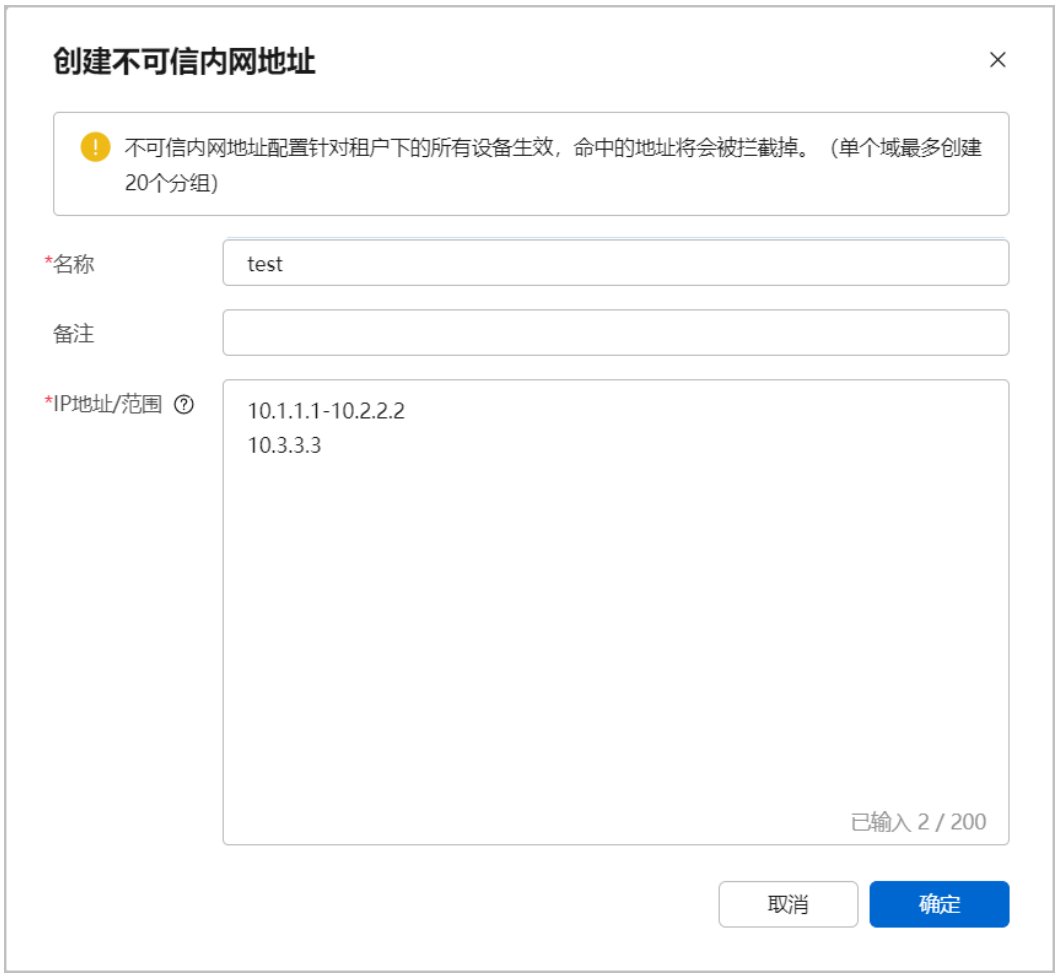
步骤3 在“全局地址管理 > 不可信内网地址”区域配置不可信内网地址。

说明

- “IP地址/范围”的输入规则请将鼠标悬停在图标上查看。
- 不可信内网地址支持名称自定义，用户可以根据业务需求，灵活设置多个不可信内网地址（单个域最多创建20个）。

版权所有 © 华为技术有限公司

图 2-50 新建不可信内网地址



----结束

后续处理

- 您可以单击全局地址管理中的不可信内网地址，修改已有配置。
- 您可以单击全局地址管理中已有不可信内网地址的图标，删除已有配置。

2.4.6.4 配置设备安全域

背景信息

华为乾坤需要识别攻击的发出区域、到达区域属于的安全域类型用于分析威胁事件。

华为乾坤提供以下几种类型的安全域：

- 信任域：用户信任的安全区域，通常用来定义用户的内部网络，华为乾坤不会对该区域发起的“威胁流量”进行封禁。
- 混合域：介于信任域和非信任域之间安全区域，属于一个特殊的网络，华为乾坤不会对该区域发起的“威胁流量”进行封禁。
- 非信任域：属于用户不信任的安全区域，通常用来定义Internet等不安全的网络，华为乾坤会自动封禁从该区域发起的“威胁流量”。

版权所有 © 华为技术有限公司

华为乾坤默认将trust区域和DMZ区域添加到信任域中，untrust区域添加到混合域中。同时华为乾坤根据威胁事件判断，将其他区域添加到相应的安全域中（非信任域除外）。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 地址安全域管理”。

步骤3 **可选:** 在“设备安全域管理”区域中单击“创建”，将相应的安全区域添加到非信任域，此处以untrust为例。

如果您需要华为乾坤对威胁事件下发IP黑名单，则请将相应的安全区域添加到非信任域。

图 2-51 创建安全域

步骤4 **可选:** 单击设备卡片右上角的“编辑”，拖动安全区域所在的信任域类型。

您可以根据实际需求，通过拖动的方式调整安全区域所在的信任域类型，以帮助华为乾坤判定威胁事件。

版权所有 © 华为技术有限公司

图 2-52 设置区域标签

步骤5 完成后单击设备卡片右上角的“保存”。

----结束

2.4.7 授权管理

2.4.7.1 黑白名单授权

背景信息

- 天关向华为乾坤提供日志后，华为乾坤将使用自动化分析模型进行分析判定，并根据分析结果自动执行下发IP黑名单操作或向租户发送告警。对于未命中分析模型的事件，则交给业务运营人员处置，比如执行下发IP黑名单操作。只有在租户授予黑名单管理权限后，华为乾坤才可以对此租户的设备自动执行下发IP黑名单操作，业务运营人员也才可以对此租户的设备执行下发IP黑名单操作。

  华为乾坤自动下发的IP黑名单有效期为2天。业务运营人员下发IP黑名单的有效期由其在执行下发操作时设置。
- 天关向华为乾坤提供日志后，华为乾坤将使用自动化分析模型进行分析判定，并根据分析结果自动执行下发域名黑名单。只有在租户授予黑名单管理权限后，华为乾坤才可以对此租户的设备自动执行下发域名黑名单操作。

目前仅一级租户享有黑白名单的授权权限。

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > 授权管理 > 黑白名单授权”。

步骤3 确认已完成**地址安全域管理**后，进行授权。

版权所有 © 华为技术有限公司

图 2-53 黑白名单授权

按照以下步骤完成地址安全域配置，华为乾坤才能正确下发IP黑名单。

1. **配置设备安全域**。

   只有当威胁事件的发出区域位于非信任域时，华为乾坤才会对此威胁事件下发IP黑名单。因此您需要将相应的安全区域添加到非信任域。

2. **配置全局白名单**。

   配置后华为乾坤（包括自动下发、业务运营人员下发）不能将全局白名单中的地址当做IP黑名单下发给天关，保证华为乾坤能够正确下发IP黑名单。

3. **配置不可信内网地址**。

   配置后华为乾坤（包括自动下发、业务运营人员下发）才能将这些内网地址当作IP黑名单下发给天关，保证华为乾坤能够正确下发IP黑名单。

----结束

后续处理

为功能授权后，您可以进行以下操作：

- **管理黑白名单**。
- 按照实际需要，随时“取消授权”或重新“授权”。

2.4.8 配置 Metadata 检测防护规则

前提条件

- Metadata检测功能仅适用于USG6603F-C、USG6606F-C。
- Metadata检测功能仅边界防护与响应服务**专业版**套餐支持。

背景信息

对于内网重要资产，用户可根据实际需要配置Metadata检测防护规则。华为乾坤根据配置的防护网段接收Metadata数据，并基于Metadata数据进行威胁分析，以便更好地保护内网重要资产。

防护网段配置规则如下：

- 已配置防护网段的设备，采集：
  - HTTP协议并且目的IP在防护网段内的Metadata数据。
  - DNS协议并且源IP在防护网段内的Metadata数据。
- 未配置防护网段的设备，不采集Metadata数据。

版权所有 © 华为技术有限公司

操作步骤

步骤1 登录华为乾坤控制台，选择“ ≡ > 我的服务 > 边界防护与响应”。

步骤2 在右上角菜单栏选择“服务配置 > Matedata检测防护规则”。

步骤3 单击“创建”，按页面提示创建Metadata检测防护规则。

图 2-54 创建 Matedata 检测防护规则

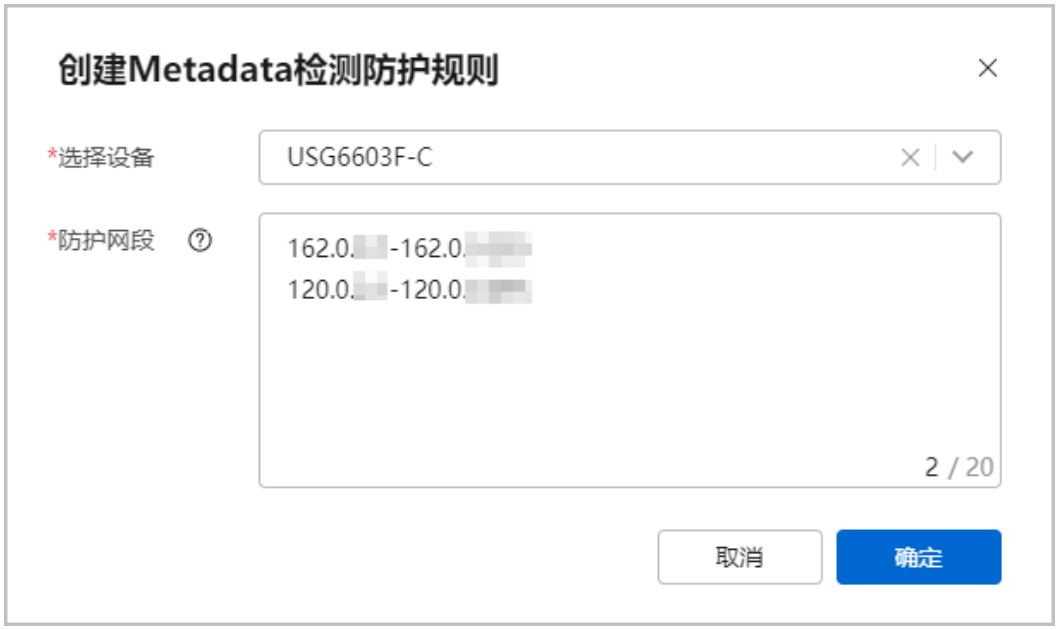


表 2-10 关键参数说明

参数	说明
选择设备	输入设备SN或设备名称进行模糊查询并勾选。
防护网段	• 每行可配置1个防护网段或者范围。 • 行之间用回车分隔。 • 总防护ip数目不超过65535。 示例： 127.0.0.1 127.0.0.1/24 127.0.0.2-127.0.0.10

----结束

后续处理

创建Metadata检测防护规则后，您可以进行以下操作：

- 修改：单击“操作”列的“修改”对现存的Metadata检测防护规则进行修改，仅支持修改防护网段，不支持重新指定设备。

版权所有 © 华为技术有限公司

- 删除：单击“操作”列的“删除”对现存的Metadata检测防护规则进行删除。

2.4.9 MSP 代维指导

2.4.9.1 代维方式介绍

MSP（Managed Service Provider，管理服务供应商），一般是指为普通租户提供网络部署、管理、安全检测、安全防御以及运维等一系列工作的机构。MSP通常具备较为专业的业务管理和维护能力。

当普通租户购买华为乾坤后，发现本身不具备完备的网络建设、业务管理、安全运维能力时，可以委托专业的MSP管理，以降低企业人力和资金的投入。租户委托MSP后，MSP可以对委托业务进行日常状态监控、定期巡检，发现并处理业务运行中存在的异常和问题，同时给出风险评估和事件处置方法。

一个租户帐号可与多个MSP帐号建立委托关系，一个MSP帐号可代维多个租户帐号下的服务。

MSP支持以下两种代维方式：

- 以租户维度进行代维：MSP直接以租户身份进入租户页面进行操作。
- 以服务维度进行代维：MSP对单服务下所有代维租户进行管理和操作。

边界防护与响应服务的代维既支持**按租户**维度代维，也支持**按服务**维度代维。

2.4.9.2 MSP 首页介绍

MSP首页介绍请参见《MSP操作指南》中“**MSP首页介绍**”章节，本手册不再做重复说明。

2.4.9.3 执行代维操作

前提条件

租户已成功委托MSP管理边界防护与响应服务，具体操作请参见《租户操作指南》中“**委托MSP管理**”章节。

背景信息

根据MSP代维服务的不同，MSP代维操作也并不相同。此处仅对MSP代维边界防护与响应服务的特有操作做介绍，其余公共基础操作，例如个性化设置、分权分域、代建租户、工单创建、日志查看等，请参见**MSP基础操作**。

边界防护与响应服务既支持**按租户**维度代维，也支持**按服务**维度代维。如无特殊说明，以下代维操作的介绍均以**按租户**维度代维为例。

搜索和关注租户

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“租户”。

步骤2 在左侧租户列表执行相关操作。

- 搜索租户

  在搜索框输入租户名称，单击左侧 图标或者按回车键直接搜索。

版权所有 © 华为技术有限公司

- 查看租户信息
  选择目标租户，租户列表右侧显示对应的用户信息，如名称、手机号码、邮箱。
- 特别关注
  单击“特别关注”，列表中租户名会以星标展示，如果不需要继续关注，单击“取消关注”即可。
- 打标签
  单击“打标签”，列表中租户名下方会显示标签详情，如果需要删除标签，单击标签后的×号即可。
- 过滤租户
  单击租户列表右上方的 按钮，支持按标签筛选租户。

----结束

进入/退出代维

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“租户”。

步骤2 在左侧租户列表选择代维租户。

步骤3 进入/退出代维。

- 进入代维
  单击“进入代维”，MSP直接以代维租户的身份进入租户页面。MSP代维操作与租户操作相同。
- 退出代维
  代维操作结束后，单击控制台首页“退出代维”，返回MSP帐号界面。

  图 2-55 退出代维

----结束

处置威胁事件

此处以**按服务**维度代维进行介绍。

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“服务”。

步骤2 （可选）在租户列表区域根据租户名或租户标签筛选租户。

步骤3 单击服务卡片或租户列表右侧的“查看详情”。

步骤4 在右上角菜单栏选择“威胁事件”，对威胁事件进行处置。

具体操作请参见**处置威胁事件**。

----结束

管理黑白名单

此处以**按服务**维度代维进行介绍。

版权所有 © 华为技术有限公司

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“服务 > 边界防护与响应”。

步骤2 （可选）在租户列表区域根据租户名或租户标签筛选租户。

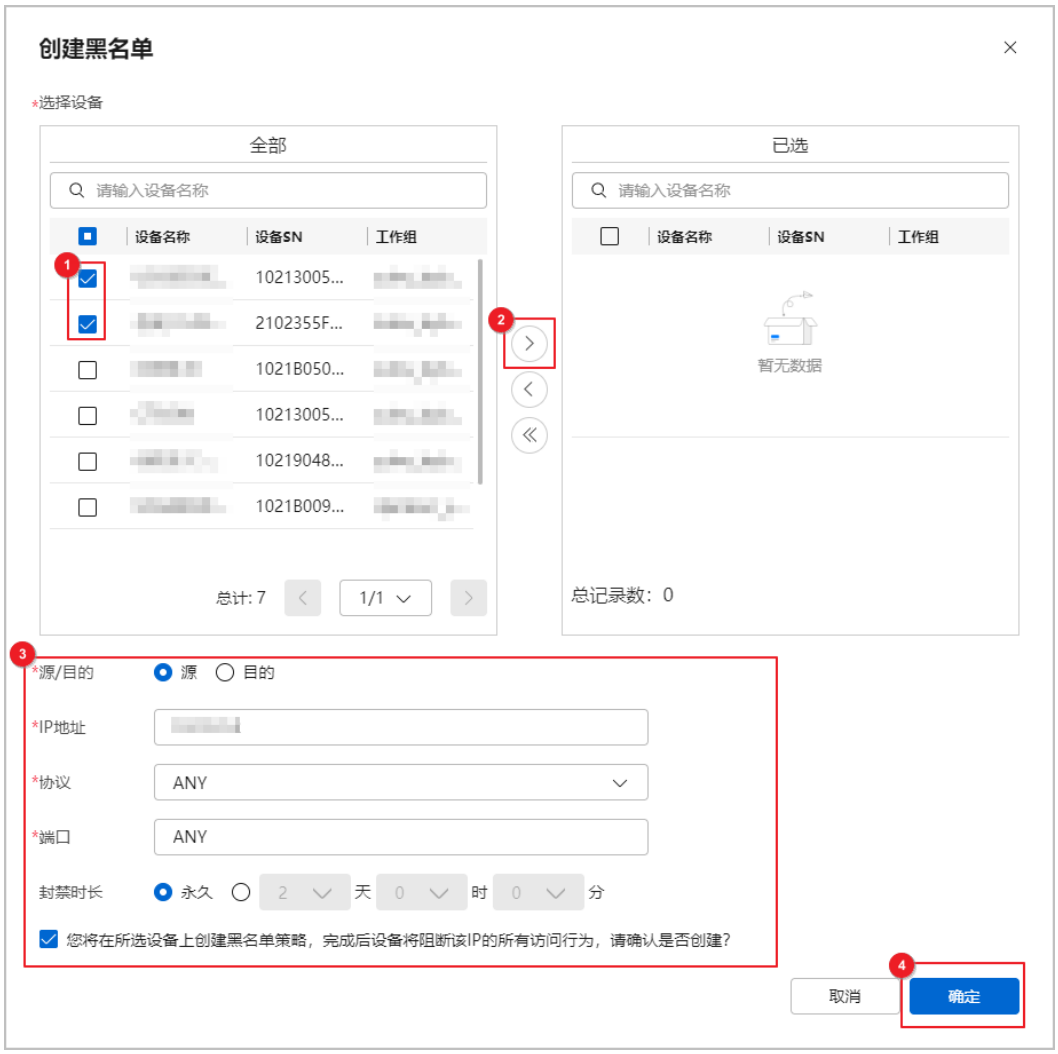
步骤3 单击服务卡片或租户列表右侧的“查看详情”。

步骤4 在右上角菜单栏选择“黑白名单”。

步骤5 此处以批量下发IP黑名单为例。

选择“黑名单 > IP黑名单”，单击“创建”，填写相关信息后，将IP黑名单批量部署到指定租户的指定设备。

图 2-56 批量下发 IP 黑名单



----结束

查看安全报表

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“租户”。

步骤2 在左侧租户列表选择代维租户。

步骤3 单击“进入代维”，选择“☰ > 我的服务 > 边界防护与响应”。

版权所有 © 华为技术有限公司

步骤4 在右上角菜单栏选择“安全报表”，对安全报表进行查看。

具体操作请参见**查看安全报表**。

----结束

创建自定义报表

MSP可以指定自定义周期生成个体报表，对代维租户进行推送。仅在**按服务**维度代维场景下查看时，MSP才能使用此功能。

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“服务 > 边界防护与响应”。

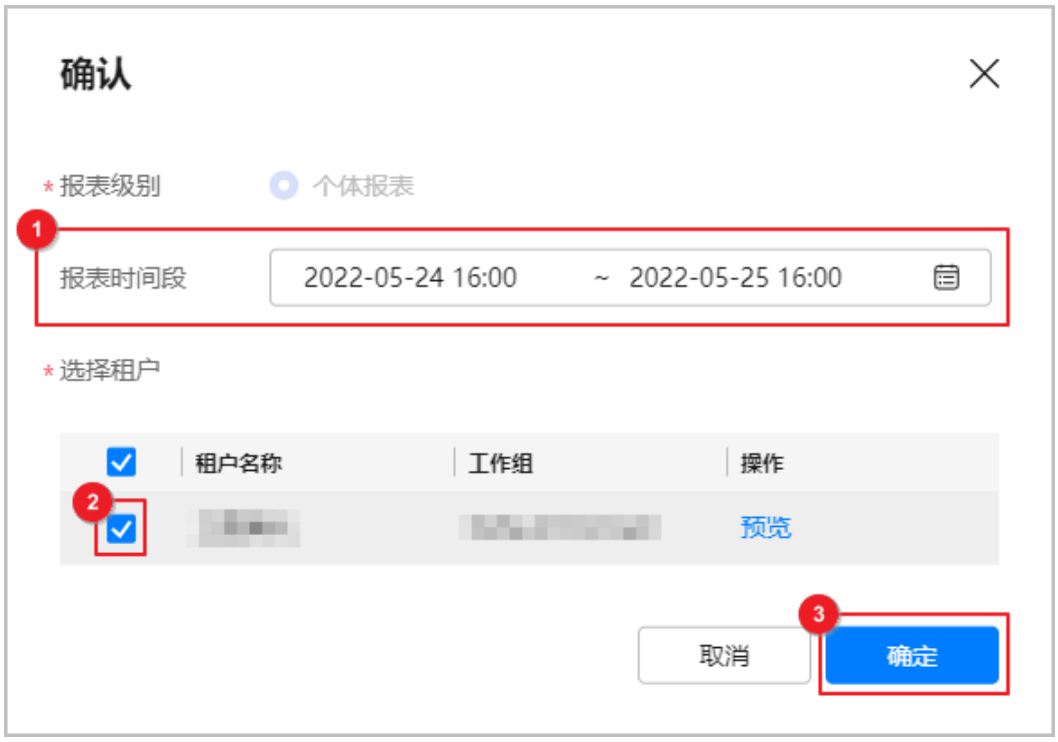
步骤2 （可选）在租户列表区域根据租户名或租户标签筛选租户。

步骤3 单击服务卡片或租户列表右侧的“查看详情”。

步骤4 在右上角菜单栏选择“安全报表”，选择“自定义报表”页签，单击“创建”。

步骤5 填写相关参数，确认并推送。

图 2-57 自定义报表



----结束

查看安全防护大屏

MSP安全防护大屏展示所有代维租户的安全事件的相关数据。

步骤1 以MSP帐号登录华为乾坤控制台，单击左上角菜单栏的“大屏”。

步骤2 **可选:** 单击页面左上角的按钮，根据租户标签筛选租户，自定义显示相关数据。

版权所有 © 华为技术有限公司

步骤3 查看MSP安全防护大屏。

图 2-58 MSP 安全防护大屏

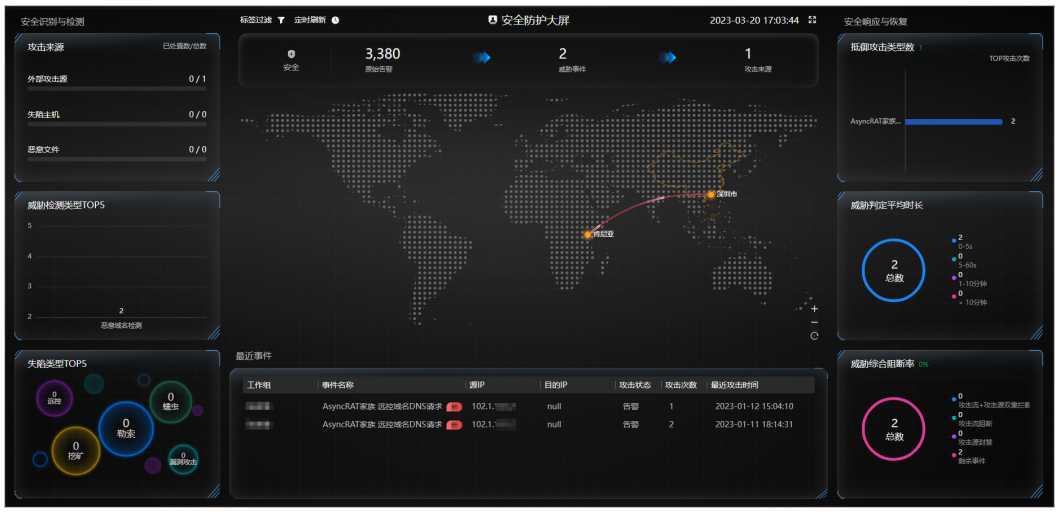


表 2-11 MSP 安全防护大屏模块说明

模块	说明
攻击来源	展示已处置的外部攻击源、失陷主机、恶意文件数量与总数的对比。
威胁检测类型TOP5	展示数量排名TOP5的威胁事件类型。
失陷类型TOP5	展示数量排名TOP5的失陷主机类型。
安全事件	展示各类安全事件数量 ● 原始告警：华为乾坤根据天关提供的威胁日志识别的原始事件。 ● 威胁事件：华为乾坤利用自动化模型分析和业务运营人员人工处置后，将原始事件聚合为威胁事件。 ● 攻击来源：华为乾坤进一步智能处置后，将威胁事件分为外部攻击源、失陷主机和恶意文件三种类型，您可以在此处查看尚未处理的事件数量。
攻击地图	动态呈现最新威胁事件源到端的攻击方向及地域分布。
最近事件	按时间顺序由近到远呈现威胁事件相关信息。
抵御攻击类型数	展示数量排名TOP5已抵御的攻击类型。
威胁判定平均时长	华为乾坤根据天关提供的威胁日志，进行分析后判断是否识别为威胁事件，展示其平均检测时长。

版权所有 © 华为技术有限公司

模块	说明
威胁综合阻断率	展示威胁事件阻断情况。 • 攻击流+攻击源双重拦截：天关的安全防御策略识别到并已拦截和华为乾坤已执行下发黑名单操作的威胁事件。 • 攻击流阻断：天关的安全防御策略识别到并已拦截的威胁事件。 • 攻击源封禁：华为乾坤已执行下发黑名单操作的威胁事件。 • 剩余事件：未处理的威胁事件。

----结束

导出失陷主机报告

仅在**按服务**维度代维场景下查看时，MSP才能使用此功能。

步骤1 以MSP帐号登录华为乾坤控制台，选择右上角菜单栏的“服务 > 边界防护与响应”。

步骤2 （可选）在租户列表区域根据租户名或租户标签筛选租户。

步骤3 单击服务卡片或租户列表右侧的“查看详情”。

步骤4 在右上角菜单栏选择“威胁事件”，在失陷主机卡片的右上角单击“查看更多”。

步骤5 单击“导出”，按提示导出研判分析报告。

----结束

2.4.10 更多操作

2.4.10.1 租户基础操作

表 2-12 租户基础操作

操作任务	使用场景	操作入口	详细参考链接
委托MSP管理	当您需要委托MSP（服务渠道商）进行日常运维时，需要执行委托操作。当前仅边界防护与响应服务支持MSP委托。	单击右上角个人帐号，选择“委托”。	委托MSP管理
创建工单	当您在使用服务时，一旦发现问题即可创建问题工单。随后，华为工程师根据工单记录进行问题分析和处理。	单击右上角个人帐号，选择“我的工单”。	工单管理
新建用户	华为乾坤支持分权分域管理。您可以根据组织结构划分不同的工作组，并为不同的工作组创建用户。	单击右上角个人帐号，选择“权限管理”。	创建用户

版权所有 © 华为技术有限公司

操作任务	使用场景	操作入口	详细参考链接
订阅	华为乾坤支持订阅功能。订阅之后，华为乾坤会向订阅接受者发送订阅主题相关的信息。	单击右上角个人帐号，选择“订阅”。	订阅管理
查看日志	日志主要包括操作日志和安全日志。当您需要了解相关信息的时候，可以查看。	单击右上角个人帐号，选择“日志”。	日志查看

2.4.10.2 MSP 基础操作

表 2-13 MSP 基础操作

操作任务	使用场景	操作入口	详细参考链接
登录控制台	当您使用服务时，需要使用MSP帐号登录控制台。	访问华为乾坤商城，单击右上角“登录”进行登录。	注册并登录控制台
个人中心设置	当您需要对个人帐号信息进行个性化设置，包括用户名、密码、邮箱、头像等修改。	单击控制台右上角个人帐号，选择“个人中心”。	个人中心设置
分权分域	支持分权分域管理。您可以根据组织结构划分不同的工作组，并为不同的工作组创建MSP帐号。	单击控制台右上角个人帐号，选择“权限管理”。	帐号管理
管理租户	支持MSP创建、查询、修改、导出租户信息。	单击控制台右上角“租户”。	租户管理
创建工单	当您使用服务时，一旦发现问题可立即创建工单。随后，华为乾坤工程师根据工单记录进行问题分析和处理。	单击控制台右上角个人帐号，选择“我的工单”。	工单管理
查看日志	日志主要包括操作日志和安全日志。	单击控制台右上角个人帐号，选择“日志”。	日志查看
查看公告	当您需要了解服务最新消息，如产品公告、安全公告、升级公告等，可以查看。	单击控制台右上角个人帐号，选择“公告”。	查看公告
套餐管理	当您需要了解代维租户的套餐状态。	单击控制台右上角“运营 > 套餐”。	套餐管理

版权所有 © 华为技术有限公司