云防火墙

快速入门

文档版本 04

发布日期 2024-10-12

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

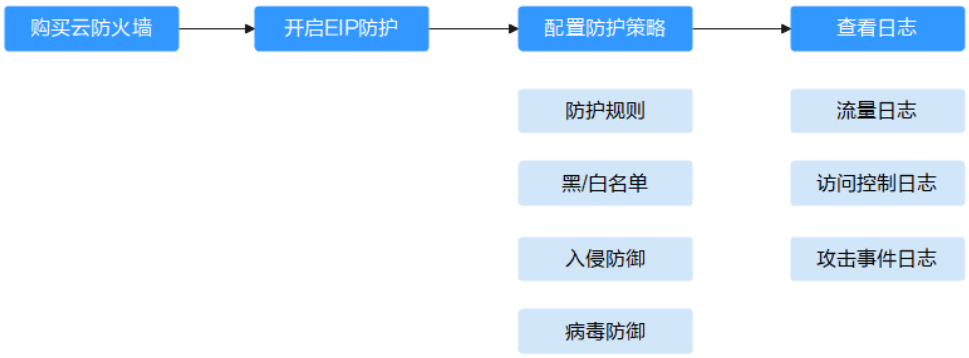
目 录

1 入门指引

云防火墙（Cloud Firewall，CFW）为云上业务提供互联网边界、VPC边界、NAT网关的流量防护。

本文为您介绍防护不同场景的配置流程。

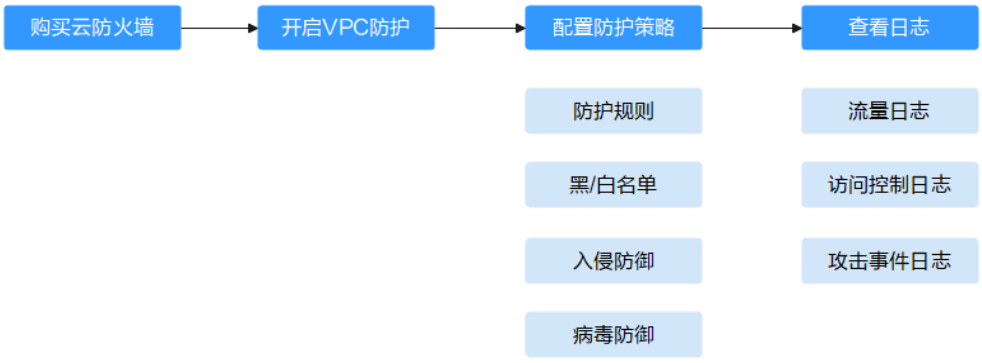
互联网边界流量防护



操作步骤	说明	相关文档
购买云防火墙	购买1个云防火墙实例，防护区域需和云资源所在区域一致。	**购买云防火墙**
开启EIP防护	开启1个或多个弹性公网IP（EIP）的防护。 云防火墙通过对EIP的防护实现互联网边界流量的防护。	**开启EIP防护**

操作步骤	说明	相关文档
配置防护策略	云防火墙默认放行所有流量，您需要配置防护策略实现流量防护。 提供以下防护策略： • 防护规则：按照IP地址、IP地址组、地域、域名等维度设置特定的规则管控流量。 • 黑/白名单：按照IP地址、IP地址组设置特定的规则管控流量，匹配到白名单的流量会直接放行，不再经过其他功能的检测。 • 入侵防御：根据多个IPS规则库拦截网络攻击。 • 病毒防御：通过协议类型拦截病毒文件。	防护规则：**通过添加防护规则拦截/放行流量** 黑/白名单：**通过添加黑白名单拦截/放行流量** 入侵防御：**拦截网络攻击** 病毒防御：**拦截病毒文件**
查看日志	通过日志查看流量的防护效果。	**查看日志**
场景示例： • 通过防护规则精细化管控EIP流量：请参见**配置防护规则放行指定EIP的入方向流量** • 通过入侵防御功能防护常见攻击：请参见**切换入侵防御模式为EIP拦截攻击**		

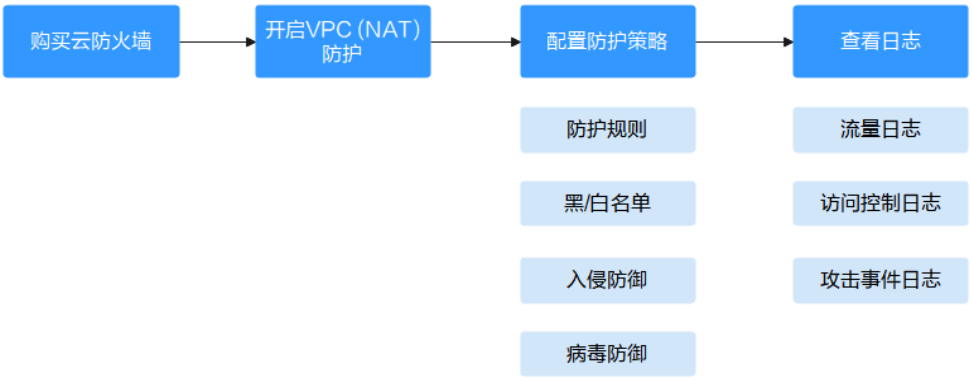
VPC 边界流量防护



操作步骤	说明	相关文档
购买云防火墙	购买1个云防火墙实例，防护区域需和云资源所在区域一致。	**购买云防火墙**
开启VPC防护	开启2个或以上虚拟私有云（VPC）的防护。 云防火墙通过对VPC的防护实现VPC边界流量的防护。	**开启VPC边界流量防护**

操作步骤	说明	相关文档
配置防护策略	云防火墙默认放行所有流量，您需要配置防护策略实现流量防护。 提供以下防护策略： • 防护规则：按照IP地址、IP地址组、地域、域名等维度设置特定的规则管控流量。 • 黑/白名单：按照IP地址、IP地址组设置特定的规则管控流量，匹配到白名单的流量会直接放行，不再经过其他功能的检测。 • 入侵防御：根据多个IPS规则库拦截网络攻击。 • 病毒防御：通过协议类型拦截病毒文件。	防护规则：**通过添加防护规则拦截/放行流量** 黑/白名单：**通过添加黑白名单拦截/放行流量** 入侵防御：**拦截网络攻击** 病毒防御：**拦截病毒文件**
查看日志	通过日志查看流量的防护效果。	**查看日志**
场景示例： 通过防护规则精细化管控VPC间流量：请参见**通过配置CFW防护规则实现两个VPC间流量防护**		

NAT 网关流量防护



操作步骤	说明	相关文档
购买云防火墙	购买1个云防火墙实例，防护区域需和云资源所在区域一致。	**购买云防火墙**
开启VPC（NAT）防护	开启2个或以上虚拟私有云（VPC）的防护。 云防火墙通过防护NAT网关所在的VPC，实现对NAT网关流量的防护。	**开启NAT网关流量防护**

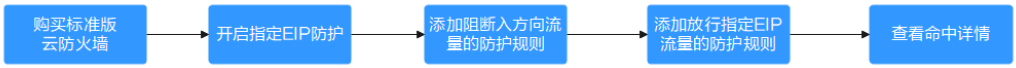
操作步骤	说明	相关文档
配置防护策略	云防火墙默认放行所有流量，您需要配置防护策略实现流量防护。 提供以下防护策略： • 防护规则：按照IP地址、IP地址组、地域、域名等维度设置特定的规则管控流量。 • 黑/白名单：按照IP地址、IP地址组设置特定的规则管控流量，匹配到白名单的流量会直接放行，不再经过其他功能的检测。 • 入侵防御：根据多个IPS规则库拦截网络攻击。 • 病毒防御：通过协议类型拦截病毒文件。	防护规则：**通过添加防护规则拦截/放行流量** 黑/白名单：**通过添加黑白名单拦截/放行流量** 入侵防御：**拦截网络攻击** 病毒防御：**拦截病毒文件**
查看日志	通过日志查看流量的防护效果。	**查看日志**
场景示例： 通过防护规则精细化管控NAT网关流量：请参见**通过配置CFW防护规则实现SNAT流量防护**		

2 配置防护规则放行指定 EIP 的入方向流量

配置合适的防护规则能有效地帮助您对云上资产与互联网之间的流量进行精细化管控，防止内部威胁扩散，增加安全战略纵深。

本文指导您通过标准版防火墙配置防护规则实现放行指定弹性公网IP（EIP）的入方向流量，帮助您快速精细化管控云上资产的流量。

操作流程



操作步骤	说明
准备工作	注册华为账号、开通华为云，为账户充值、赋予CFW权限。
步骤一：购买标准版云防火墙	购买CFW，选择防护的区域、版本规格（本文以标准版为例）等信息。
步骤二：开启指定EIP的防护	在CFW上对需要防护的EIP开启防护，使流量经过防火墙。
步骤三：添加防护规则——阻断所有入方向流量	配置一条阻断所有入方向流量的防护规则，并将它优先级置于最低。
步骤四：添加防护规则——放行访问指定EIP的入方向流量	配置一条放行指定EIP（本文以xx.xx.xx.1为例）入方向流量的防护规则，并将它优先级设置在阻断规则之上。
步骤五：通过访问控制日志查看命中详情	查看防护规则是否生效。

准备工作

1. 在购买云防火墙之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**、**实名认证**。
   如果您已开通华为云并进行实名认证，请忽略此步骤。

2. 请保证账户有足够的资金，防止购买云防火墙失败。具体操作请参见**账户充值**。
3. 请确保已为账号赋予相关CFW权限。具体操作请参见**创建用户组并授权使用CFW**。

表 2-1 CFW 系统角色

角色名称	描述	类别	依赖关系
CFW FullAccess	云防火墙服务的所有权限。	系统策略	无
CFW ReadOnlyAccess	云防火墙服务的只读权限。	系统策略	无

步骤一：购买标准版云防火墙

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

本文以购买标准版云防火墙为例进行介绍，如需购买其他版本请参见**购买云防火墙**，各版本功能差异请参见**服务版本差异**。

1. **登录管理控制台**，在左侧导航树中，单击左上方的 ☰，选择“安全与合规 > 云防火墙”。
2. 单击“购买云防火墙”，进入“购买云防火墙”页面，配置参数。

   本示例中仅解释必要参数，其他参数根据具体情况选择。

参数	示例	参数说明
区域	华北-北京四	选择资源（EIP）所在的区域。 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域?** 。
版本规格	标准版。	选择服务版本。

3. 确认信息无误后，单击“立即购买”。
4. 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。
5. 在“付款”页面，选择付款方式进行付款。

步骤二：开启指定 EIP 的防护

1. 在左侧导航栏中，选择“资产管理 > 弹性公网IP管理”，进入“弹性公网IP管理”页面。
2. 开启弹性公网IP。

- 开启单个弹性公网IP：在所在行的“操作”列中，单击“开启防护”。
- 开启多个弹性公网IP：勾选需要开启防护的弹性公网IP，单击表格上方的“开启防护”。

须知

- 弹性公网IP防护目前不支持IPv6防护。
- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

3. 在弹出的界面确认信息无误后，单击“绑定并开启防护”，可查看操作行的“防护状态”列显示“防护中”。

说明

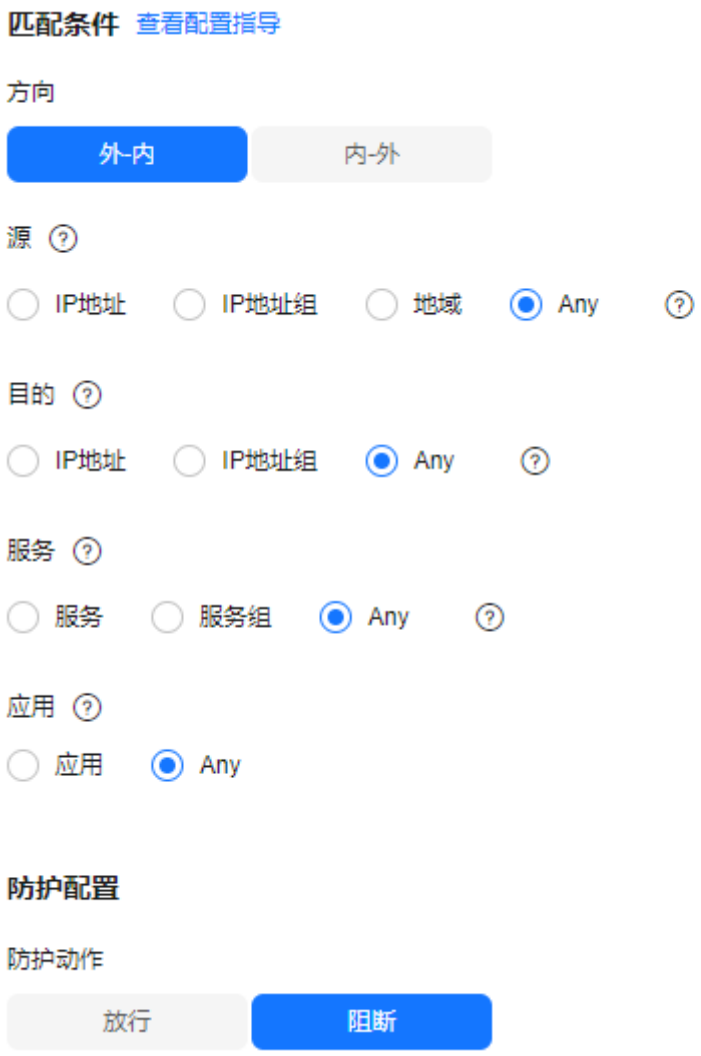
EIP开启防护后，访问控制策略默认动作为“放行”。

步骤三：添加防护规则——阻断所有入方向流量

1. 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面。
2. 单击“添加”，在弹出的“添加防护规则”中，填写参数。

   本示例中仅解释必要参数，其他参数配置请参见**通过添加防护规则拦截/放行流量**。

图 2-1 拦截所有流量



参数	示例	参数说明
方向	外-内（表示入方向流量）	选择流量的方向： • 外-内：互联网访问云上资产（EIP）。 • 内-外：云上资产（EIP）访问互联网。
源	Any	设置访问流量中发送数据的地址参数。
目的	Any	设置访问流量中的接收数据的地址参数。
服务	Any	设置协议类型、源端口和目的端口。
应用	Any	设置针对应用层协议的防护策略。

参数	示例	参数说明
动作	阻断	设置流量经过防火墙时的处理动作。 ● 放行：防火墙允许此流量转发。 ● 阻断：防火墙禁止此流量转发。
策略优先级	置顶（已设置过防护规则时，需选择“移动至选中规则后”，将本条规则设置为最低优先级）	设置该策略的优先级： ● 置顶：表示将该策略的优先级设置为最高。 ● 移动至选中规则后：表示将该策略优先级设置到某一规则后。

3. 单击“确认”，完成配置防护规则。

步骤四：添加防护规则——放行访问指定 EIP 的入方向流量

1. 在“访问策略管理”页面的“防护规则”页签中，单击“添加”，在弹出的“添加防护规则”中，填写以下参数。

图 2-2 放行指定 IP

参数	示例	参数说明
方向	外-内（表示入方向流量）	选择流量的方向： ● 外-内：互联网访问云上资产（EIP）。 ● 内-外：云上资产（EIP）访问互联网。

参数	示例	参数说明
源	Any	设置访问流量中发送数据的地址参数。
目的	xx.xx.xx.1	设置访问流量中的接收数据的地址参数。
服务	Any	设置协议类型、源端口和目的端口。
应用	Any	设置针对应用层协议的防护策略。
动作	放行	设置流量经过防火墙时的处理动作。 ● 放行：防火墙允许此流量转发。 ● 阻断：防火墙禁止此流量转发。
策略优先级	置顶（至少需高于上一条阻断规则）	设置该策略的优先级： ● 置顶：表示将该策略的优先级设置为最高。 ● 移动至选中规则后：表示将该策略优先级设置到某一规则后。

2. 单击“确认”，完成配置防护规则。

步骤五：通过访问控制日志查看命中详情

在左侧导航栏中，选择“日志审计 > 日志查询”。默认进入“攻击事件日志”页面，选择“访问控制日志”页签。

访问控制日志满足以下记录时，证明规则已生效：

- “目的IP”列是放行的EIP（例如本文中设置的xx.xx.xx.1）：对应的“响应动作”是“放行”。
- “目的IP”列是其余IP地址：对应的“响应动作”是“阻断”。

相关信息

- 关于添加防护规则的详细参数说明请参见**添加防护规则**。
- 如果希望防护其他账号下的EIP，您需要将其他账号添加至防火墙实例的“多账号管理”中，具体操作请参见**添加组织成员账号**。

3 切换入侵防御模式为 EIP 拦截攻击

CFW提供入侵防御功能，结合多年攻防积累的经验规则，针对访问流量进行检测与防护，覆盖多种常见的网络攻击，有效保护您的资产。

本文指导您通过标准版防火墙将入侵防御模式切换至“拦截模式-中等”实现弹性公网IP（EIP）的防护，帮助您灵活防护云上资产。

操作流程

操作步骤	说明
准备工作	注册华为账号、开通华为云，为账户充值、赋予CFW权限。
步骤一：购买标准版云防火墙	购买CFW，选择防护的区域、版本规格（本文以标准版为例）等信息。
步骤二：开启EIP的防护	在CFW上对需要防护的EIP开启防护，使流量经过防火墙。
步骤三：将入侵防御模式设置为观察模式	“观察模式”下，防火墙检测到攻击事件时记录到“攻击事件日志”中，不做拦截，避免出现误拦截造成流量中断。
步骤四：定期通过攻击事件日志查看是否存在误拦截可能	查看攻击事件日志，排查是否有被误判的正常流量，记录对应的“规则ID”。
步骤五：调整拦截的IPS规则并将入侵防御模式设置为拦截模式	调整误判规则的防护动作，将入侵防御模式修改至拦截模式（本文以“拦截模式-中等”为例）。
步骤六：通过攻击事件日志查看防护效果	查看攻击事件日志，确认正常流量是否被放行。

准备工作

1. 在购买云防火墙之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**、**实名认证**。

   如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 请保证账户有足够的资金，防止购买云防火墙失败。具体操作请参见**账户充值**。
3. 请确保已为账号赋予相关CFW权限。具体操作请参见**创建用户组并授权使用CFW**。

表 3-1 CFW 系统角色

角色名称	描述	类别	依赖关系
CFW FullAccess	云防火墙服务的所有权限。	系统策略	无
CFW ReadOnlyAccess	云防火墙服务的只读权限。	系统策略	无

步骤一：购买标准版云防火墙

云防火墙提供了“基础版”、“标准版”、“专业版”供您使用，包括访问控制、入侵防御、流量分析以及日志审计等功能。

本文以购买标准版云防火墙为例进行介绍，如需购买其他版本请参见**购买云防火墙**，各版本功能差异请参见**服务版本差异**。

1. **登录管理控制台**，在左侧导航树中，单击左上方的 ☰，选择“安全与合规 > 云防火墙”。
2. 单击“购买云防火墙”，进入“购买云防火墙”页面，配置参数。

   本示例中仅解释必要参数，其他参数根据具体情况选择。

参数	示例	参数说明
区域	华北-北京四	选择资源（EIP）所在的区域。 购买的云防火墙只能在当前选择的区域使用，如需在其它区域使用，请切换到对应区域进行购买。有关支持购买CFW的区域说明，请参见**云防火墙支持哪些区域?**。
版本规格	标准版。	选择服务版本。

3. 确认信息无误后，单击“立即购买”。
4. 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。
5. 在“付款”页面，选择付款方式进行付款。

步骤二：开启 EIP 的防护

1. 在左侧导航栏中，选择“资产管理 > 弹性公网IP管理”，进入“弹性公网IP管理”页面。
2. 开启弹性公网IP。
   - 开启单个弹性公网IP：在所在行的“操作”列中，单击“开启防护”。
   - 开启多个弹性公网IP：勾选需要开启防护的弹性公网IP，单击表格上方的“开启防护”。

须知

- 弹性公网IP防护目前不支持IPv6防护。
- 一个EIP只能在一个防火墙上开启防护。
- 仅支持当前账号所属企业项目下的弹性公网IP。

3. 在弹出的界面确认信息无误后，单击“绑定并开启防护”，可查看操作行的“防护状态”列显示“防护中”。

说明

EIP开启防护后，访问控制策略默认动作为“放行”。

步骤三：将入侵防御模式设置为观察模式

1. 在左侧导航栏中，选择“攻击防御 > 入侵防御”。
2. 在“防护模式”中，选择“观察模式”。

说明

本文以“观察模式”为例，如果您的业务防护级别较高，您可以切换至“拦截模式”，建议优先选择防护粒度较低（例如“拦截模式-宽松”）的模式，观察一段时间后，更换为防护粒度高的模式。

步骤四：定期通过攻击事件日志查看是否存在误拦截可能

1. 在左侧导航栏中，选择“日志审计 > 日志查询”。
2. 在“攻击事件日志”页面，查看日志记录，根据“方向”、“源IP”、“目的IP”参数判断是否是正常流量，如果是，则记录“规则ID”。

   例如：从外部的xx.xx.xx.82访问内部EIPxx.xx.xx.58是正常业务流量，但被IPS中ID是806310的规则识别为风险，此时开启拦截模式将会拦截本条流量，则此处记录规则ID（806310）。

图 3-1 查看攻击事件日志

步骤五：调整拦截的 IPS 规则并将入侵防御模式设置为拦截模式

1. 在左侧导航栏中，选择“攻击防御 > 入侵防御” 。
2. 单击“基础防御”中的“查看生效中的规则”，进入“基础防御”页面。
3. 筛选出“规则ID”为“806310”的规则，单击“操作”列“观察”，将“当前动作”修改为“观察”。

   图 3-2 修改基础防御动作

4. 返回至“入侵防御”页面，在“防护模式”中，选择“拦截模式-中等”。

步骤六：通过攻击事件日志查看防护效果

1. 在左侧导航栏中，选择“日志审计 > 日志查询”。
2. 在“攻击事件日志”页面，查看日志记录，是否存在正常业务流量被识别为攻击事件，即“响应动作”为“阻断”。

相关信息

- 关于入侵防御的详细参数说明请参见**拦截网络攻击**。
- 如果希望防护其他账号下的EIP，您需要将其他账号添加至防火墙实例的“多账号管理”中，具体操作请参见**添加组织成员账号**。

4 入门实践

当您配置入侵防御和访问控制策略后，可以根据业务场景使用CFW提供的一系列常用实践。

表 4-1 常用实践

实践	描述
仅放行云内资源对指定域名的访问流量	介绍如何快速放行云内资源对某个域名的访问流量，适用于业务仅需要访问指定域名时的场景。
使用CFW防御网络攻击	介绍如何使用CFW防护各类网络攻击，适用为云上业务拦截网络攻击的场景。
VPC间边界防火墙配置	介绍VPC边界防火墙的配置流程，适用于对VPC间流量防护有需求的场景。
等保二级解决方案	该解决方案能帮您快速在华为云上搭建等保二级合规安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。
等保合规安全解决方案	该解决方案介绍，华为云依托自身安全能力与安全合规生态，为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。