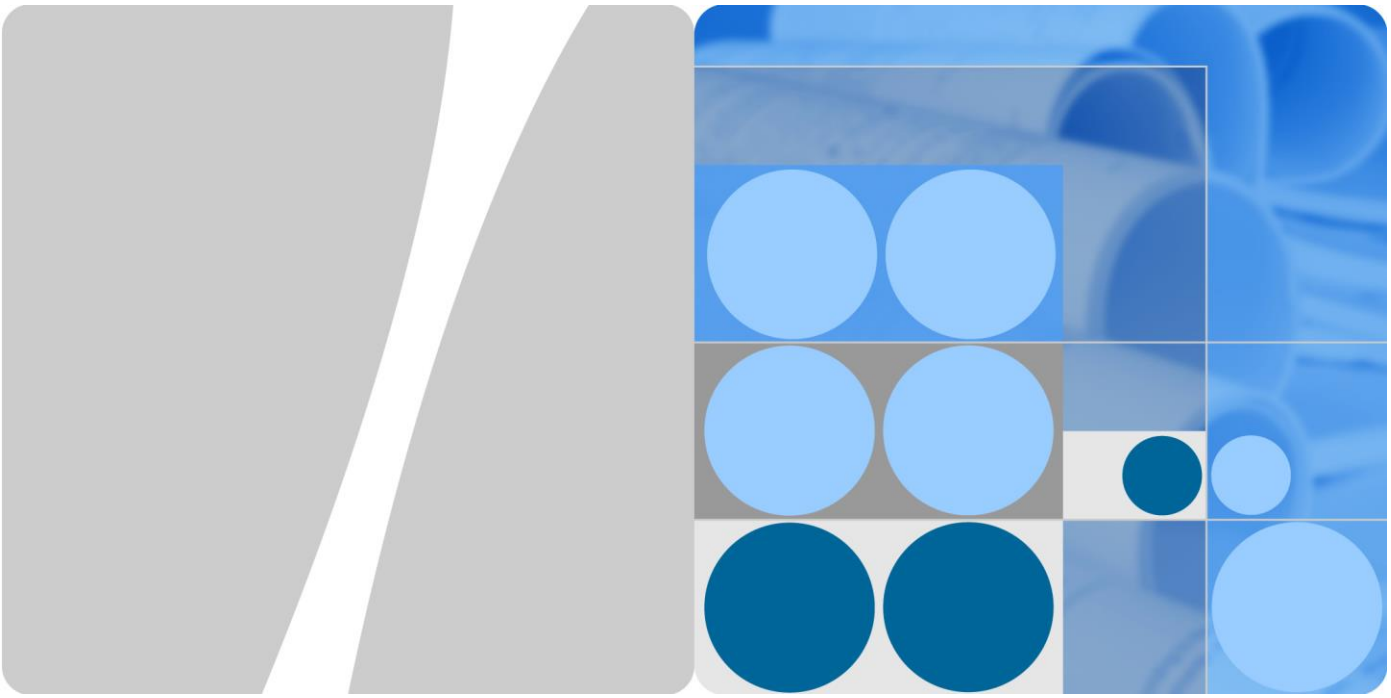


SAP

安全白皮书

文档版本 01

发布日期 2018-03-12

华为技术有限公司

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默示的声明或保证。

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。

华为技术有限公司

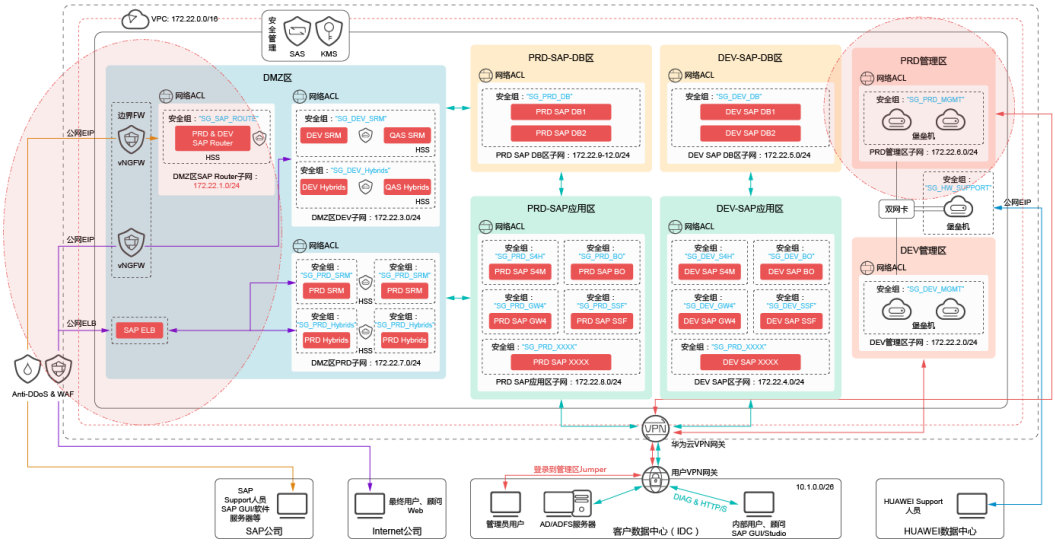
目 录

1 生产环境安全解决方案

1.1 网络隔离与访问控制

SAP 生产环境安全解决方案如图 1-1 所示。

图1-1 生产环境安全解决方案全景图



根据业务特点，参考企业安全实践，建议将云上系统(生产环境、开发测试环境)划分为不同安全级别的多个子区域(以子网为粒度进行隔离)，包括管理区、应用区、SAP DB 区、DMZ 区。

其中 DMZ 区较为特殊，其与 Internet 有交互，并且 DMZ 区为开发测试、生产共用区域。各区域建议采用相应的安全策略，限制区域间以及外部的访问。

- DMZ 区：直接与 Internet 互联，承载公网用户以及 SAP 支持人员对业务系统的访问，安全级别最低，安全风险最高。
- 应用区：部署 SAP 应用，供企业内部(IDC)用户接入使用，以及与 AD 服务器等系统互联，安全级别高于 DMZ 区。

- SAP DB 区：主要部署 SAP DB，仅能被内网应用区、管理区等受限访问，安全级别最高。
- 管理区：部署运维跳板机，作为系统运维人员(企业内部)，管理、运维其它区域云主机及系统的中转区域。

各区域采用相应的安全策略(使用安全组、网络 ACL 实现)，限制区域间以及外网的访问，策略的设置建议遵从“默认失败”、“最小化”原则：针对特定的访问源，仅开放业务必须的*[IP]:[PORT]*。

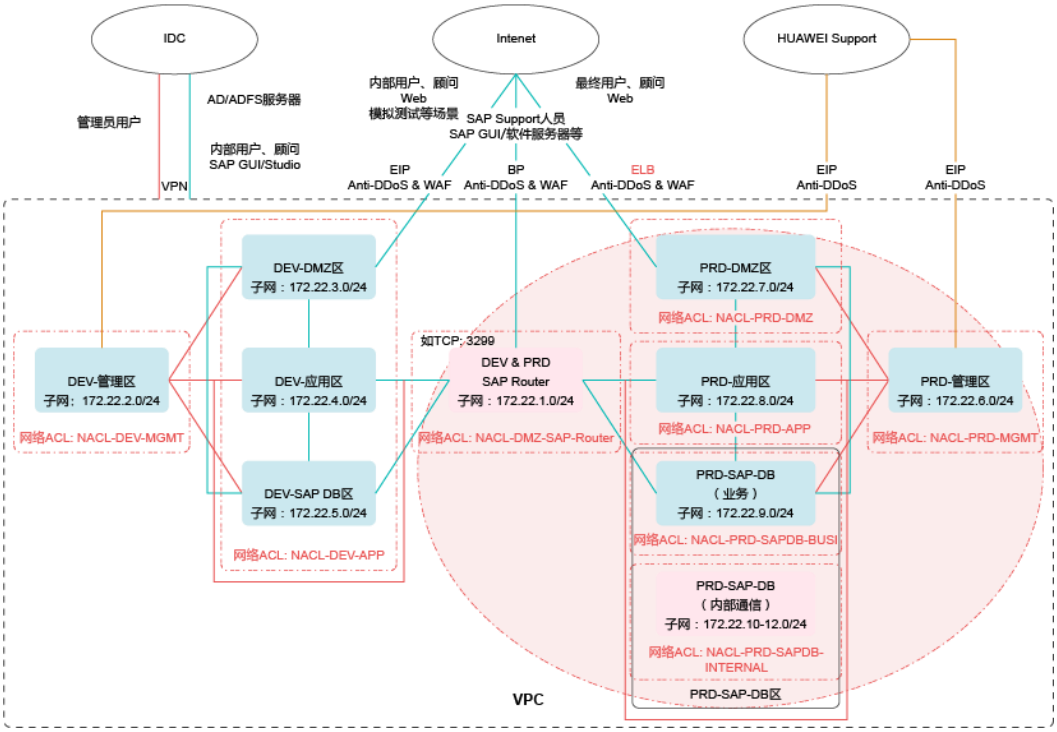
例如，对于企业内部管理员，可访问管理区跳板机远程登录端口，而其他一般用户，或内部系统则无法访问。对于企业内部一般用户，应仅能访问内网应用区的 SAP 业务端口。系统内部各区域间(子网隔离)，应使用网络 ACL 限制默认拒绝所有流量，业务必须流量已白名单方式添加。

本章节将主要描述生产环境内部区域间的访问控制策略，基于上文提到的两个原则，给出网络 ACL 及安全组的设置建议(开发测试环境较为特殊，为了保证 IDC 内用户对该区资源的访问效率以及网络灵活性，相比生产环境，内部采用稍弱的访问控制策略，详见 2 开发测试环境安全解决方案)。

安全策略

如图 1-2 所示，生产环境涉及 8 个子网，建议分别创建相应的网络 ACL 实例：NACL-DMZ-SAP-Router、NACL-PRD-DMZ、NACL-PRD-APP、NACL-PRD-SAPDB-BUSI、NACL-PRD-SAPDB-INTERNAL、NACL-PRD-MGMT。

图1-2 生产环境子网、网络 ACL 分布图



网络 ACL“NACL-DMZ-SAP-Router”，关联生产环境、开发测试环境公用的 DEV&PRD-SAP-Router 子网。通过策略限制，出方向限制可由 SAP-Router 访问生产环境 SAP 应用区、SAP-DB 区指定的业务端口，入方向限制可由管理区跳板机访问子网内服务器的管理端口(22 等)。

说明
本节中提到的 IP 地址及端口号仅为示例，如有其它管理端口，可根据实际情况增加策略。本节仅涉及生产环境内部策略。

表1-1 网络 ACL“NACL-DMZ-SAP-Router”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 PRD-应用区	172.22.8.0/24	TCP	234	允许	允许 SAP-Router 服务器访问 PRD-应用区域内服务器 234 业务端口。
对 PRD-SAP-DB 区	172.22.9.0/24	TCP	345	允许	允许 SAP-Router 服务器访问 PRD-SAP-DB 区域内服务器 345 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表1-2 网络 ACL“NACL-DMZ-SAP-Router”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 PRD-管理区	172.22.6.0/24	TCP	22	允许	允许生产环境管理区跳板机访问本区域内服务器 SSH 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

网络 ACL“NACL-PRD-MGMT”，关联生产环境 PRD-管理子网，出方向通过策略限制可由管理区跳板机访问生产环境其它区域服务器的管理端口(22 等)，并拒绝由其它区域发起的对管理区跳板机的连接。

表1-3 网络 ACL“NACL-PRD-MGMT”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 PRD-DMZ 区	172.22.7.0/24	TCP	22	允许	允许生产环境管理区跳板机访问 PRD-DMZ 区服务器 SSH 端口。
对 PRD-应用区	172.22.8.0/24	TCP	22	允许	允许生产环境管理区跳板机访问 PRD-应用区服务器 SSH 端口。
对 PRD-SAP-DB 区	172.22.9.0/24	TCP	22	允许	允许生产环境管理区跳板机访问 PRD-SAP-DB 区服务器 SSH 端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	22	允许	允许生产环境管理区跳板机访问 DEV&PRD-SAP-Router 服务器 SSH 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-4 网络 ACL“NACL-PRD-MGMT”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
					经前置规则处理的数据流。

网络 ACL“NACL-PRD-DMZ”，关联生产环境 PRD-DMZ 区子网，入方向通过策略限制可由管理区跳板机访问区域内服务器的管理端口(22 等)，出方向限制可由本子网访问 PRD-应用区以及 PRD-SAP-DB 区必要的业务端口。

表1-5 网络 ACL“NACL-PRD-DMZ”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 PRD-应用区	172.22.8.0/24	TCP	8080	允许	允许生产环境 DMZ 区主机访问 PRD-应用区服务器 8080 业务端口。
对 PRD-应用区	172.22.8.0/24	TCP	8443	允许	允许生产环境 DMZ 区主机访问 PRD-应用区服务器 8443 业务端口。
对 PRD-SAP-DB 区	172.22.9.0/24	TCP	345	允许	允许生产环境 DMZ 区主机访问 PRD-SAP-DB 区服务器 345 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-6 网络 ACL“NACL-PRD-DMZ”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 PRD-管理区	172.22.6.0/24	TCP	22	允许	允许生产环境管理区跳板机访问本区域内服务器 SSH 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL“NACL-PRD-APP”，关联生产环境 PRD-应用区子网，入方向通过策略限制可由管理区跳板机访问区域内服务器的管理端口(22 等)，限制可由 SAP-Router、PRD-DMZ 区访问本子网内服务器的业务端口；出方向限制可由本子网访问 PRD-SAP-DB 区必要的业务端口。

表1-7 网络 ACL“NACL-PRD-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 PRD-SAP-DB 区	172.22.9.0/24	TCP	345	允许	允许生产环境应用区主机访问 PRD-SAP-DB 区服务器 345 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-8 网络 ACL“NACL-PRD-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 PRD-管理区	172.22.6.0/24	TCP	22	允许	允许生产环境管理区跳板机访问本区域内服务器 SSH 端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	234	允许	允许 SAP-Router 服务器访问本 PRD-应用区域内服务器 234 业务端口。
对 PRD-DMZ 区	172.22.7.0/24	TCP	8080	允许	允许生产环境 DMZ 区主机访问 PRD-应用区服务器 8080 业务端口。
对 PRD-DMZ 区	172.22.7.0/24	TCP	8443	允许	允许生产环境 DMZ 区

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
					主机访问 PRD-应用区服务器 8443 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL“NACL-PRD-SAPDB-BUSI”，关联生产环境 PRD-SAP-DB 区业务子网(172.22.9.0/24)，入方向通过策略限制可由管理区跳板机访问区域内服务器的管理端口(22 等)，限制可由 SAP-Router、PRD-DMZ 区、PRD-应用区访问本子网内服务器的业务端口。

表1-9 网络 ACL“NACL-PRD-SAPDB-BUSI”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-10 网络 ACL“NACL-PRD-SAPDB-BUSI”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 PRD-管理区	172.22.6.0/24	TCP	22	允许	允许生产环境管理区跳板机访问本区域内服务器 SSH 端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	345	允许	允许 SAP-Router 服务器访问 PRD-SAP-DB 区服务器 345 业务端口。
对 PRD-DMZ 区	172.22.7.0/24	TCP	345	允许	允许生产环境 DMZ 区主机访问 PRD-SAP-DB 区服务器 345 业务端口。
对 PRD-应用区	172.22.8.0/24	TCP	345	允许	允许生产环境应用区主机访问 PRD-SAP-DB 区服务器 345 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
					则处理的数据流。

网络 ACL“NACL-PRD-SAPDB-INTERNAL”，关联生产环境 PRD-SAP-DB 区内部通信子网(172.22.10-12.0/24)，内部通信子网仅供涉及的子网内部通信，需通过网络 ACL 拒绝所有入站与出站流量。

表1-11 网络 ACL“NACL-PRD-SAPDB- INTERNAL”出方向

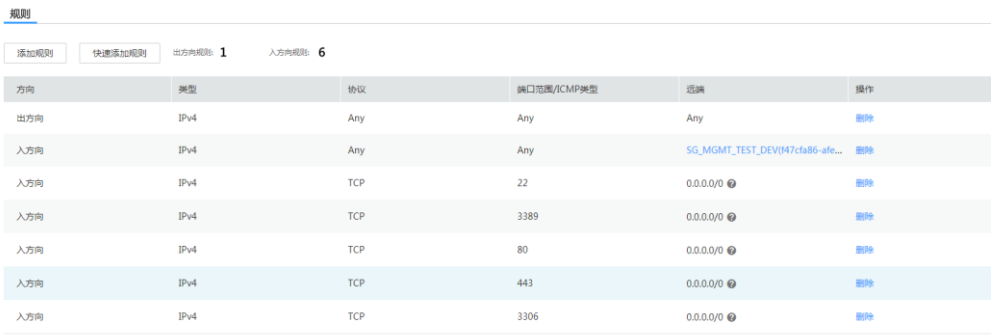
规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-12 网络 ACL“NACL-PRD-SAPDB- INTERNAL”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

安全组，如 SG_PRD_MGMT、SG_PRD_DB 等(与公网无交互)，关联生产环境中相应子网中的云服务器器，需严格按照最小化的原则控云服务器机对外开放的端口范围，可参考以下图 1-3(具体端口请根据实际情况设置)。对 IP 的访问控制策略，通过网络 ACL 实现。其它开发测试环境与公网无交互的安全组(详见图 1-1)，可参考实施。

图1-3 安全组策略示例



安全组，如 SG_SAP_ROUTER(与公网有交互)，关联生产环境中相应子网中的云服务器，需严格按照最小化的原则控制云服务器对外开放的端口范围以及源 IP 范围，如公网 IP 较为固定，可参考以下图 1-4(具体端口请根据实际情况设置)。

图1-4 安全组策略示例

如公网 IP 不固定的场景，可根据业务需要(如模拟测试，技术支持)，临时放通特定公网源 IP，相应事务完成后删除策略。

安全组，如 SG_PRD_SRM、SG_PRD_Hybrids(与公网有交互)，业务端口需要对全网开放，可参考以下图 1-5(具体端口请根据实际情况设置)。其中对 22/3389 等管理端口的源 IP 控制，将由网络 ACL 实现，控制只能由管理区跳板机访问。80 等业务端口将对 Internet 全网开放，不做源 IP 访问控制，建议采用合适的安全产品进行防护，详见 1.2.1 业务边界。

图1-5 安全组策略示例

1.2 网络边界安全

针对 DMZ 区、内网应用区、管理区，由于能够被外部访问，建议采取相应的边界防护措施。

1.2.1 业务边界

根据业务特点，由于生产环境需对公网提供服务，同时也需要与其它 IDC 进行互联，需建立与企业内网(IDC)互联的 VPN 通道，同时需要设置云上与云下以及云上与互联网之间的访问控制策略。

VPN

由于企业内部使用，多为静态连接需求，综合考虑安全性与时延，推荐的优先级为：专线(DC)>VPN(IPSec)>SSL VPN。

说明
华为 VPN 云服务当前仅提供专线和 IPSec VPN 形式，暂不支持 SSL VPN，如需使用 SSL VPN 可选用第三方镜像产品自行部署。

安全策略

由于开发环境同时需要与企业内部通信，还需提供互联网的业务访问，综合考虑通过网络 ACL 进行相应的访问控制策略。

网络 ACL “NACL-DMZ-SAP-Router”关联生产环境相应子网，需严格控制互联网访问的入方向策略，限制特定外网网段能够访问特定的*[IP]:[PORT]*。

说明
本节中提到的 IP 地址及端口号仅为示例，如公网 IP 不固定的场景，可根据业务需要(如技术支持)，临时放通特定源 IP，相应事务完成后删除策略。如有其它业务流，可根据实际情况增加策略。

表1-13 网络 ACL“NACL-DMZ-SAP-Router” 出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表1-14 网络 ACL“NACL-DMZ-SAP-Router”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 SAP 技术支持人员，SAP GU/软件服务器 I 等	123.123.123.0/24	TCP	3299	允许	允许互联网 SAP 技术支持人员(特定源 IP)，SAP GUI/软件服务器等访问开发测试环境中的 DEV&PRD-SAP-Router，进而访问后端业务。

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL “NACL-PRD-DMZ”关联生产环境相应子网，需严格控制互联网/IDC 访问的入方向策略，限制外部网络仅能访问开发测试环境特定的*[IP]:[PORT]*。

表1-15 网络 ACL“NACL-PRD-DMZ”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 AD/ADFS 服务器	IDC-AD/ADFS 网络	TCP	AD/ADF 端口	允许	允许与 IDC 内部 AD/ADFS 服务器进行对接。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-16 网络 ACL“NACL-PRD-DMZ”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 Internet 用户	0.0.0.0/0	TCP	80	允许	允许互联网用户、IDC 内部用户，访问生产环境中的 WEB 服务。
对 Internet 用户	0.0.0.0/0	TCP	443	允许	允许互联网用户、IDC 内部用户，访问生产环境中的 WEB 服务。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL “NACL-PRD-APP”关联生产环境相应子网，需严格控制 IDC 访问的入方向策略，限制特定 IDC 网络仅能访问开发测试环境特定的*[IP]:[PORT]*，出方向策略同上。

表1-17 网络 ACL“NACL-PRD-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对	IDC-	TCP	AD/ADF	允许	允许与 IDC 内部

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
AD/ADFS 服务器	AD/ADFS 网络		端口		AD/ADFS 服务器进行对接。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-18 网络 ACL“NACL-PRD-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 IDC 内部用户、顾问。	客户数据中心某子网-b	TCP	8080	允许	允许客户数据中心某子网-b 中的内部用户、顾问，访问生产环境中的应用区 8080 业务端口。
对 IDC 内部用户、顾问。	客户数据中心某子网-b	TCP	8443	允许	允许客户数据中心某子网-b 中的内部用户、顾问，访问生产环境中的应用区 8443 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

对于网络 ACL “NACL-PRD-SAPDB-BUSI/INTERNEL”，由于无与外部网络交互需求，只需根据 1.1 网络隔离与访问控制设置内部访问控制策略即可。

安全组策略请见 2.1 网络隔离与访问控制中相关内容。

安全服务

- Anti-DDoS

根据业务特点，由于生产环境有公网访问需求，需要针对 SAP Router、SRM、Hybrids 服务器部署 Anti-DDoS 防护，推荐使用华为云 Anti-DDoS 流量清洗服务，对相应的 EIP 进行 DDoS 防护。

- Web 应用防火墙-WAF

根据业务特点，由于生产环境需向互联网提供 Web 应用服务，需要部署 Web 应用防火墙，应对诸如 OWASP TOP10 Web 攻击，推荐华为云 Web 应用防火墙服务，创建 WAF 实例防护相应 EIP/ELB。

- 虚拟下一代防火墙-vNGFW

根据业务特点，SAP Router 会提供给第三方使用并接入内部系统，开发测试环境 SRM/Hybrids 会对外方开放用于模拟测试。以上入口均面临网络攻击入侵风险，建议部署虚拟下一代防火墙对后端进行防护。

1.2.2 运维边界

由于管理区无公网访问需求，参考企业安全实践，仅需设置与 IDC 间的访问控制策略。

安全策略

如图 1-2 所示，网络 ACL“NACL-PRD-MGMT”关联生产环境管理区子网，对于由 IDC 发起的对生产环境的入方向策略(管理员)，可限制能够访问管理区主机的 22/3389 等管理端口。

说明
本节中提到的 IP 地址及端口号仅为示例，如有其它管理端口，可根据实际情况增加策略。

表1-19 网络 ACL“NACL-PRD-MGMT”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对管理员	客户数据中心某子网-a	TCP	22	允许	允许客户数据中心某子网-a 中的管理员访问生产环境管理区的 VM。
对管理员	客户数据中心某子网-a	TCP	3389	允许	允许客户数据中心某子网-a 中的管理员访问生产环境管理区的 VM。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表1-20 网络 ACL“NACL-PRD-MGMT”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
1	0.0.0.0/0	ANY	ANY	允许	对于由管理区发起的出方向流量不做限制。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

安全服务

参考企业安全实践，通过堡垒机实现运维/运营人员不接触系统账户密码(各系统部件账号托管在堡垒机系统)，对运维人员通过堡垒机进行的操作范围进行权限控制，限制高危操作权限，并对运维人员操作全流程审计记录，做到事件可监控、可追踪、可回溯。堡垒机以云服务器模式部署于管理区子网中。

1.2.3 与开发测试环境边界

由于测试环境仍属于安全级别较低的区域，安全风险较高，如需与生产环境互联，此边界需要特别关注，采用较严格的访问控制策略：由开发测试环境发起对生产环境的访问，需严格控制(默认失败)，仅能访问生产环境中必要的*[IP]:[PORT]* (最小化)；由生产环境发起的对开发测试环境的访问，可以采用稍弱的访问控制策略。

安全策略

网络 ACL“NACL-PRD-DMZ/APP/SAPDB-BUSI”关联生产环境相应子网，需严格按照最小化的原则控制访问开发测试环境的入方向策略，限制其仅能访问生产环境中特定的*[IP]:[PORT]*；对于由生产环境发起的对开发测试环境的出方向策略，这里可以根据实际情况设置稍弱的访问控制策略。

说明
强的、安全性高的、复杂的访问控制策略，会一定程度增加部署配置及运维成本，可以根据企业自身情况适当减少策略。

与开发测试环境边界的策略主要包括对 DEV-DMZ 区、对 DEV-应用区、对 DEV-DB 区的策略，详细请参考表 1-21、表 1-22、表 1-23、表 1-24、表 1-25 和表 1-26。

说明
本节中提到的 IP 地址及端口号仅为示例，如有其它业务流，可根据实际情况增加策略。本节仅涉及开发测试区与生产环境策略。

表1-21 网络 ACL“NACL-PRD-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 DEV-应用区	172.22.4.0/24	TCP	2433	允许	允许测试环境 DEV-应用区中的 VM 访问生产环境 PRD-应用区中服务器 2433 端口进行软件/代码推送更新。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表1-22 网络 ACL“NACL-PRD-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 DEV-应用区	172.22.8.0/24	TCP	ANY	允许	允许生产环境 PRD-应用区中的 VM 访问 DEV-应用区域中服务器任意 TCP 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站数据流。

表1-23 网络 ACL“NACL-PRD-DMZ”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 DEV-DMZ 区	172.22.3.0/24	TCP	1433	允许	允许测试环境 DMZ 区中的 VM 访问生产环境 PRD-DMZ 区中服务器 1433 端口进行软件/代码推送更新。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表1-24 网络 ACL“NACL-PRD-DMZ”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 DEV-DMZ 区	172.22.4.0/24	TCP	ANY	允许	允许生产环境 PRD-DMZ 区中的 VM 访问 DEV-DMZ 区域中服务器任意 TCP 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站数据流。

表1-25 网络 ACL“NACL-PRD-SAPDB-BUSI”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 DEV-SAP DB	172.22.5.0/24	TCP	3433	允许	允许测试环境 DEV-SAP DB 区中的 VM 访问生产环

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
区					境 PRD-SAP-DB 区中服务器 3433 端口进行软件/代码推送更新。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表1-26 网络 ACL“NACL-PRD-SAPDB-BUSI”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 DEV-SAP DB 区	172.22.5.0/24	TCP	ANY	允许	允许生产环境 PRD-SAP DB 区中的 VM 访问 DEV- SAP DB 区域中服务器任意 TCP 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站数据流。

1.3 安全管理

安全评估

对于 Web 站点及关键主机，建议定期进行安全评估(安全体检服务-专业安全评估)，以及时发现、规避安全风险。

- 服务测试范围包括：
  - 网站类：SQL 注入、XSS 跨站、文件包含、任意文件上传、任意文件下载、Web 弱口令、服务弱口令。
  - 主机类：远程漏洞扫描、弱口令扫描、高危端口识别、高危服务识别、基线检查。
- 华为安全专家团队会对专业机构提交的体检报告进行审核，引导专业机构提高服务质量，给客户更佳的用户体验。
- 提供准确的漏洞信息和对应的修复建议，并可为用户定制整体安全解决方案，帮助用户构筑完善的安全防御机制。

网站监控

- 非法篡改监控(监测网页篡改行为，特别是一些越权篡改、暗链篡改等)。

- 坏链检测（如链接目的页面已经删除或转移;网站搬家导致链接无效，设置静态链接导致原内文章链接地址无法访问等）。
- 脆弱性检测（SQL 注入、XSS 跨站、文件包含、敏感信息泄露、任意文件下载等）。
- 可用性检测（通过全国多地监测和 DNS 解析监测监控网站的可用性）。
- 对外服务开放监测（定期对网站开放服务进行扫描，检测是否开放多余服务）。
- 敏感内容审计（定期对网站内容进行检测，对出现敏感内容页面进行告警）。
- 协同预警（协同技术小组根据最新漏洞与威胁跟踪结果提供预警）。

秘钥管理

业务系统中如有数据加密场景，建议使用华为云 KMS 服务进行密钥管理，以满足安全、合规等要求。

1.4 主机安全

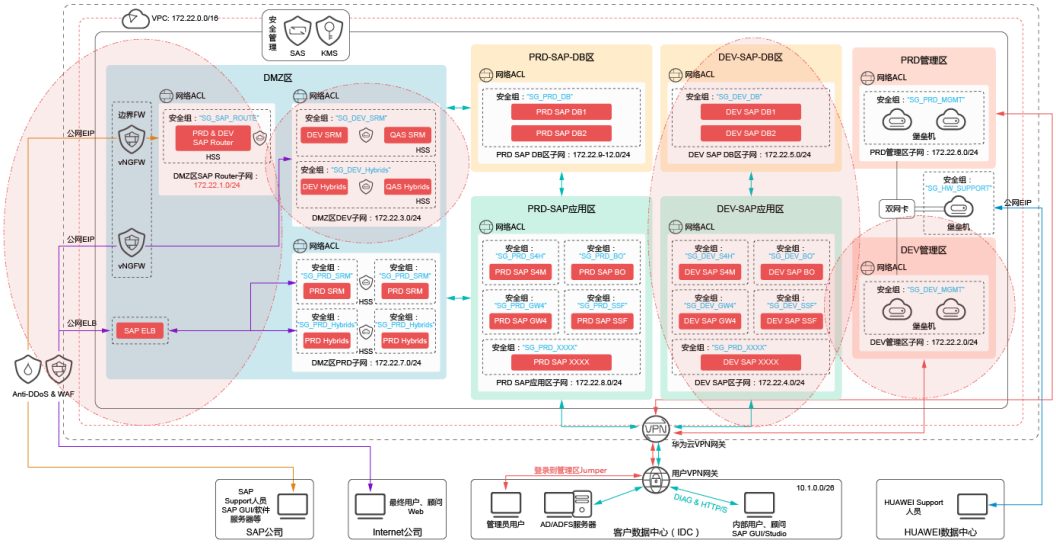
- 与公网有交互的云服务器建议参考华为云主机防暴力破解解决方案进行相应的加固。主要涉及系统加固，以及主机安全产品(HIDS/AV 等)的应用。
- 为了增加业务关键云主机的可靠性，建议(云服务器创建阶段)将同类的关键节点关联到一个云服务器组，将云主机尽量分散到不同的物理主机上(反亲和策略)，提高业务可靠性。比如 ELB 的后端主机、SAP DB 云主机等，可以设置相应的云服务器组。

2 开发测试环境安全解决方案

2.1 网络隔离与访问控制

SAP 生产环境安全解决方案如图 2-1 所示。

图2-1 开发测试环境安全解决方案全景图



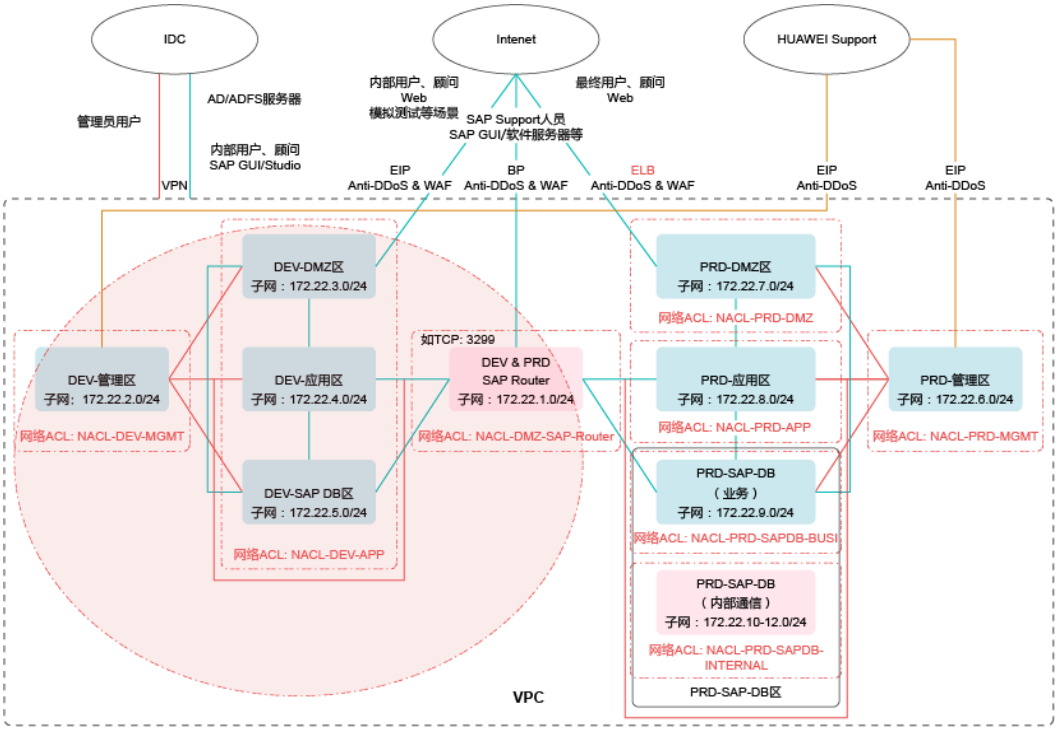
根据业务特点，由于开发测试环境仅供企业内部开发、测试使用，并参考企业安全实践，开发测试环境内部可采用稍弱的网络隔离与访问控制策略，提高网络部署灵活性。

但是，测试环境仍属于安全级别较低的区域，安全风险较高，如需与生产环境互联，此边界需要特别关注，采用较严格的访问控制策略(详见 2.2.1 与生产环境边界)。

另外，开发测试环境中所有云服务器对外开放的端口范围由安全组控制，遵从最小化原则。安全组不做源 IP 控制，由网络 ACL 进行控制。

SAP 开发测试环境子网如图 2-2 所示。

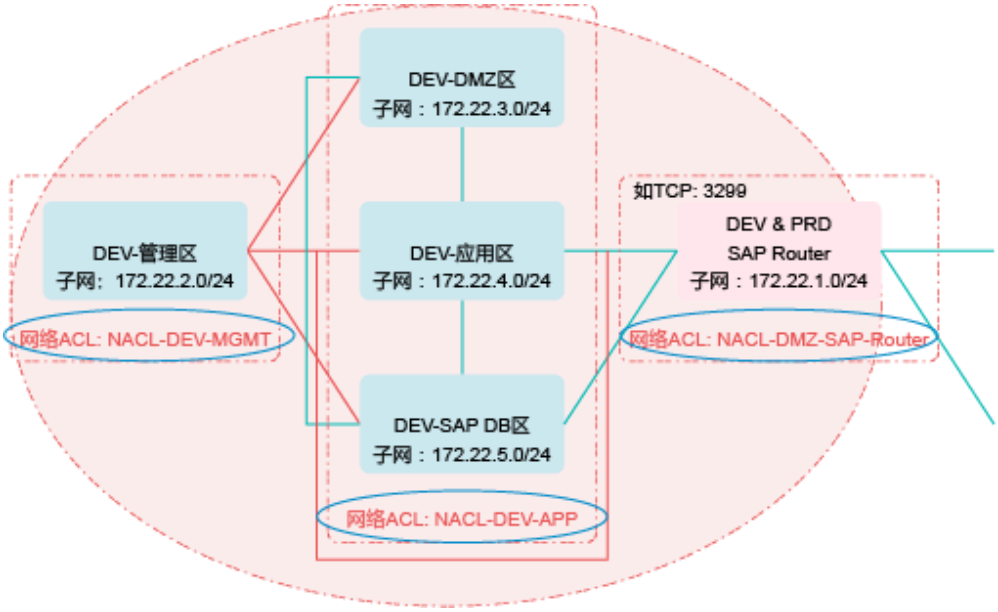
图2-2 开发测试环境子网、网络 ACL 分布图



安全策略

开发测试环境内部涉及如下网络 ACL 实例：网络 ACL“NACL-DEV-MGMT”、“NACL-DEV-APP”、“NACL-DMZ-SAP-Router”，分别关联图 2-3 中所示子网。各网络 ACL 实例默认拒绝所有流量(默认失败)，跨 ACL 的子网间如需互通，需以白名单形式添加策略放通相应流量(最小化)。

图2-3 开发测试环境子网、网络 ACL 分布图



网络 ACL“NACL-DEV-MGMT”，关联开发测试环境 DEV-管理区子网，通过策略限制可由管理区跳板机访问开发测试环境其它区域服务器的管理端口(22 等)，并拒绝由开发测试环境其它区域发起的对管理区跳板机的连接。

说明

本节中提到的 IP 地址及端口号仅为示例，如有其它管理端口，可根据实际情况增加策略。本节仅涉及开发测试区内部策略。

表2-1 网络 ACL“NACL-DEV-MGMT”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 DEV-DMZ 区	172.22.3.0/24	TCP	22	允许	允许测试环境管理区跳板机访问 DEV-DMZ 区服务器 SSH 端口。
对 DEV-应用区	172.22.4.0/24	TCP	22	允许	允许测试环境管理区跳板机访问 DEV-应用区服务器 SSH 端口。
对 DMZ-SAP-DB 区	172.22.5.0/24	TCP	22	允许	允许测试环境管理区跳板机访问 DEV-SAP-DB 区服务器 SSH 端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	22	允许	允许测试环境管理区跳板机访问 DEV&PRD-SAP-Router 服务器 SSH 端

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
					口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表2-2 网络 ACL“NACL-DEV-MGMT”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL“NACL-DEV-APP”，关联开发测试环境 DEV-DMZ 区、DEV-应用区、DEV-SAP-DB 区子网，入方向，通过策略限制可由管理区跳板机访问区域内服务器的管理端口(22 等)，限制可由 SAP-Router 访问区域内服务器的业务端口。

表2-3 网络 ACL“NACL-DEV-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表2-4 网络 ACL“NACL-DEV-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 DEV-管理区	172.22.2.0/24	TCP	22	允许	允许测试环境管理区跳板机访问本区域内服务器 SSH 端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	234	允许	允许 SAP-Router 服务器访问本 DEV-应用区域内服务器 234 业务端口。
对 DEV&PRD-SAP-Router	172.22.1.0/24	TCP	345	允许	允许 SAP-Router 服务器访问本 DEV-SAP-DB 区域内服务器 345 业务端口。

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

网络 ACL“NACL-DMZ-SAP-Router”，关联 DEV&PRD-SAP-Router 子网，入方向，通过策略限制可由管理区跳板机访问区域内服务器的管理端口(22 等)，出方向限制可由 SAP-Router 访问开发测试环境应用区、SAP-DB 区指定的业务端口。

表2-5 网络 ACL“NACL-DMZ-SAP-Router”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 DEV-应用区	172.22.4.0/24	TCP	234	允许	允许 SAP-Router 服务器访问 DEV-应用区域内服务器 234 业务端口。
对 DEV-SAP-DB 区	172.22.5.0/24	TCP	345	允许	允许 SAP-Router 服务器访问 DEV-SAP-DB 区域内服务器 345 业务端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表2-6 网络 ACL“NACL-DMZ-SAP-Router”入方向

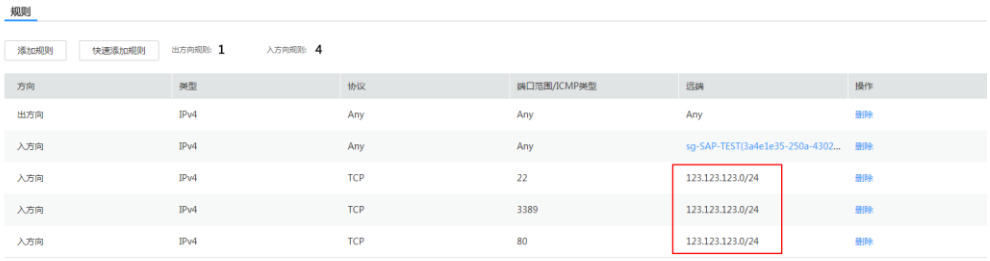
规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 DEV-管理区	172.22.2.0/24	TCP	22	允许	允许测试环境管理区跳板机访问本区域内服务器 SSH 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

安全组，如 SG_DEV_MGMT、SG_DEV_DB 等(与公网无交互)，关联开发测试环境中相应子网中的云服务器，需严格按照最小化的原则控制云服务器对外开放的端口范围，可参考以下图 2-4(具体端口请根据实际情况设置)。对 IP 的访问控制策略，通过网络 ACL 实现。其它开发测试环境与公网无交互的安全组(详见全景图)，可参考实施。

图2-4 安全组策略示例

安全组，如 SG_DEV_SRM、SG_DEV_Hybrids、SG_SAP_ROUTER(与公网有交互)，关联开发测试环境中相应子网中的云服务器，需严格按照最小化的原则控制云服务器对外开放的端口范围以及源 IP 范围，如公网 IP 较为固定，可参考以下图 2-5(具体端口请根据实际情况设置)。

图2-5 安全组策略示例



如公网 IP 不固定的场景，可根据业务需要(如模拟测试，技术支持)，临时放通特定公网源 IP，相应事务完成后删除策略。

2.2 网络边界安全

2.2.1 与生产环境边界

由于测试环境仍属于安全级别较低的区域，安全风险较高，如需与生产环境互联，此边界需要特别关注，采用较严格的访问控制策略：由开发测试环境发起对生产环境的访问，需严格控制(默认失败)，仅能访问生产环境中必要的*[IP]:[PORT]* (最小化)。由生产环境发起的对开发测试环境的访问，可以采用稍弱的访问控制策略。

安全策略

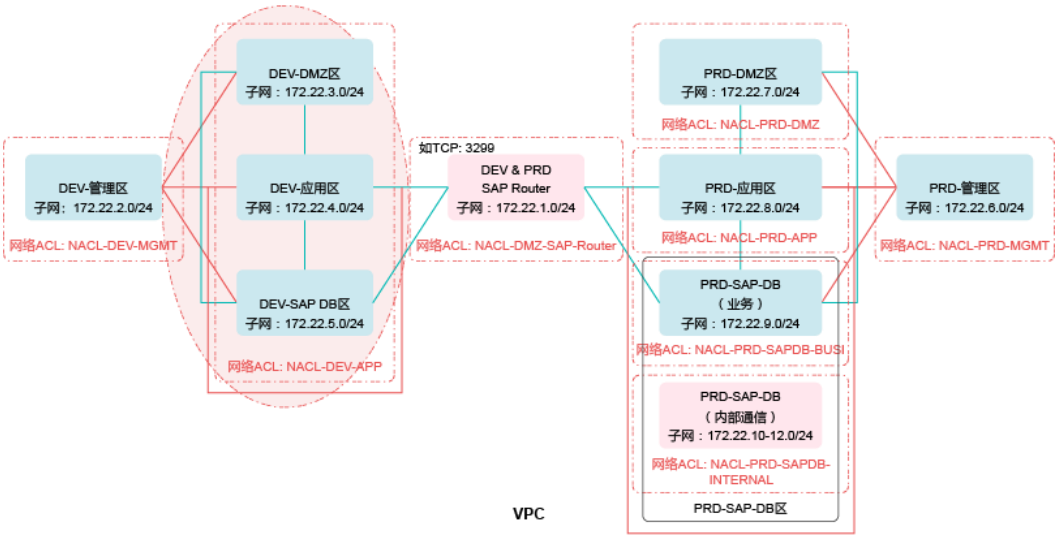
如图 2-6 所示，网络 ACL“NACL-DEV-APP”关联开发测试环境子相应网，需严格按照最小化的原则控制访问生产环境的出方向策略，限制其仅能访问生产环境中特定的

[IP]:[PORT]；对于由生产环境发起的对开发测试环境的入方向策略，这里可以根据实际情况设置稍弱的访问控制策略。

说明

强的、安全性高的、复杂的访问控制策略，会一定程度增加部署配置及运维成本，可以根据企业自身情况适当减少策略。

图2-6 开发测试环境子网、网络 ACL 分布图



与生产环境边界的策略主要包括对 PRD-DMZ 区、对 PRD-应用区、对 PRD-DB 区的策略，详细请参考下方表 2-7 与表 2-8。

说明

本节中提到的 IP 地址及端口号仅为示例，如有其它业务流，可根据实际情况增加策略。本节仅涉及开发测试区与生产环境策略。

表2-7 网络 ACL“NACL-DEV-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 PRD-DMZ 区	172.22.7.0/24	TCP	1433	允许	允许测试环境子网中的 VM 访问生产环境 PRD-DMZ 区中服务器 1433 端口进行软件/代码推送更新。
对 PRD-应用区	172.22.8.0/24	TCP	2433	允许	允许测试环境子网中的 VM 访问生产环境 PRD-应用区中服务器 2433 端口进行软件/代码推送更新。
对 PRD-DB 区	172.22.9.0/24	TCP	3443	允许	允许测试环境子网中的 VM 访问生产环境 PRD-DB 区中服务器 3443 端口进行软件/代码推送更新。

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的入站数据流。

表2-8 网络 ACL“NACL-DEV-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 PRD-DMZ 区	172.22.7.0/24	TCP	ANY	允许	允许生产环境 PRD-DMZ 区中的 VM 访问本区域中服务器任意 TCP 端口。
对 PRD-应用区	172.22.8.0/24	TCP	ANY	允许	允许生产环境 PRD-应用区中的 VM 访问本区域中服务器任意 TCP 端口。
对 PRD-DB 区	172.22.9.0/24	TCP	ANY	允许	允许生产环境 PRD-DB 区中的 VM 访问本区域中服务器任意 TCP 端口。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则 (不可修改) 处理的出站数据流。

安全组策略请见 2.1 网络隔离与访问控制中相关内容。

2.2.2 业务边界

根据业务特点，由于开发测试环境需与企业内部开放、测试使用，也有公网访问需求，需建立与企业内网(IDC)互联的 VPN 通道，同时需要设置云上与云下以及云上与互联网之间的访问控制策略。

VPN

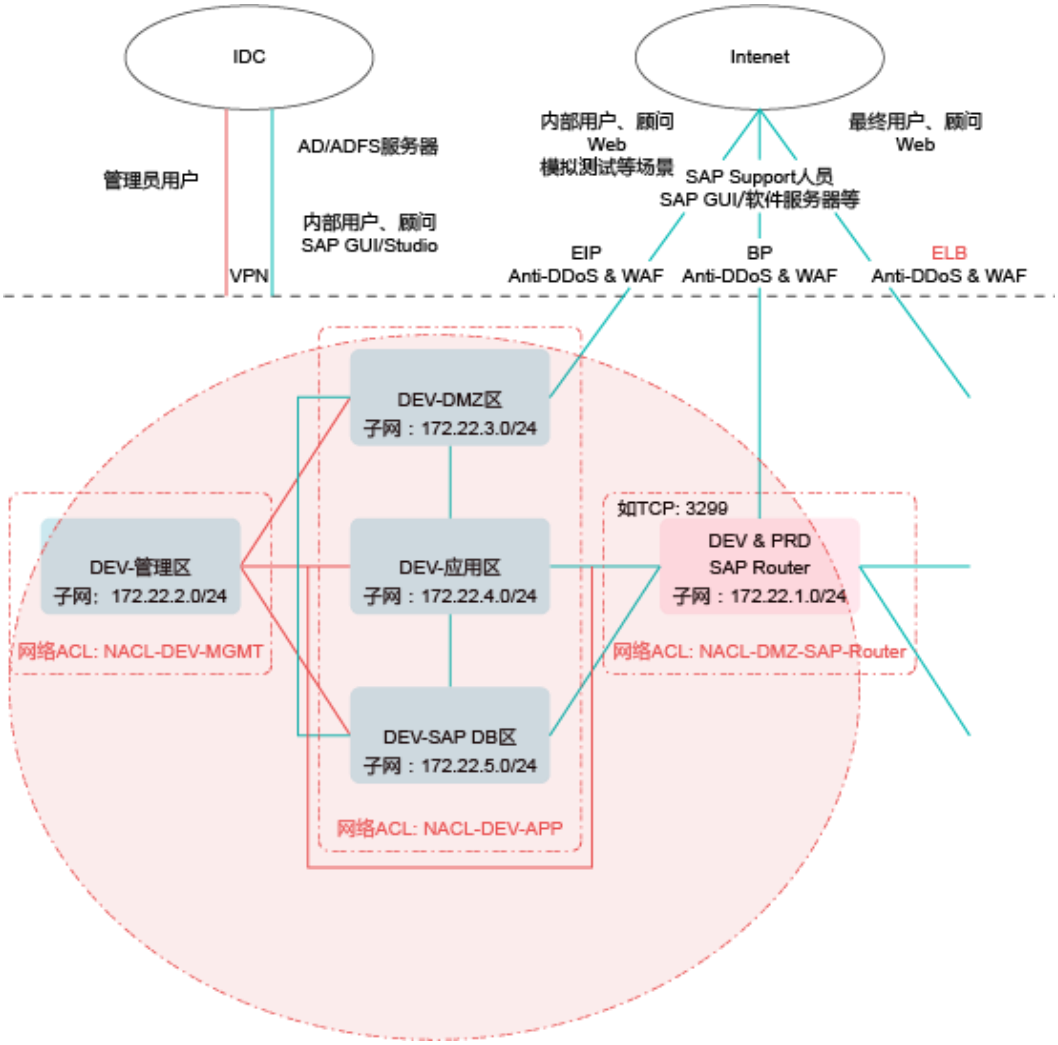
由于开发测试环境供企业内部开放、测试使用，多为静态连接需求，综合考虑安全性与时延，推荐的优先级为：专线(DC)>VPN(IPSec)>SSL VPN。

说明
华为 VPN 云服务当前仅提供专线和 IPSec VPN 形式，暂不支持 SSL VPN，如需使用 SSL VPN 可选用第三方镜像产品自行部署。

安全策略

由于开发环境同时需要与企业内部通信，还需提供互联网的业务访问，综合考虑通过网络 ACL 进行相应的访问控制策略。

图2-7 开发测试环境子网、网络 ACL 分布图



如图 2-7 所示，网络 ACL“NACL-DEV-APP”关联开发测试环境相应子网，需严格控制访问企业内网环境(IDC)的出方向策略，限制其仅能访问企业内网环境(IDC)中特定的*[IP]:[PORT]*。

对于由 IDC 发起的对开发测试环境的入方向策略，根据场景不同设置相应的访问控制策略。如 AD 服务器与保留系统，场景较为固定，应设置相应的策略，使其能够与云上特定*[IP]:[PORT]*互通。而对于 End user，可限制能够访问的特定 IP 段与端口(业务端口)区间，以及 22/3389 等管理端口。

网络 ACL“NACL-DEV-APP”“NACL-DMZ-SAP-Router”关联开发测试环境相应子网，需严格控制互联网访问的入方向策略，限制外网仅能访问开发测试环境特定的*[IP]:[PORT]*。

说明

本节中提到的 IP 地址及端口号仅为示例。如公网 IP 不固定的场景，可根据业务需要(如技术支持)，临时放通特定源 IP，相应事务完成后删除策略。如有其它业务流，可根据实际情况增加策略。

表2-9 网络 ACL“NACL-DMZ-SAP-Router” 出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则(不可修改) 处理的入站数据流。

表2-10 网络 ACL“ NACL-DMZ-SAP-Router”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 SAP 技术支持人员，SAP GU/软件服务器 I 等	123.123.123.0/24	TCP	3299	允许	允许互联网 SAP 技术支持人员(特定源 IP)，SAP GUI/软件服务器等访问开发测试环境中的 DEV&PRD-SAP-Router，进而访问后端业务。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表2-11 网络 ACL“NACL-DEV-APP”出方向

规则 #	目的 IP	协议	目的端口	允许/拒绝	说明
对 AD/ADFS 服务器	IDC-AD/ADFS 网络	TCP	AD/ADF 端口	允许	允许与 IDC 内部 AD/ADFS 服务器进行对接。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表2-12 网络 ACL“NACL-DEV-APP”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对 Internet 内部用户/顾	123.123.123.0/24	TCP	80	允许	允许互联网特定 IP 的内部用户、顾问，访问开发测试环境中的 WEB 服务。

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
问。					
对 Internet 内部用户/顾问。	123.123.123.0/24	TCP	443	允许	允许互联网特定 IP 的内部用户、顾问，访问开发测试环境中的 WEB 服务。
对 IDC 内部用户、顾问。	客户数据中心某子网-b	TCP	80	允许	允许客户数据中心某子网-b 中的内部用户、顾问，访问开发测试环境中的 WEB 服务。
对 IDC 内部用户、顾问。	客户数据中心某子网-b	TCP	443	允许	允许客户数据中心某子网-b 中的内部用户、顾问，访问开发测试环境中的 WEB 服务。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

安全组策略请见 2.1 网络隔离与访问控制中相关内容。

安全服务

- Anti-DDoS

根据业务特点，由于开发测试环境有公网访问需求，建议 SAP-Router、SRM、Hybrids 服务器部署 Anti-DDoS 防护，推荐使用华为云 Anti-DDoS 流量清洗服务，对相应的 EIP 进行 DDoS 防护。

- WAF

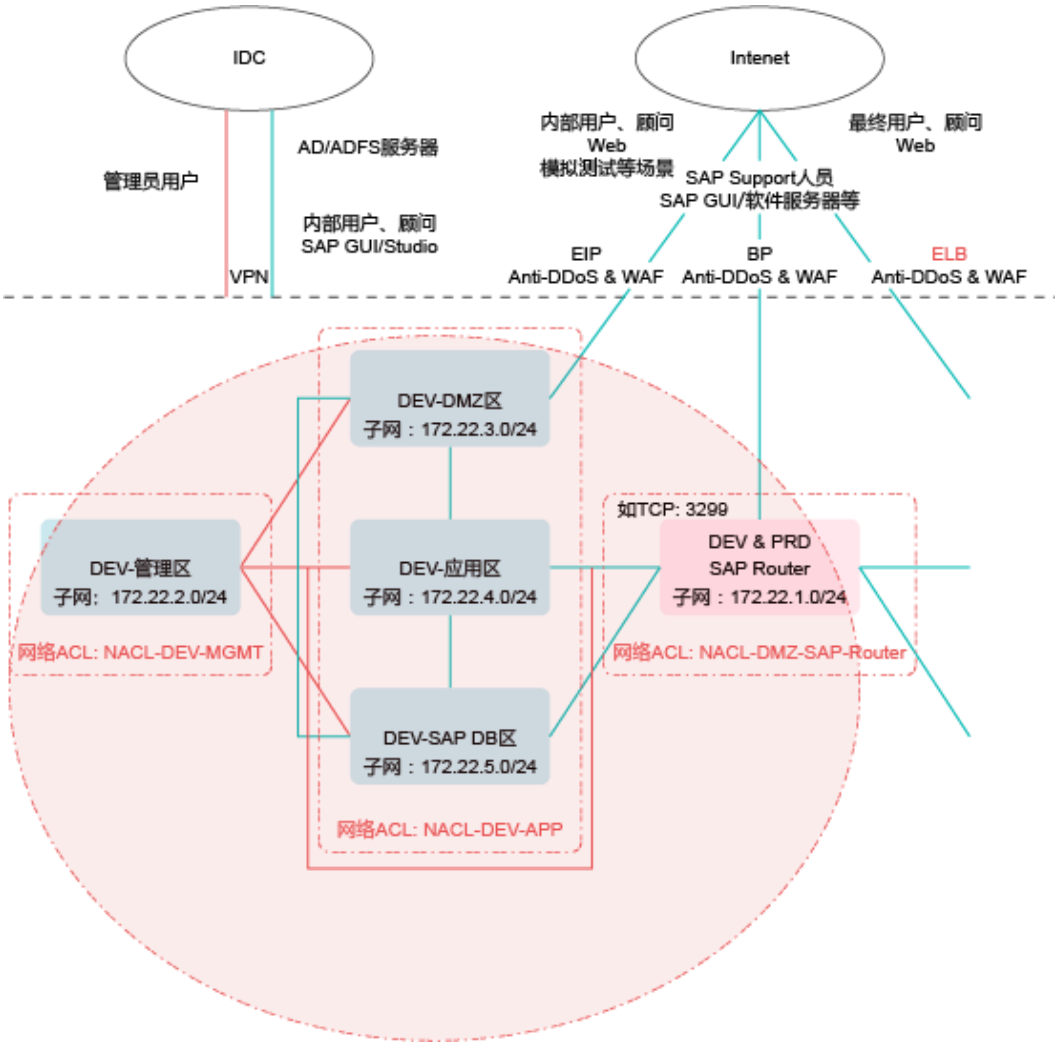
根据业务特点，由于开发测试环境需向互联网提供 Web 应用服务，建议部署 Web 应用防火墙，应对诸如 OWASP TOP10 Web 攻击，推荐华为云 Web 应用防火墙服务，创建 WAF 实例防护相应 EIP。

2.2.3 运维边界

由于管理区无公网访问需求，参考企业安全实践，仅需设置与 IDC 间的访问控制策略。

安全策略

图2-8 生产环境子网、网络 ACL 分布图



如图 2-8 所示，网络 ACL“NACL-DEV-MGMT”关联生产环境管理区子网，对于由 IDC 发起的对生产环境的入方向策略(管理员)，可限制能够访问管理区主机的 22/3389 等管理端口。

说明

本节中提到的 IP 地址及端口号仅为示例。管理员也可设置具备 End Uesr 角色相应的策略，使管理员可访问开发测试环境业务端口。

表2-13 网络 ACL“NACL-DEV-MGMT”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对管理员	客户数据中心某子网-a	TCP	22	允许	允许客户数据中心某子网-a 中的管理员访问开发测试环境管

规则#	源 IP	协议	目的端口	允许/拒绝	说明
					理区的 VM。
对管理员	客户数据中心某子网-a	TCP	3389	允许	允许客户数据中心某子网-a 中的管理员访问开发测试环境管理区的 VM。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

表2-14 网络 ACL“NACL-DEV-MGMT”出方向

规则#	目的 IP	协议	目的端口	允许/拒绝	说明
1	0.0.0.0/0	ANY	ANY	允许	对于由管理区发起的出方向流量不做限制。
*	0.0.0.0/0	ANY	ANY	拒绝	拒绝所有未经前置规则处理的数据流。

安全组策略请见 2.1 网络隔离与访问控制中相关内容。

安全服务

参考企业安全实践，通过堡垒机实现运维/运营人员不接触系统账户密码(各系统部件账号托管在堡垒机系统)，对运维人员通过堡垒机进行的操作范围进行权限控制，限制高危操作权限，并对运维人员操作全流程审计记录，做到事件可监控、可追踪、可回溯。堡垒机以云服务器模式部署于管理区子网中。

2.3 安全管理

安全评估

对于 Web 站点及关键主机，建议定期进行安全评估(安全体检服务-专业安全评估)，以及时发现、规避安全风险。

- 服务测试范围包括：
  - 网站类：SQL 注入、XSS 跨站、文件包含、任意文件上传、任意文件下载、Web 弱口令、服务弱口令。
  - 主机类：远程漏洞扫描、弱口令扫描、高危端口识别、高危服务识别、基线检查。

- 华为安全专家团队会对专业机构提交的体检报告进行审核，引导专业机构提高服务质量，给客户更佳的用户体验。
- 提供准确的漏洞信息和对应的修复建议，并可为用户定制整体安全解决方案，帮助用户构筑完善的安全防御机制。

网站监控

- 非法篡改监控(监测网页篡改行为，特别是一些越权篡改、暗链篡改等)。
- 坏链检测（如链接目的页面已经删除或转移;网站搬家导致链接无效，设置静态链接导致原内文章链接地址无法访问等）。
- 脆弱性检测（SQL 注入、XSS 跨站、文件包含、敏感信息泄露、任意文件下载等）。
- 可用性检测（通过全国多地监测和 DNS 解析监测监控网站的可用性）。
- 对外服务开放监测（定期对网站开放服务进行扫描，检测是否开放多余服务）。
- 敏感内容审计（定期对网站内容进行检测，对出现敏感内容页面进行告警）。
- 协同预警（协同技术小组根据最新漏洞与威胁跟踪结果提供预警）。

秘钥管理

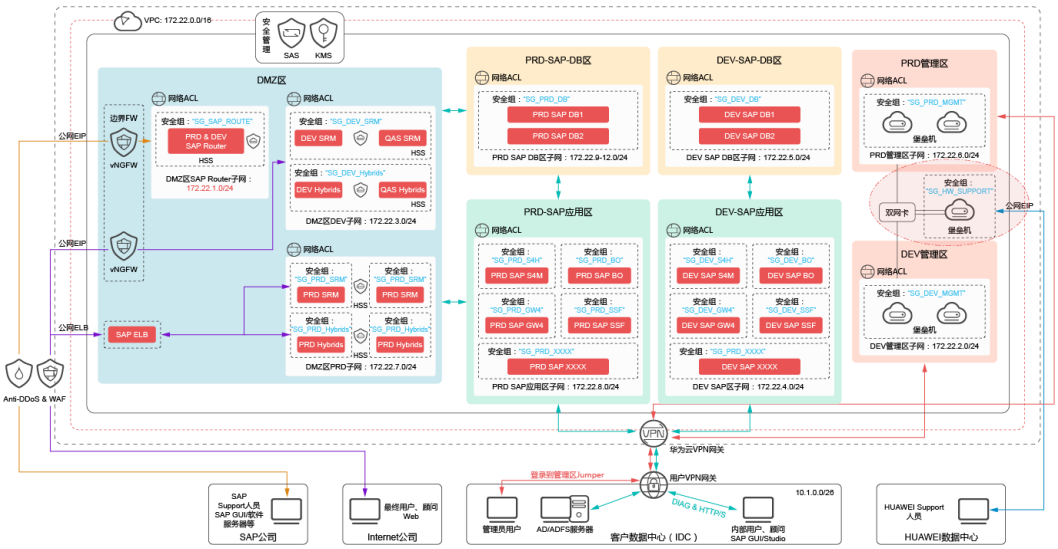
业务系统中如有数据加密场景，建议使用华为云 KMS 服务进行密钥管理，以满足安全、合规等要求。

2.4 主机安全

与公网有交互的虚拟机建议参考华为云主机防暴力破解解决方案进行相应的加固。主要涉及系统加固，以及主机安全产品(HIDS/AV 等)的应用。

3 华为技术支持通道安全方案

图3-1 华为技术支持通道安全方案



如涉及华为技术人员场景，需要单独部署华为技术人员专用堡垒机，保障运维通道安全，方案详见图 3-1。

该方案与企业内部堡垒机对比有如下几点区别：

- 华为专用堡垒机需配置双网卡，分别属于 PRD 管理区与 DEV 管理区。
- 华为专用堡垒机需配置一个 EIP，以便华为技术人员接入。

  由于华为专用堡垒机需 Internet 可访问，EIP 绑定的网卡所属的子网需增加网络 ACL 入站策略，出站策略无需变动，放通 Internet 对专用堡垒的访问。

  以 EIP 网卡属于 DEV-管理区子网为例，增加如下入站 ACL 策略：

说明

本节中提到的 IP 地址及端口号仅为示例。如有特殊情况，需新增临时策略放通其它源 IP。

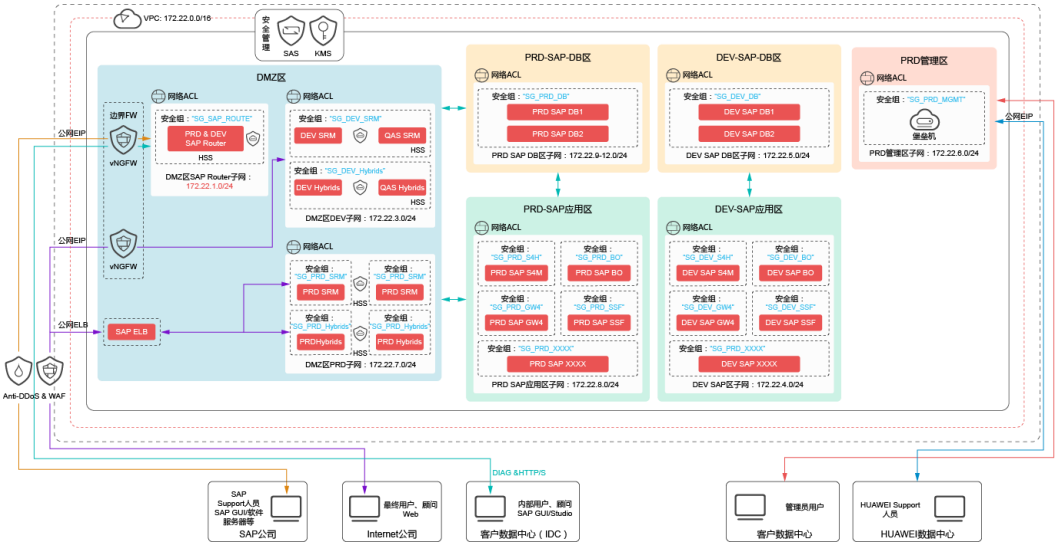
表3-1 网络 ACL“NACL-DEV-MGMT”入方向

规则 #	源 IP	协议	目的端口	允许/拒绝	说明
对华为技术人员	2.2.2.0/24	TCP	8443	允许	允许华为技术支持人员(固定源 IP 范围)中的管理员访问专用堡垒机。

4 其它场景安全方案

如果出于成本考虑，云上 SAP 系统较为轻量，不准备采用 VPN/专线方案，所有业务以及运维通道均通过公网接入，安全方案建议见图 4-1。

图4-1 特殊场景安全方案



此方案主要区别为：

- 管理区合一，部署一台堡垒机，不在区分 PRD 与 DEV。
- 各业务出口、运维通道，如无必要对全网开放，建议加强网络 ACL 策略，严格限制源 IP。

5 安全方案配套表

说明
截止当前时间（2018 年 3 月 5 日），华为云 HSS 服务暂不支持 Windows 系统，Windows 版本仅限网页防篡改特性。

表5-1 华为云 SAP 安全解决方案配套建议

需求项	服务/产品	是否第三方	备注	默认配置建议
网络隔离与访问控制	VPC-网络 ACL	否	必选	N/A
	VPC-安全组	否	必选	N/A
Anti-DDoS	Anti-DDoS 流量清洗	否	必选，所有 EIP/公网 ELB 均开启防护	N/A
虚拟下一代防火墙	vNGFW：山石网科	是	强烈推荐，需根据业务带宽要求，决定规格与实例数量	旗舰版*2，主备
Web 防护	Web 应用防火墙	否	必选，所有公网站点接入 WAF 防护	专业版 * 1 年* N，N 为合同年限，下同
专线/VPN	云专线服务	否	必选，推荐专线(DC)>VPN(IPSec)，二选一	N/A
	VPN 服务	否	必选，推荐专线(DC)>VPN(IPSec) ，二选一	N/A
堡垒机	云安宝-云匣子	是	必选，根据实际需求决定部署实例数量及规格	50 资产 * 2 (PRD、DEV 各一台)

需求项	服务/产品	是否第三方	备注	默认配置建议
华为技术支持专用堡垒机	云安宝-云匣子	是	可选，根据实际需求决定部署实例数量及规格	100 资产 * 1
安全体检服务	SAS-专业安全评估包(站点&主机)	否	必选，根据站点及核心主机数量，按需购买	数量：10 (网站/主机) * 1 年 * N
	网站监控	否	可选，根据站点数量，按需购买	数量：2 * 1 年 * N
主机安全(HIDS/AV 等)	瑞星企业终端安全管理系统软件	是	必选，四选一即可	数量：10 Agent
	McAfee	是	必选，四选一即可	数量：10 Agent
	服务器安全狗	是	必选，四选一即可	数量：10 Agent
	HSS	否	必选，四选一即可	数量：10 Agent(Linux 企业版) * 1 年 *N，N 为合同年限
密钥管理	KMS	否	可选	按需
双因素认证	SecID	是	可选，根据实际需求决定规格	用户 10，主机 10

A 修订记录

修订记录	发布日期
第一次发布。	2018-03-12