☆**内 部**

百望内部网络使用规范

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **制度代码** | **版本** | **实施日期** | **主编单位** | **批准人** |
| BW-ZD-IT-04 | V1.0 | 2019-10 | IT组 |  |
| 说明： | | | | |

目录

[第一章 总则 1](#_Toc22067285)

[第二章 名词解释 1](#_Toc22067286)

[第三章 网络系统管理 1](#_Toc22067287)

[第四章 终端设备网络使用 2](#_Toc22067288)

[第五章 办公区网络互访规范 3](#_Toc22067289)

[第六章 租赁机房网络使用 3](#_Toc22067290)

[第七章 机房网络互访规范 3](#_Toc22067291)

[第八章 公有云端网络使用 4](#_Toc22067292)

[第九章 公有云网络互访规范 5](#_Toc22067293)

## 总则

1. 为加强对计算机信息网络的保护，保障通过计算机网络联网传播信息安全，维护业务系统和公共秩序稳定，特制定本规范。

## 名词解释

1. 生产网络系统，是指负责公司生产业务系统通信的网络设备所组成的系统。
2. 办公区是指公司员工日常工作的区域；IDC区是指公司自建或租赁第三方的机房机柜区域；云端区域是指公司购买的公有云服务，包括阿里云，腾讯云等。
3. VPN（Virtual Private Network）是一种虚拟专线网络技术，用于通过国际互联网安全的访问公司内部网络。

## 网络系统管理

1. 公司网络信息安全责任小组，由基础系统部人员组成，负责本单位网络安全工作的策略、制度和实施；对本单位的网络安全工作负领导责任。
2. 网络安全管理员，每月定期进行安全策略检查和梳理，及时修正相关策略，同时做好相关备份工作。
3. 生产网络系统发生变更，需要通过基础系统部领导同意，重大调整需CTO同意后执行。
4. 办公区域采用192.168.0.0/16网段。（部分测试区业务系统暂时分配了该段地址）。
5. IDC服务器网络和第三方专线接入时，采用172.16.0.0/16-172.31.0.0/16网段。
6. 云端网络和VPN终端接入时，采用10.0.0.0/8网段。（部分测试区业务系统暂时分配了该段地址）
7. 网络设备管理统一采用堡垒机和Web控制台方式进行维护。其中机房设备采用堡垒机地址为“jump.51baiwang.com”；云端网络设备管理采用云端Web控制台。

## 终端设备网络使用

1. 公司网络系统有无线和有线两种方式，接入时终端电脑地址需配置为自动获取。
2. 有线网络默认关闭，如有需要需IT组配置开启。
3. 终端电脑无线接入网络，有“办公无线网络(office)”和“内部无线网络(inner)”可以使用, 其中办公无线网络仅用于访问公网互联网，内部无线网络用于访问公网互联网和内部业务系统。
4. 办公无线网（offic）采用WPA/WPA2-PSK密码认证，每台终端接入需输入统一的预共享密码，该密码每年度修改一次。
5. 内部无线网络（inner）采用WPA/WPA2的802.1x认证，每台终端接入需输入个人的AD账号。
6. 打印设备使用无线“BW-Print”接入点，采用WPA/WPA2-PSK密码+Mac地址绑定方式认证接入。
7. 远程办公需要使用公司的VPN系统，认证登录采用个人AD账号进行。
8. 访客接入网络默认仅可以使用“办公无线网络(office)”， 如有特殊要求，需由内部员工申请AD账号，申请人提交钉钉“IT资源申请”通过后由网络管理员配置执行。

## 办公区网络互访规范

1. 办公区设备默认允许访问国际互联网，默认禁止对国际互联网直接提供服务，不支持特殊申请。
2. 办公区终端管理机房服务器（如SSH/RDP协议）默认采用堡垒机（jump.51baiwang.com）进行维护，支持特殊业务申请。
3. 办公区访问机房和云端默认策略如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 源区域 | 目的区域 | 默认策略 | 特殊申请变更 |
| 办公区 | 机房非生产环境 | 允许 | 支持 |
| 办公区 | 机房生产环境 | 禁止 | 支持 |
| 办公区 | 云端非生产环境 | 允许 | 支持 |
| 办公区 | 云端生产环境 | 禁止 | 支持 |

如有特殊要求，需由使用人提交钉钉“访问安全策略申请”，通过后由网络管理员配置执行。

## 租赁机房网络使用

1. 机房网络系统有无线和有线两种方式，无线网络仅用于管理人员维护接入。
2. 机房有线网络默认关闭，使用前需由网络管理员分配地址并启用接入端口。
3. 机房无线网络采用采用WPA/WPA2-PSK密码+Mac地址绑定方式认证接入，仅限机房相关运维人员使用。
4. 多机房之间互通采用专线或VPN技术实现。

## 机房网络互访规范

1. 机房设备默认禁止访问国际互联网，默认禁止对国际互联网提供服务，根据业务需要支持特殊申请。
2. 机房区域访问其他区域默认策略如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 源区域 | 目的区域 | 默认策略 | 特殊申请变更 |
| 有孚机房非生产环境 | 办公区 | 允许 | 支持 |
| 有孚机房生产环境 | 办公区 | 禁止 | 支持 |
| 有孚机房非生产环境 | 云端非生产环境 | 允许 | 支持 |
| 有孚机房生产环境 | 云端非生产环境 | 禁止 | 支持 |
| 有孚机房非生产环境 | 云端生产环境 | 禁止 | 支持 |
| 有孚机房生产环境 | 云端生产环境 | 禁止 | 支持 |

如有特殊要求，需由使用人提交钉钉“访问安全策略申请”，通过后由网络管理员配置执行。

## 公有云端网络使用

1. 云端网络产品包括虚拟专有网络（VPC）、虚拟交换（VSW）、边界路由器（VBR）、负载均衡（SLB）、网络地址转换（NAT）、虚拟专线（VPN/智能接入网关）、弹性公网地址（EIP）和共享带宽包、以及互联产品高速通道和云企业网。
2. 云端网络安全产品包括安全组、云防火墙、Web应用防火墙（WAF）。
3. 云端资源对外提供服务使用负载均衡（SLB）+弹性公网地址（EIP）和共享带宽。
4. 云端资源访问国际互联网使用网络地址转换（NAT）+弹性公网地址（EIP）和共享带宽。
5. 弹性公网地址（EIP）按照出入端口统一且最少原则进行整合与分配。根据业务系统（如开放平台以及大客户前置类业务等）和系统环境（如生产、预生产、测试、外包环境等）不同维度的类别划分出口和入口地址。

## 公有云网络互访规范

1. 云端所有资源（包括ECS/RDS等资源）默认禁止访问国际互联网，默认禁止直接对国际互联网提供服务，支持特殊申请。
2. 云端资源各个区域（如生产、测试区、大客户资源区）之间默认禁止访问，不支持特殊申请。
3. 云端网络访问其他区域默认策略如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 源区域 | 目的区域 | 默认策略 | 特殊申请变更 |
| 云端非生产环境 | 办公区 | 允许 | 支持 |
| 云端生产环境 | 办公区 | 禁止 | 支持 |
| 云端非生产环境 | 有孚非生产环境 | 允许 | 支持 |
| 云端生产环境 | 有孚非生产环境 | 禁止 | 支持 |
| 云端非生产环境 | 有孚生产环境 | 禁止 | 支持 |
| 云端生产环境 | 有孚生产环境 | 禁止 | 支持 |

如有特殊要求，需由使用人提交钉钉“访问安全策略申请”，通过后由网络管理员配置执行。