阿里云效代码防泄漏使用指南

北京完信科技有限公司

2023 年 3 月

产品简介

北京完信零信任控制网关是基于零信任理念实现的软件定义边界解决方案，适用于企业/事业单位实现无边界互联网办公，企业关键资产保护的网络安全系统。本系统在当前移动和云办公形式下，提供多终端接入认证、内外网访问的一致性体、关键资产的安全防护功能，实现支持企业高性能的WEB化办公，关键资产的客户端访问需求。本系统是北京完信科技有限公司自主研发，支持国密加解密算法，具有完全的知识产权。

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京完信科技有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京完信科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

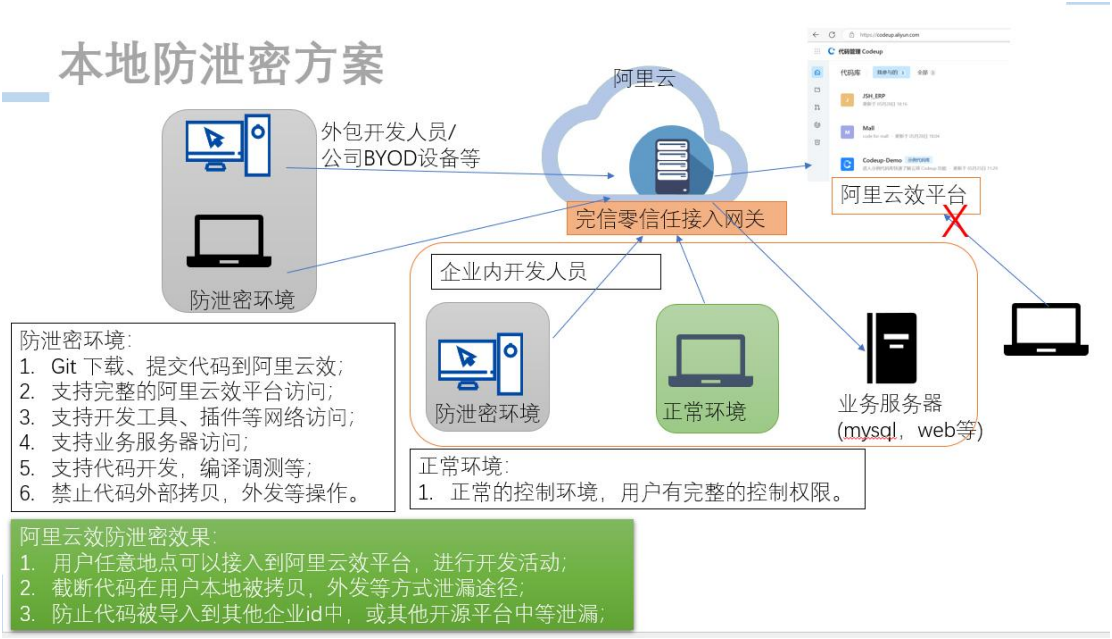
您可以访问完信科技有限公司官方网站：http://www.lstcloud.com/获得最新技术和产品信息。

目录

1.概述

完信零信任数据防泄密解决方案，针对阿里云效平台，推出无缝衔接代码防护方案。通过在云平台部署完信零信任网关，开发者机器部署零信任终端，阿里云效平台配置 IP 访问白名单，仅允许完信零信任网关访问项目空间，实现数据代码的流转闭环。零信任终端通过零信任网关，接入阿里云效进行代码下载，提交。代码下载到本地时，由零信任终端实现对代码的透明加密，U 盘访问控制，外发控制，拷贝控制，打印控制等泄漏防护，同时在本地不影响用户正常的上网、办公等活动，实现防泄漏的目标。

方案描述如下图:



完信零信任防泄密工作空间，通过在用户终端设备上建立工作目录，对该目录进行数据加密保护，工作数据自动保存到工作目录中，由内核驱动隔离安全空间内进程和安全空间外部进程，数据只能由外部空间流转到安全空间，对工作空间内数据外泄途径进行控制，包括外部网络访问，本机还回网络发送数据，U 盘访问，打印，拷贝等，让数据在工作空间内无法外泄，同时外部程序，包括恶意程序也无法对工作数据进行读写控制，还具有防勒索的效果;

1. 在PC上建立工作空间，仅对工作空间内数据进行防泄密控制；不影响工作空间外数据和上网行为。
优点：
1. 控制途径闭环，如git也无法将代码导出到互联网；
2. 外接U盘启动也无法访问保护数据；
3. 企业内部、外部等使用效果一致，适应各种场景。

特征1：

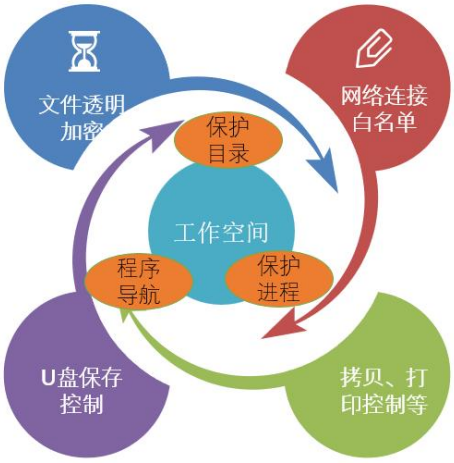
外部空间数据可以拷贝到工作空间内，工作空间数据禁止拷贝出去。

特征2：

工作空间内程序仅允许访问接入服务器，通过接入服务器访问公司内部网站或业务，也可以受控访问互联网(接入服务器做访问过滤）。

特征3：

非工作空间正常使用电脑，办公、上网等不受影响。



利用完信防泄密方案，可以实现对内部开发者、外包开发、BYOD 场景等，一套方案实现多场景防泄密防护。

2.网关基本配置

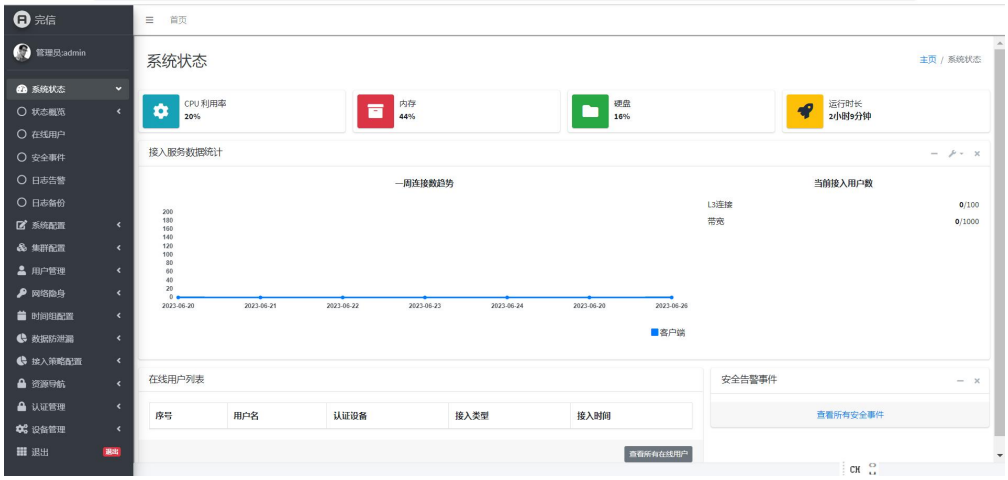
1. 在云服务器中，对网关云主机实例的防火墙，开通通信端口：tcp 18999，udp：18999
云防火墙对网关需要开放的端口：

端口	协议	授权对象	说明
7080	TCP	远程服务器接入 IP	远程服务器接入端口，按照业务开通情况增加该配置。
18999	TCP	0.0.0.0	用户接入端口
18999	UDP	0.0.0.0	用户接入端口

2. 利用默认用户接入网关，默认用户：adminUser，Wanxin@#m123

3. 接入后，打开管理员网址：https://192.25.25.1:15443/wsgui/，登陆用户信息：admin/gawt~90XjQ0#8

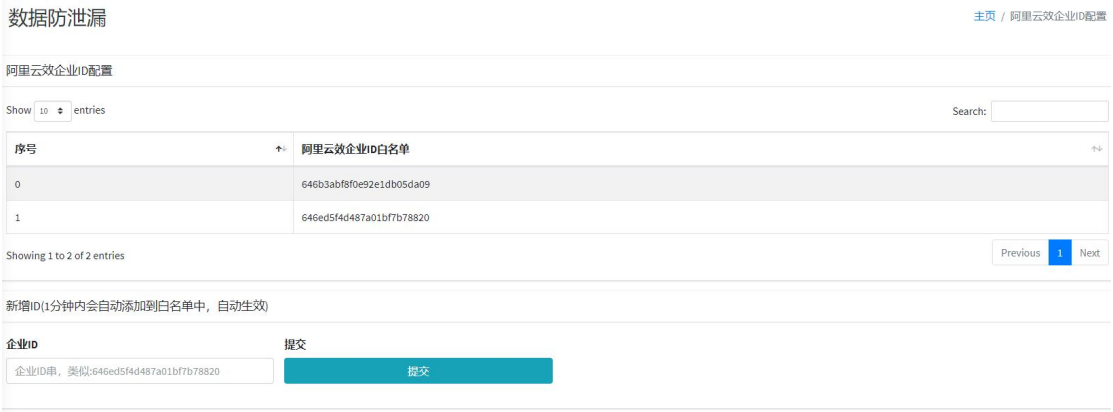
4 在 WEB 上配置基本属性如主机名，配置用户组，接入 IP 池数据。



3 管理员配置代码应用策略

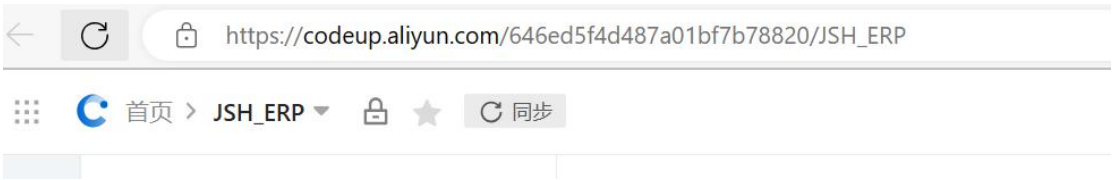
管理员先配置零信任接入网关，对开发用户使用的开发工具进行分组，对开发人员分组，将应用组与用户组进行关联，配置如下图。开发人员接入到网关时，会显示其自身关联的应用组。

用户访问阿里云效时，需要控制仅访问合法的企业 ID，防止将代码上传到其他企业 ID 的仓库中，因此需要设置企业 ID 的白名单。



企业 ID 的获取方法:

登陆阿里效平台，打开一个代码仓库，从 URL 中可以提取企业 ID，下图中 646ed5f4d487a01bf7b78820 为企业 ID。



4.用户使用

4.1 用户接入

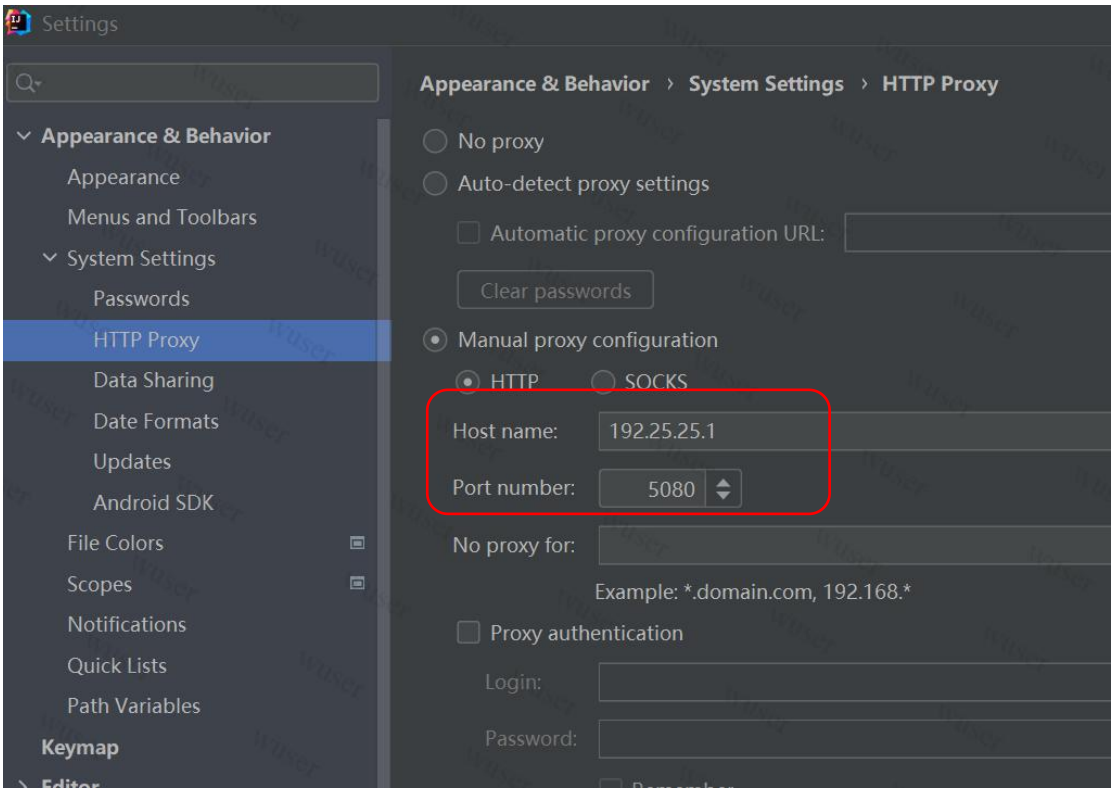
当用户接入使用完信零信任终端接入到网关时，网关自动下发该用户关联的策略，客户端接收到策略，当存在安全空间策略时，按需安装安全空间保护驱动程序。当用户没有关联到安全空间策略时，程序不会安装安全保护驱动程序。

用户接入后，如果配置了安全空间策略，登陆后会显示如下资源导航：

用户可以点击上述图标，打开应用。
用户可以启动 cmd 程序，通过控制台再打开其他应用。

4.2 用户侧上网配置

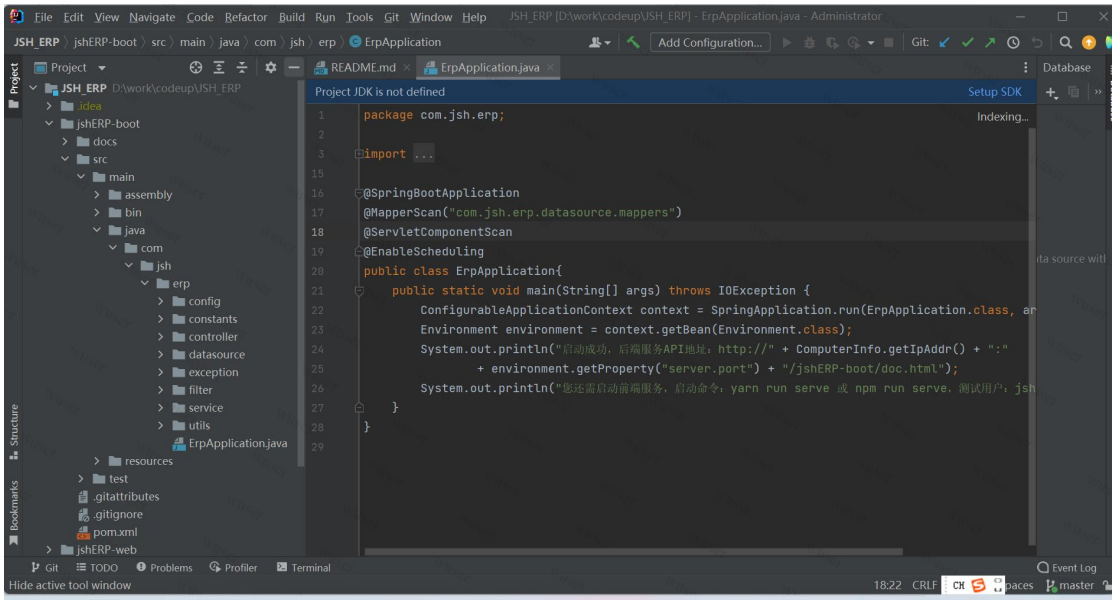
用户侧在安全空间内的程序，网络访问是受限的，仅允许访问合法网址。系统已经自动配置通用的访问通道，对浏览器、git 程序不用手动配置，可以访问合法网址。对一些应用如 IDEA 可以按需手动配置代理路径，如下图所示。



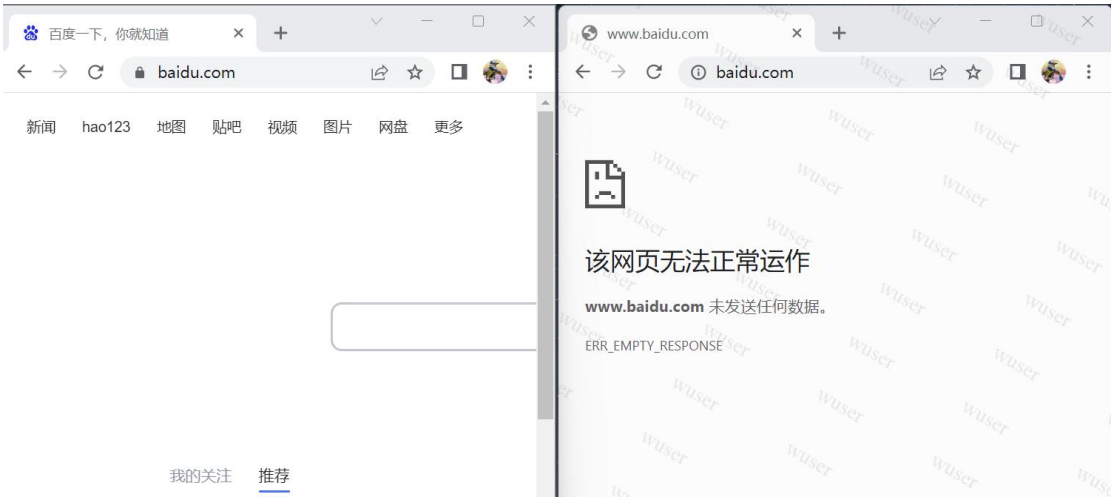
4.3 用户开发环境:

主机上安全空间外的程序不受影响，可以上网，下载文件，拷贝内容到安全空间内的程序中，安全空间内程序支持正常开发，编译，调测，代码提交等各种活动，但不支持将代码拷贝到安全空间外的程序，不支持随意的数据网络外发，U 盘保存等泄漏行为。

示例 1：用户打开 IDEA，使用方法与普通 IDEA 一致。



示例 2：安全空间内浏览器访问百度被禁止(仅能访问白名单网址)，安全空间外访问网络不受限制：



==========文档结束==========