|  |
| --- |
|  |
| **上海局杭甬客专车站信息安全V1.0升级V2.0** |
| **施工技术方案** |
|  |
| **北京信达环宇安全网络技术有限公司**  **二零一四年四月-V2** |
|  |

# 一、施工内容

1. 车站防火墙升级成车站安全边界，每个站2台；
2. 车站终端防病毒软件升级为安全加固，每个站3-5台；

# 二、防火墙升级成安全边界施工方案

2.1 施工步骤（60分钟）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 部署步骤 | 施工内容 | 影响范围 | 影响时间 | 电务配合 | 厂商配合 |
| 1 | 远程查看防火墙配置，并重启 | 车站CTC网络中断5分钟 | 5分钟 | 配合单位：杭州电务段  配合内容：协助要点，现场盯控，紧急情况旁路防火墙 | 配合单位：卡斯柯  配合内容：确认车站通道和业务应用正常 |
| 2 | 远程安装防火墙系统升级补丁，升级为安全边界 | 无影响 | 20分钟 |
| 3 | 升级成功后，重启安全边界 | 车站CTC网络中断5分钟 | 5分钟 |
| 4 | 测试车站终端业务应用 | 无影响 | 30分钟 |

2.2 测试内容

|  |  |  |
| --- | --- | --- |
| 步骤 | 测试内容 | 测试结论 |
| 1 | 从A网终端Ping 路由器A-F0/0口 |  |
| 2 | 从A网终端Ping 路由器B-F0/0口 |  |
| 3 | 从B网终端Ping 路由器A-F0/1口 |  |
| 4 | 从B网终端Ping 路由器B-F0/1口 |  |

2.3 紧急预案

当安全边界升级失败时，可以现场更换备机，如无备机，可以将车站安全边界旁路，就是恢复到没接入安全边界之前的网络状态。

旁路方法：旁路需要把安全边界从网络中旁路时，先把路由器到安全边界的4根网线拔下，再把原来交换机到路由器的4根网线接上即可。（这4根旁路线只需要接路由器端，另一端平时已接在交换机上；并且这些线就搁在路由器接口旁边，标有相应的详细线标。）

备注：

1）旁路2台安全边界只需要将2台CTC路由器A、B的F0/0、F0/1（E1/0）口的网线用与其捆绑在一起的旁路网线替换即可。

2）如果只旁路A网安全边界，则只需要替换CTC路由器A的F0/0和路由器B的F0/0（E0/0）口的网线。

3）如果只旁路B网安全边界，则只需要替换CTC路由器A的F0/1（E1/0）和路由器B的F0/1口的网线。

# 三、安全加固安装施工方案

3.1 部署步骤（150分钟）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 部署步骤 | 施工内容 | 影响范围 | 影响时间 | 电务配合 | 厂商配合 |
| 1 | 远程推送安装SAV | 相关终端设备 | 15分钟 | 配合单位：杭州电务段  配合内容：协助要点，准备终端备机两台，紧急情况更换备机 | 配合单位：卡斯柯  配合内容：确认车站业务应用正常 |
| 2 | 查杀病毒 | 相关终端设备 | 45分钟 |
| 3 | 远程推送安装安全加固客户端 | 相关终端设备 | 20分钟 |
| 4 | 安全管理中心注册客户端 | 相关终端设备 | 10分钟 |
| 6 | 测试车站终端业务应用 | 相关终端设备 | 30分钟 |

备注：绍兴北、上虞北、杭州南杭甬场车站已安装SAV杀毒软件，只需升级病毒定义，查杀病毒即可，余姚北、庄桥、杭州南线路所未安装SAV杀毒软件，需安装SAV，并查杀病毒。

3.2 测试内容

|  |  |  |
| --- | --- | --- |
| 步骤 | 测试内容 | 测试结论 |
| 1 | 车务终端A 应用是否正常 |  |
| 2 | 车务终端B 应用是否正常 |  |
| 3 | 信号员终端A应用是否正常 |  |
| 4 | 信号员终端B应用是否正常 |  |
| 5 | 维护终端应用是否正常 |  |

3.3 紧急预案

1、在安装杀毒软件SAV查杀病毒时，如车站终端病毒较多无法短时间清除干净、设备反复出现重启、死机等现象，需要更换车站终端备机。

2、安装完安全加固后，如业务不能正常使用，紧急情况卸载安全加固。

# 四、施工流程图



# 五、人员安排

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **中心人员** | **联系方式** | **车站人员** | **电话** | **备注** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |

## 附表1、车站安全边界升级和接入实施详细步骤

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **阶段** | **步骤** | **操作内容** | **预期结果** | **实际结果** |
| 车站安全边界升级 | 第1步 | 升级前，远程查看防火墙配置，并重启 | 车站业务5分钟内恢复 |  |
| 第2步 | 远程安装防火墙系统升级补丁，升级为安全边界 | 20分钟 |  |
| 第3步 | 升级成功后，重启安全边界 | 车站业务5分钟内恢复 |  |
| 应用测试 | 第4步 | 车站业务终端进行详细业务应用测试 | 30分钟 |  |
|  |  | **共计要点** | 60分钟 |  |

## 附表2、车站安全加固实施详细步骤

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **阶段** | **步骤** | **操作内容** | **预期结果** | **实际结果** |
| 终端杀毒 | 第1步 | 远程推送安装SAV | 15分钟 |  |
| 第2步 | 查杀病毒 | 45分钟 |  |
| 安全加固部署 | 第3步 | 远程推送安装安全加固客户端 | 20分钟 |  |
| 第4步 | 安全管理中心注册客户端 | 10分钟 |  |
| 应用测试 | 第5步 | 测试车站终端业务应用 | 30分钟 |  |
|  |  | **共计要点** | 120分钟 |  |

**附件3、加固安装信息表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 车站 | 终端 | IP地址 | 系统用户名 | 系统密码 | 加固用户名 | 加固密码 |
| 杭州南线路所 | 杭州南线路所车务A | 172.22.114.40 | db2 | db20 | HangZhouNanXianLuSuoCheWu-A | Xdhypoi123 |
| 杭州南线路所 | 杭州南线路所车务B | 172.22.114.41 | db2 | db20 | HangZhouNanXianLuSuoCheWu-B | Xdhypoi123 |
| 杭州南线路所 | 杭州南线路所近端A | 172.22.114.36 | db2 | db20 | HangZhouNanXianLuSuoJinDuan-A | Xdhypoi123 |
| 杭州南线路所 | 杭州南线路所远端B | 172.22.114.37 | db2 | db20 | HangZhouNanXianLuSuoYuanDuan-B | Xdhypoi123 |
| 杭州南线路所 | 杭州南线路所维护机 | 172.22.114.38 | db2 | db20 | HangZhouNanXianLuSuoWeiHuJi | Xdhypoi123 |
| 杭州南杭甬场 | 杭州南杭甬场车务A | 172.22.114.4 | db2 | db20 | HangZhouNanHangYongChangCheWu-A | Xdhypoi123 |
| 杭州南杭甬场 | 杭州南杭甬场车务B | 172.22.114.5 | db2 | db20 | HangZhouNanHangYongChangCheWu-B | Xdhypoi123 |
| 杭州南杭甬场 | 杭州南杭甬场维护机 | 172.22.114.6 | db2 | db20 | HangZhouNanHangYongChangWeiHuJi | Xdhypoi123 |
| 杭州南杭甬场 | 杭州南杭甬场信号员A | 172.22.114.8 | db2 | db20 | HangZhouNanHangYongChangXinHaoyuan-A | Xdhypoi123 |
| 杭州南杭甬场 | 杭州南杭甬场信号员B | 172.22.114.9 | db2 | db20 | HangZhouNanHangYongChangXinHaoyuan-B | Xdhypoi123 |
| 绍兴北 | 绍兴北车务A | 172.22.108.68 | db2 | db20 | ShaoXingBeiCheWu-A | Xdhypoi123 |
| 绍兴北 | 绍兴北车务B | 172.22.108.69 | db2 | db20 | ShaoXingBeiCheWu-B | Xdhypoi123 |
| 绍兴北 | 绍兴北维护机 | 172.22.108.70 | db2 | db20 | ShaoXingBeiWeiHuJi | Xdhypoi123 |
| 上虞北 | 上虞北车务A | 172.22.108.100 | db2 | db20 | ShangYuBeiCheWu-A | Xdhypoi123 |
| 上虞北 | 上虞北车务B | 172.22.108.101 | db2 | db20 | ShangYuBeiCheWu-B | Xdhypoi123 |
| 上虞北 | 上虞北维护机 | 172.22.108.102 | db2 | db20 | ShangYuBeiWeiHuJi | Xdhypoi123 |
| 余姚北 | 余姚北车务A | 172.22.108.132 | db2 | db20 | YuYaoBeiCheWu-A | Xdhypoi123 |
| 余姚北 | 余姚北车务B | 172.22.108.133 | db2 | db20 | YuYaoBeiCheWu-B | Xdhypoi123 |
| 余姚北 | 余姚北维护机 | 172.22.108.134 | db2 | db20 | YuYaoBeiWeiHuJi | Xdhypoi123 |
| 庄桥 | 庄桥车务A | 172.22.108.164 | db2 | db20 | ZhuangQiaoCheWu-A | Xdhypoi123 |
| 庄桥 | 庄桥车务B | 172.22.108.165 | db2 | db20 | ZhuangQiaoCheWu-B | Xdhypoi123 |
| 庄桥 | 庄桥维护机 | 172.22.108.166 | db2 | db20 | ZhuangQiaoWeiHuJi | Xdhypoi123 |
| 庄桥 | 庄桥信号员A | 172.22.108.168 | db2 | db20 | ZhuangQiaoXinHaoYuan-A | Xdhypoi123 |
| 庄桥 | 庄桥信号员B | 172.22.108.169 | db2 | db20 | ZhuangQiaoXinHaoYuan-B | Xdhypoi123 |

**附件4、安全边界IP地址表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 车站 | 边界A | 边界A网关 | 边界B | 边界B网关 | 子网掩码 |
| 杭州南线路所 | 172.22.114.44 | 172.22.114.33 | 172.22.115.45 | 172.22.115.62 | 255.255.255.224 |
| 杭州南杭甬场 | 172.22.114.12 | 172.22.114.1 | 172.22.115.13 | 172.22.115.30 | 255.255.255.224 |
| 绍兴北 | 172.22.108.76 | 172.22.108.65 | 172.22.109.77 | 172.22.109.94 | 255.255.255.224 |
| 上虞北 | 172.22.108.108 | 172.22.108.97 | 172.22.109.109 | 172.22.109.126 | 255.255.255.224 |
| 余姚北 | 172.22.108.140 | 172.22.108.129 | 172.22.109.141 | 172.22.109.158 | 255.255.255.224 |
| 庄桥 | 172.22.108.172 | 172.22.108.161 | 172.22.109.173 | 172.22.109.190 | 255.255.255.224 |

注意点：

1.施工前调查终端内是否放置打印机安装程序，如果有施工时可以先删除。杀毒完后将事先准备好的已查杀过的“杀毒软件”放置回

2.防火墙无法升级，需要更换防火墙CF卡的，准备螺丝刀，查看防火墙地址是否正常。

在宁波和宁波东站施工中出现施工后出现屏幕保护和时钟同步软件失效。需采取以下措施：

1. 在施工后检查屏幕保护“电源”内电源使用方案是否已变成“一直开着”，关闭监视器“从不”。
2. 施工后查看windows time服务是否开启。如果未开启重新开启。“我的电脑”右键“管理”计算机管理“服务”“windows time”右键重新启动。