天翼云云下一代防火墙加固升级指导

1、 需要升级版本范围

- 如下版本客户可以依据文档自行升级的版本：

  R8B1，R8B5,R8B10,R9F5,R10P3.16 及对应 PRO 版本

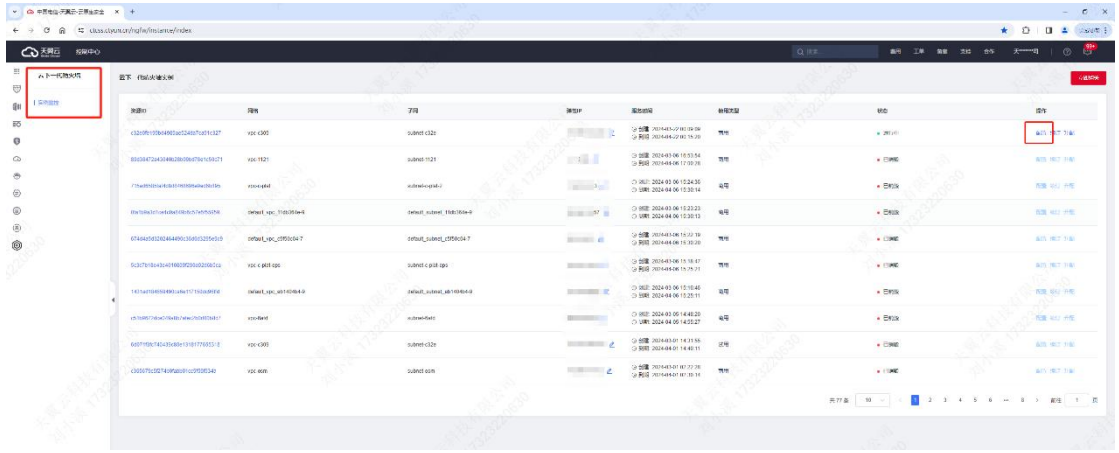
- **如下版本请确认好窗口时间提交工单由防火墙功能工程师协助升级：**

  R6P1.2，R7P8，R7P9，R7P9.5 及对应 PRO 版本

2、 如何查看云下一代防火墙实例版本

① 打开浏览器，地址栏输入 https://弹性 IP:10443【升级前版本显示页面】。

② 输入用户名密码，进行账号登录，并在系统-系统与特征库查看版本。



3、 升级建议

为了降低发生安全入侵事件的风险，建议客户将所有云下一代防火墙实例升级至 ECFW6000-5.5R10P5.10-PRO 版本。

注意：

- 非 R9F5 版本需要升级到 R9F5.1 及之后版本，才可以直接升级到 R10P5.10，详细情况见“4、下载链接及说明”。
- 升级至 R10P5.10 后，ecfwadmin 禁用 Web 登录，需通过天翼云下一代防火墙实例进行单点登录。历史防火墙实例（2023 年 11 月 8 号前开通的设备）在云控制台没有单点登录的路径，需要进入命令行开启 Web 登录的权限，详细流程见“8、历史版本升级后如何开启 Web 登录权限”。

4、 下载链接及说明

升级流程，请参照如下各个版本云下一代防火墙升级流程及注意事项表：

云下一代防火墙版本号	升级流程	注意事项
R8B1 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO 再升级到 ECFW6000-5.5R10P5.10-PRO 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。
R8B1-V6 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO-V6 再升级到 ECFW6000-5.5R10P5.10-PRO-V6 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。
R8B5 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO 再升级到 ECFW6000-5.5R10P5.10-PRO 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。
R8B5-V6 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO-V6 再升级到 ECFW6000-5.5R10P5.10-PRO-V6 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。
R8B10 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO 再升级到 ECFW6000-5.5R10P5.10-PRO 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。
R8B10-V6 及对应的 PRO 版本	先升级到 ECFW6000-5.5R9F5.1-PRO-V6 再升级到 ECFW6000-5.5R10P5.10-PRO-V6 版本	升级前需要确认下防火墙的数据盘是否大于 150G（不含），如数据盘大于 150G，请提交工单由云墙工程师协助进行升级。

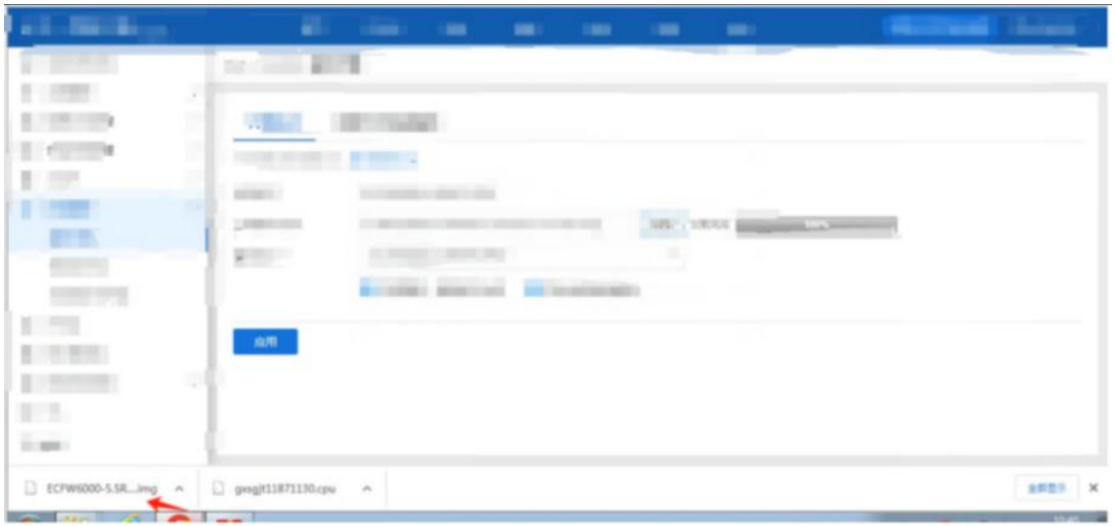
云下一代防火墙版本号	升级流程	注意事项
R9F5 及对应的 PRO 版本	直接升级到 ECFW6000-5.5R10P5.10-PRO 版本	ECFW6000-5.5R10P5.10-PRO 不支持对地址薄的单个地址进行备注，升级前需要确认是否有使用对地址进行备注的功能，如使用请提前删除相应的备注，否则升级后相关地址配置会丢失。
R9F5-V6 及对应的 PRO 版本	直接升级到 ECFW6000-5.5R10P5.10-PRO-V6 版本	ECFW6000-5.5R10P5.10-PRO-v6 不支持对地址薄的单个地址进行备注，升级前需要确认是否有使用对地址进行备注的功能，如使用请提前删除相应的备注，否则升级后相关地址配置会丢失。
R10P3.16 及对应的 PRO 版本	直接升级到 ECFW6000-5.5R10P5.10-PRO 版本	无
R10P3.16 及对应的 PRO 版本	直接升级到 ECFW6000-5.5R10P5.10-PRO-V6 版本	无
其他版本：如 R6P1.2、R6P2.3、R7P8、R7P9、R7P9.5 及对应 PRO 版本，R6P1.2-v6，R6P2.3-v6，R7P8，R7P9，R7P9.5 及对应 PRO 版本升级流程较复杂未提供相应的升级过渡包，请确认好窗口时间后，提前提交工单与云下一代防火墙工程师沟通好操作时间后由防火墙工程师协助升级。		

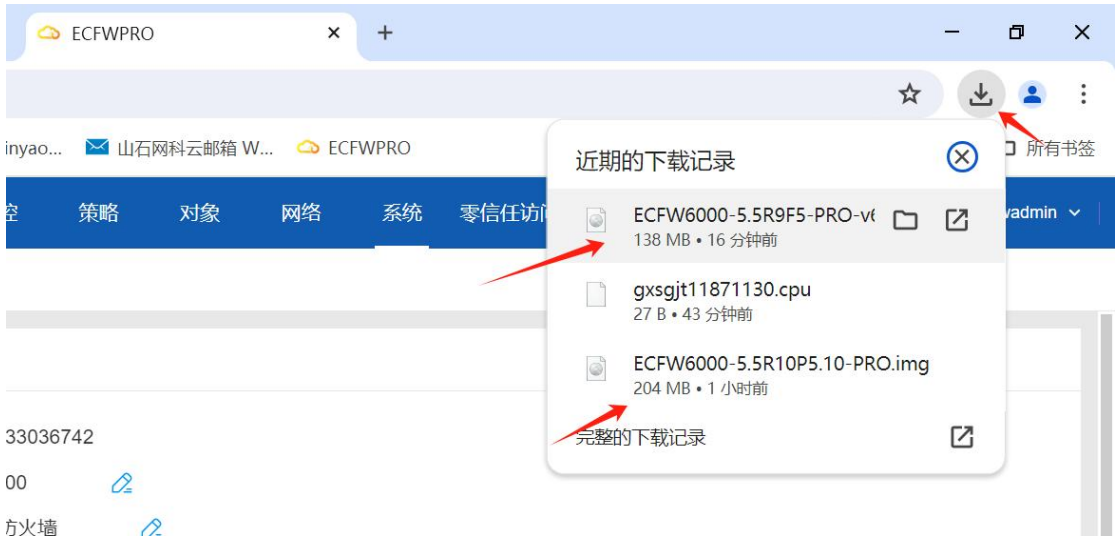
需要下载的升级包，请参见下表：

云下一代防火墙版本号	注意事项
过渡版本-IPV4： ECFW6000-5.5R9F5.1-PRO	https://ecfw.obs.cn-jssz1.ctyun.cn/ECFW6000-5.5R9F5.1-PRO.img
过渡版本-IPV6： ECFW6000-5.5R9F5.1-PRO-v6	https://ecfw.obs.cn-jssz1.ctyun.cn/ECFW6000-5.5R9F5.1-PRO-v6.img

云下一代防火墙版本号	注意事项
最终版本-IPV4	https://ecfw.obs.cn-jssz1.ctyun.cn/ECFW6000-5.5R10P5.10-PRO.img
最终版本-IPV6	https://ecfw.obs.cn-jssz1.ctyun.cn/ECFW6000-5.5R10P5.10-PRO-v6.img

备注：浏览器输入上述链接后可自行下载查看

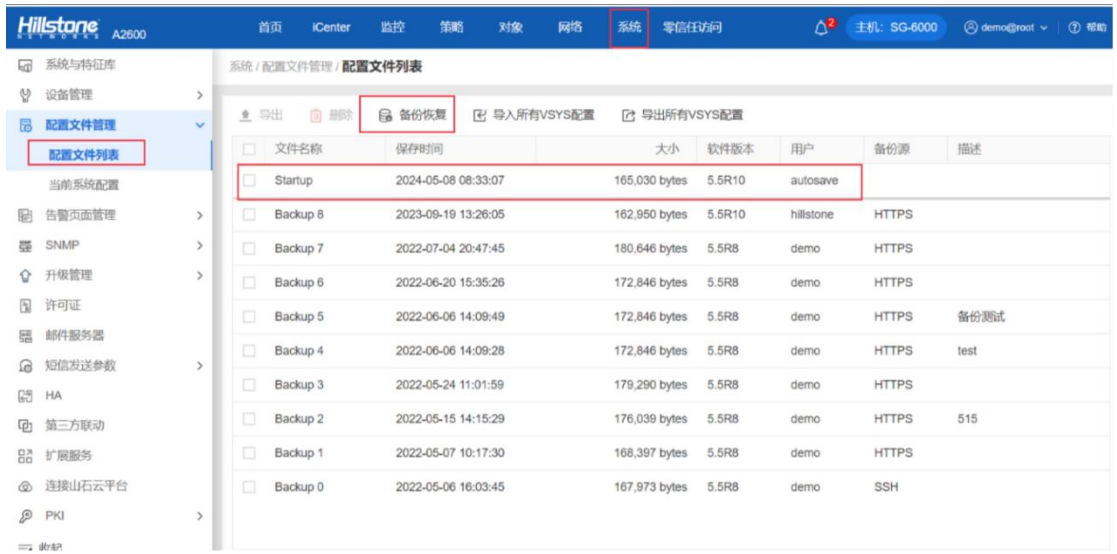




5、 升级前准备工作

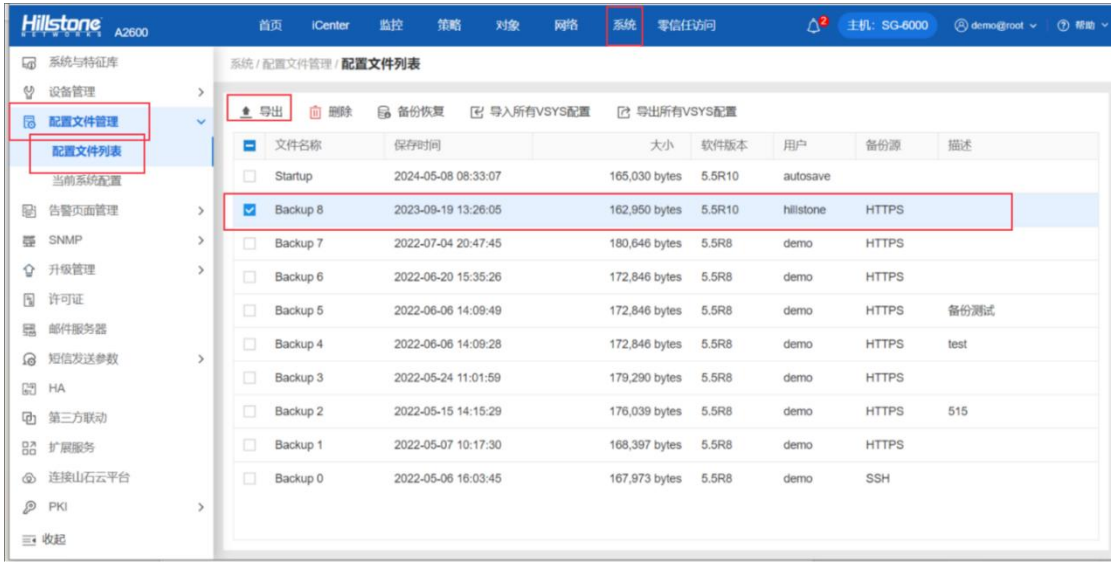
① 登录防火墙的 Web 页面。

进入系统--配置文件管理--配置文件列表--勾选 Startup-点击备份恢复。



输入描述--点击开始备份。

② 勾选生成的配置文件--点击导出。

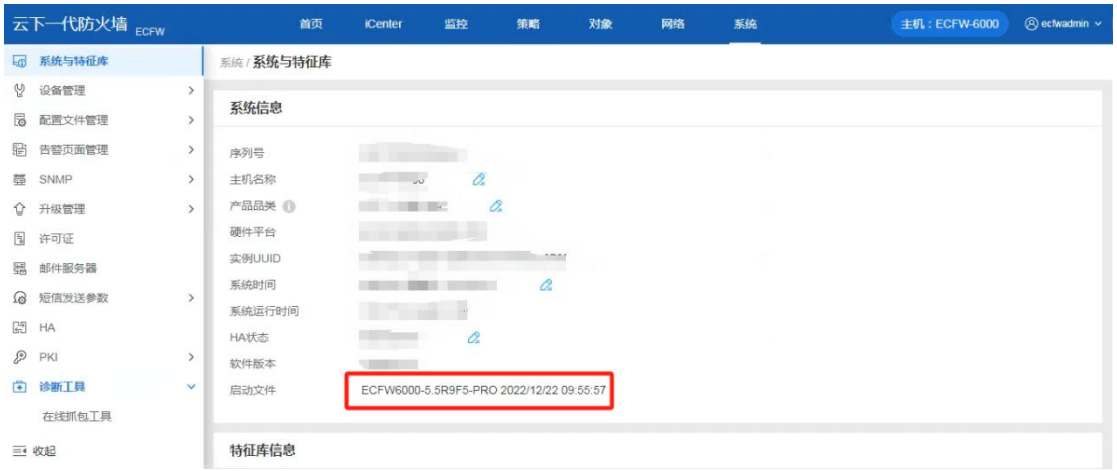


③ 截图保存，系统--系统与特征库-系统信息。

6、 升级步骤

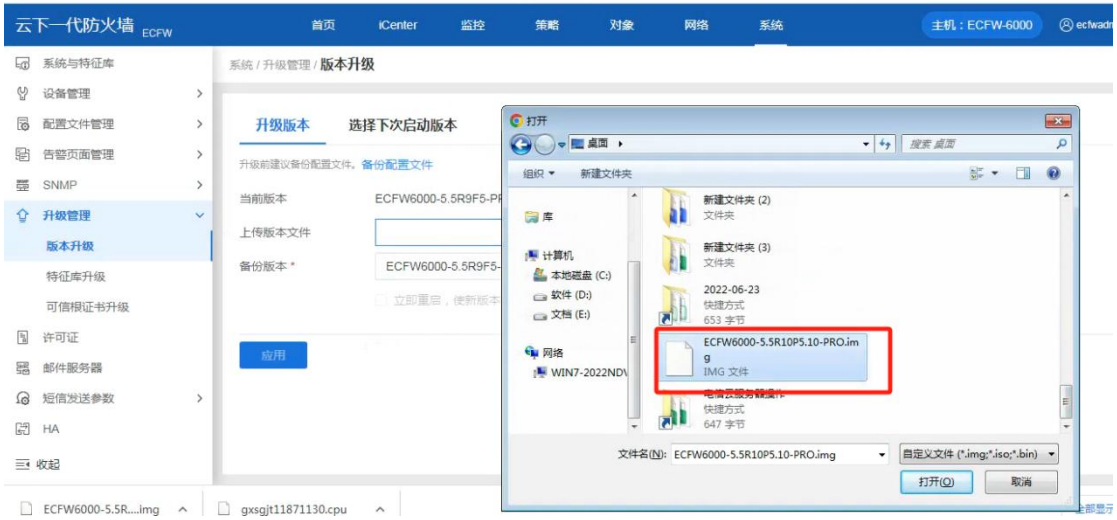
① 打开浏览器，地址栏输入 https://弹性 IP:10443。

② 系统-系统与特征库-查看当前云墙的版本信息。



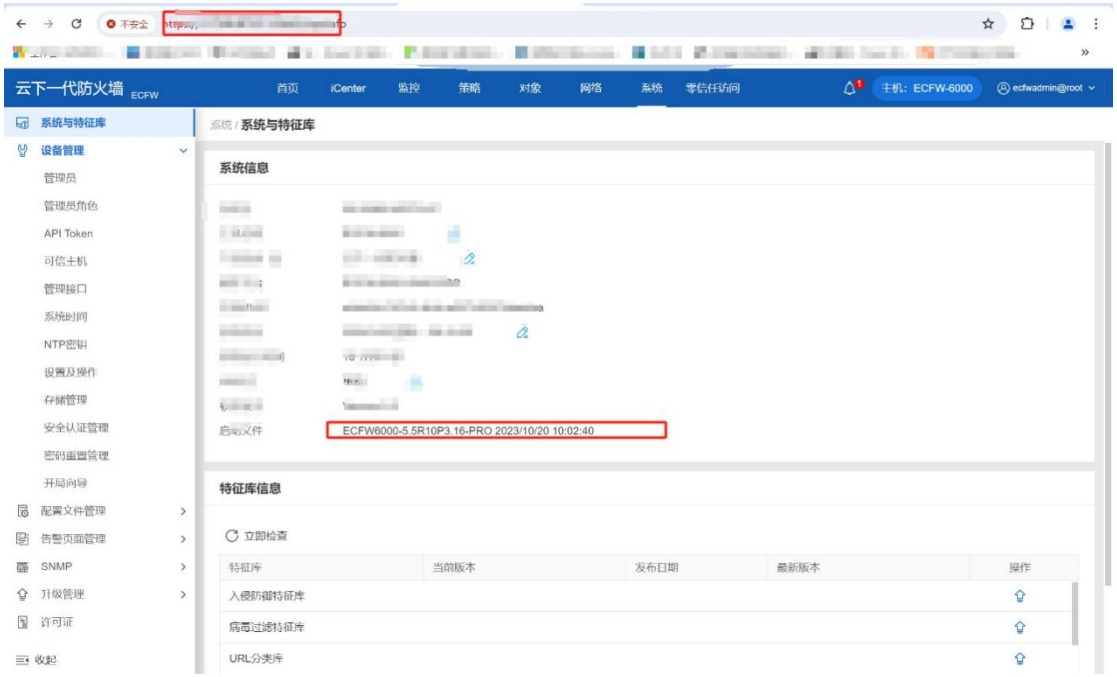
③ 系统-升级管理-版本升级-浏览。

④ 点击浏览-选择对应的版本。



⑤ 勾选立即重启，使新版本生效，点击应用，等待上传版本后自动重启。

⑥ 重启完成后查看版本信息。



7、 升级注意事项

- 本次版本升级过程会对云下一代防火墙进行重启操作，请提前安排好操作时间。
- 本次升级存在较大跨度版本升级，请在升级前做好配置备份，如有操作问题，**可提交工单至云下一代防火墙**，由专人进行指导操作。
- 云墙主备模式部署时，先升级备机，待备机升级成功并重启完成后再升级主机。

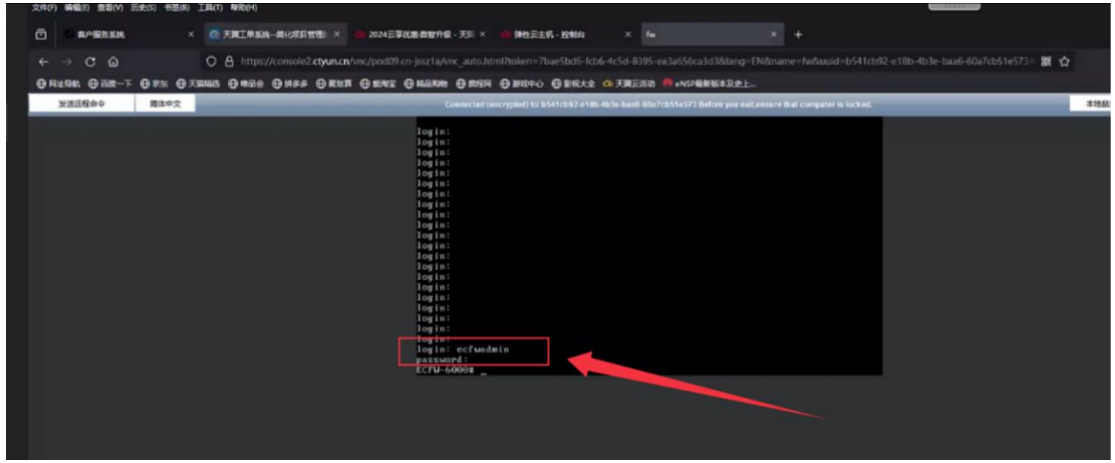
8、 历史版本升级后如何开启 Web 登录权限

因为最新 5.5R10P5.10 的版本屏蔽了账号的 Web 登录权限。2023 年 11 月 8 日前开通的防火墙实例升级完成后使用账号密码登录时会出现如下报错，此为正常现象。

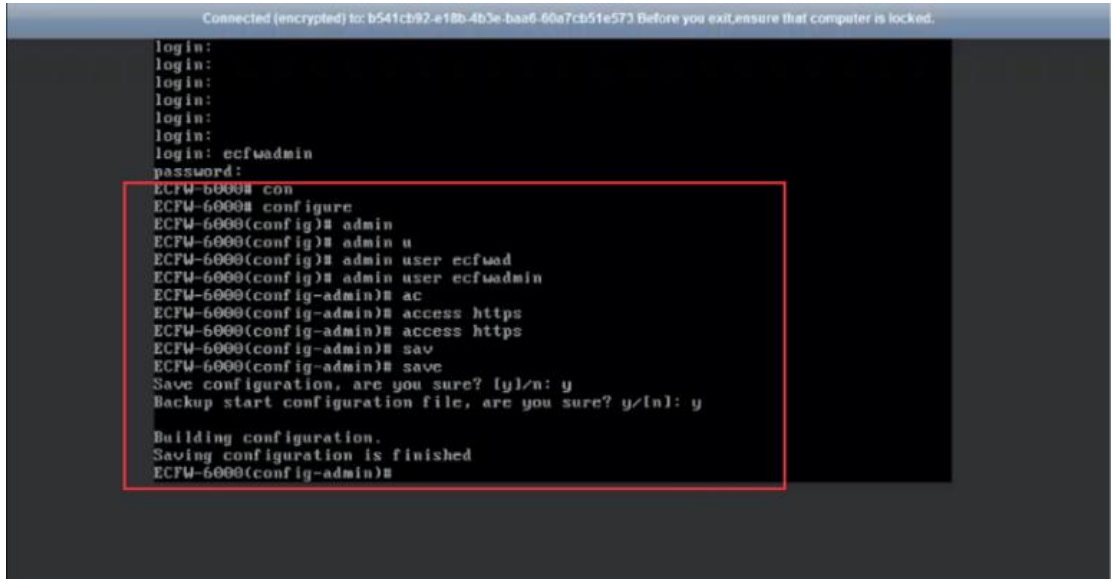
2023 年 11 月 8 日后开通的防火墙实例可以在天翼云控制台--云下一代防火墙的页面点击配置直接跳转进入防火墙管理页面，无法登录的情况可以通过如下方式来放行登录权限。

① 登录天翼云平台，找到防火墙的云主机，点击“远程登录”。

② 点击后会进入 console 界面，输入管理员账号的账号密码（账号密码同 Web 页面一样）。

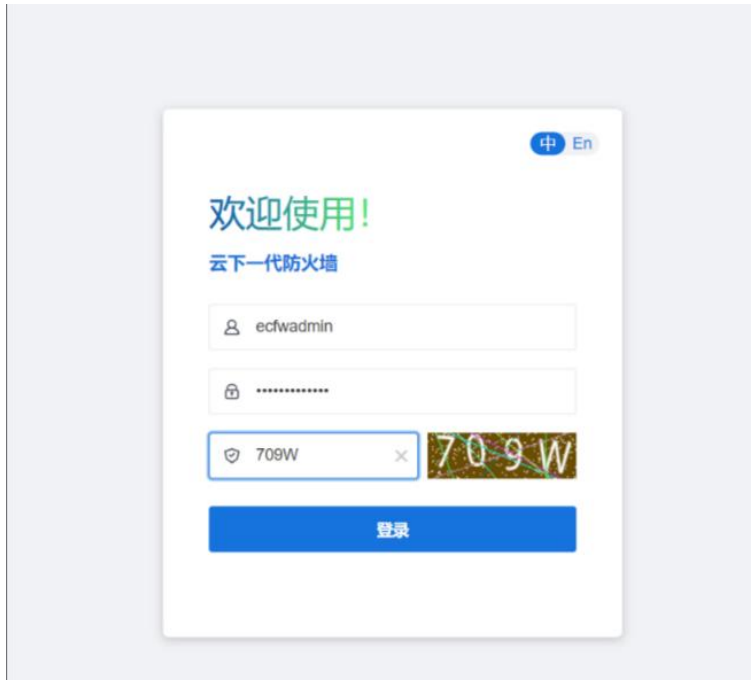


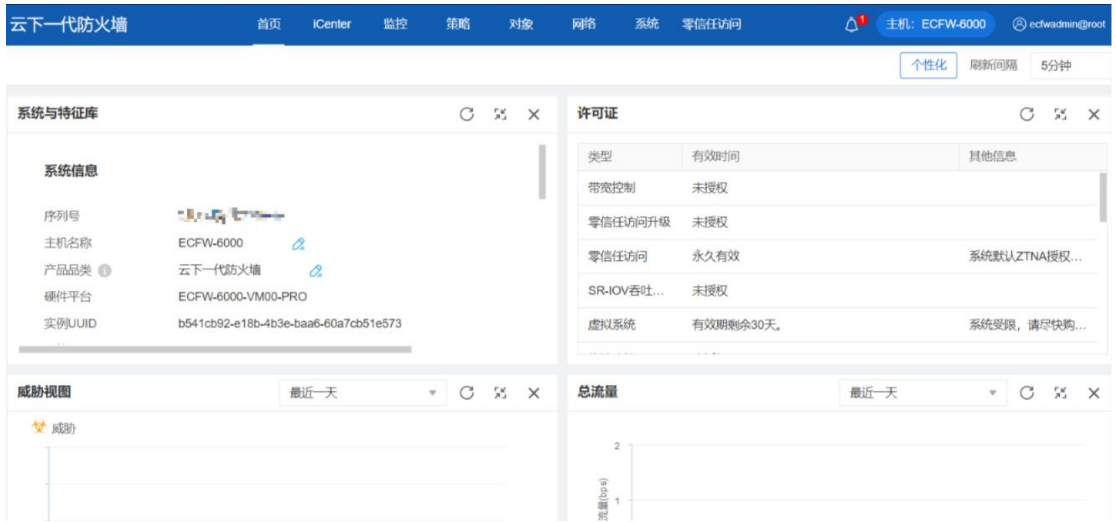
③ 输入如下命令，开通 Web 登录权限。




```
configure            //注：进入配置模式
admin user xxxxxxxxx     //注：xxxxxxxxx 为需要放行 WEB 登录权限的账号
access https          //注：放行登录 https 权限
save               //注：保存配置
y
y
```

④ 进入 Web 页面重新登录。





9、产品使用安全建议

- 将对应型号云墙产品升级到推荐的最新版本 R10P5.10。
- **账号密码：**部分用户使用旧版本，登录账密使用的是默认账密，建议用户修改默认账户及密码。使用强账号密码。

  修改密码操作：

  登录 Web 界面，右上角 ecfwadmin-修改密码。

输入旧密码，再输入新密码，确认密码，进行密码更新。

- **登录权限：**部分用户使用旧版本或进行远程运维，强制开启云墙 SSH 登录权限，存在远程登录风险。

  关闭 SSH 登录权限：

  登录 Web 界面，进入【网络】-【接口】-【勾选 ethernet0/0】-【编辑】

  关闭 SSH、Telnet、HTTP 等不安全协议。