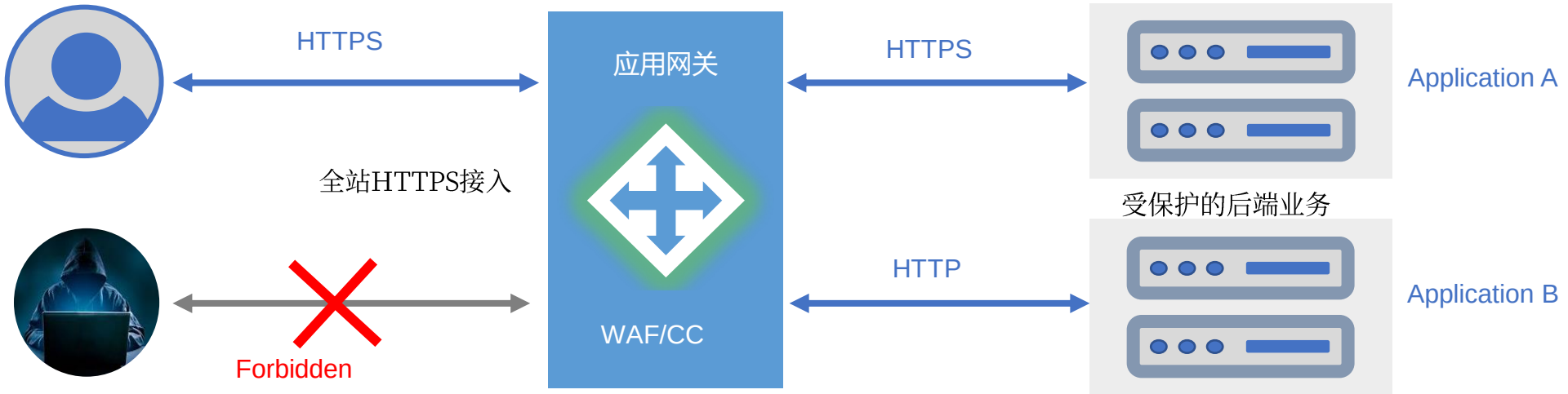
JANUSEC应用网关配置指导

应用网关提供快捷、安全的应用发布

【配置场景举例】：

- 后台业务运行地址： 192.168.100.110（8081端口），Nginx默认网页
- 应用网关运行地址： 192.168.100.110（80和443端口）

该场景中，应用网关和后台业务在同一台服务器上，网关可以使用127.0.0.1:8081访问后台业务。
接下来使用 http://www.example.com 或 https://www.example.com 发布该业务，并拦截恶意访问。

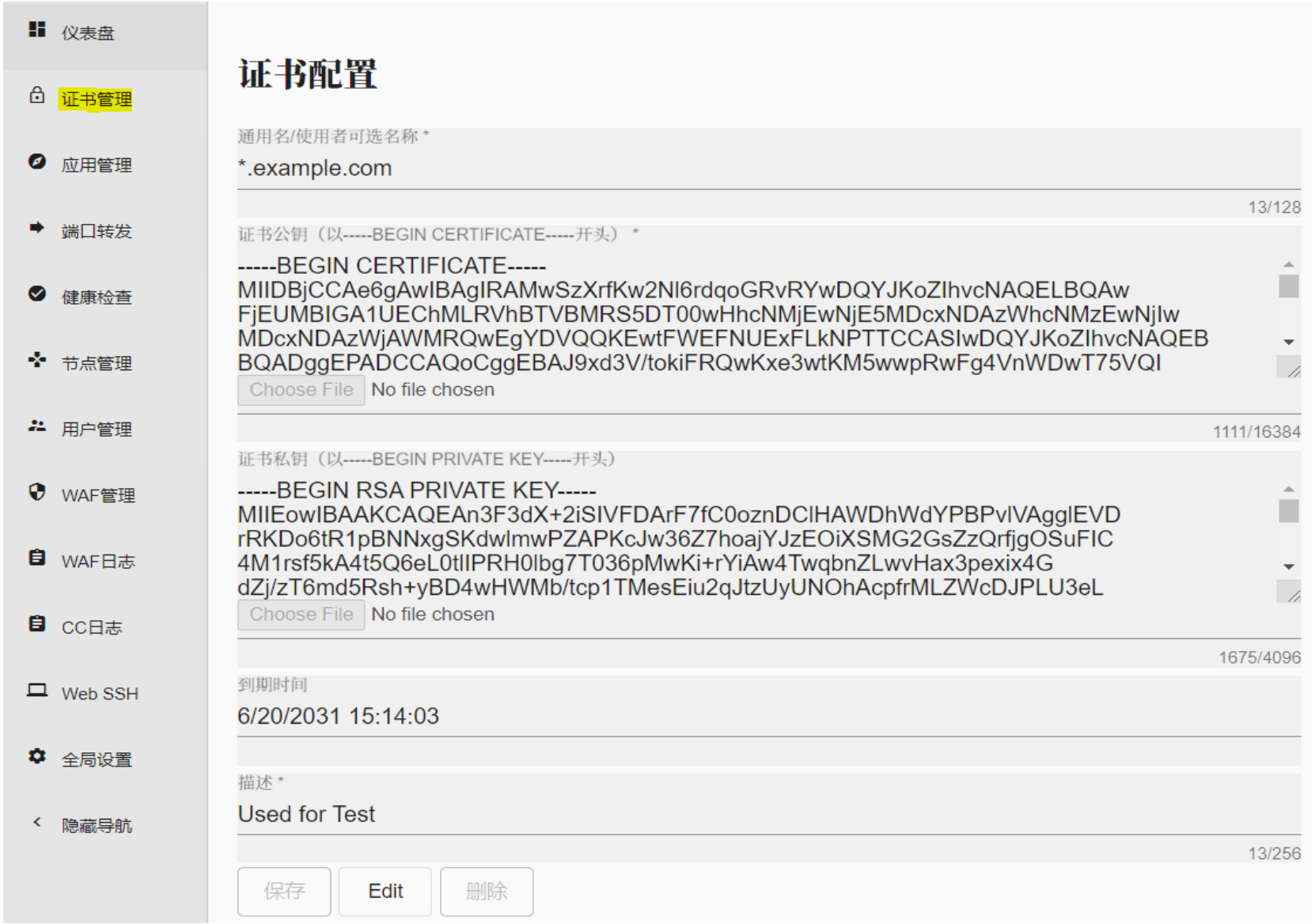


步骤1：登录后台管理界面

使用Chrome浏览器打开地址： http://192.168.100.110:9080/janusec-admin
初始管理账号为： admin / J@nusec123

步骤2：配置数字证书（可选）

数字证书用于配置HTTPS，如果没有购买数字证书或者不使用HTTPS，可跳过该步骤。



- 通用名/使用者可选名称：填写证书适用的域名（www.example.com）或通配型域名（*.example.com）
- 证书公钥：可直接从pem文件导入，或复制文件内容
- 证书私钥：可指导从key文件导入，或复制文件内容
- 到期时间：不用配置，保存后才展示
- 描述：内容不限

步骤3：配置应用（必选）

测试场景使用默认的反向代理模式。

- 应用名称：填写域名或中英文名称均可
- 后端/内部Scheme：默认选择 http

路由配置

- 请求路由：默认为 / （勿轻易修改）；当使用二级目录来扩展子应用（指向不同的后端服务器地址）时，可配置 /abc/ （用户侧URL须含/abc/）；当使用后缀扩展动态应用时，可配置 .php ；优先级从高到低为 /abc/ .php /
- 路由类型：默认为Reverse_Proxy（反向代理），此外还支持FastCGI（如PHP）和静态网站（不需要后端服务器）
- 目标IP:Port：英文半角冒号和端口号不可省
- 后端路由或绝对路径：默认 / 。反向代理模式下，只有前后端路径不一致时才会出现配置 /xyz/ 的情况（网关将/abc/替换为/xyz/）

域名配置

- 域名：www.example.com （没有域名时，可直接配置IP地址）
- 证书：根据需要选用，没有证书时选择ACME自动证书（但HTTPS生效需要域名可从互联网访问到）

步骤3：配置应用（更多设置）

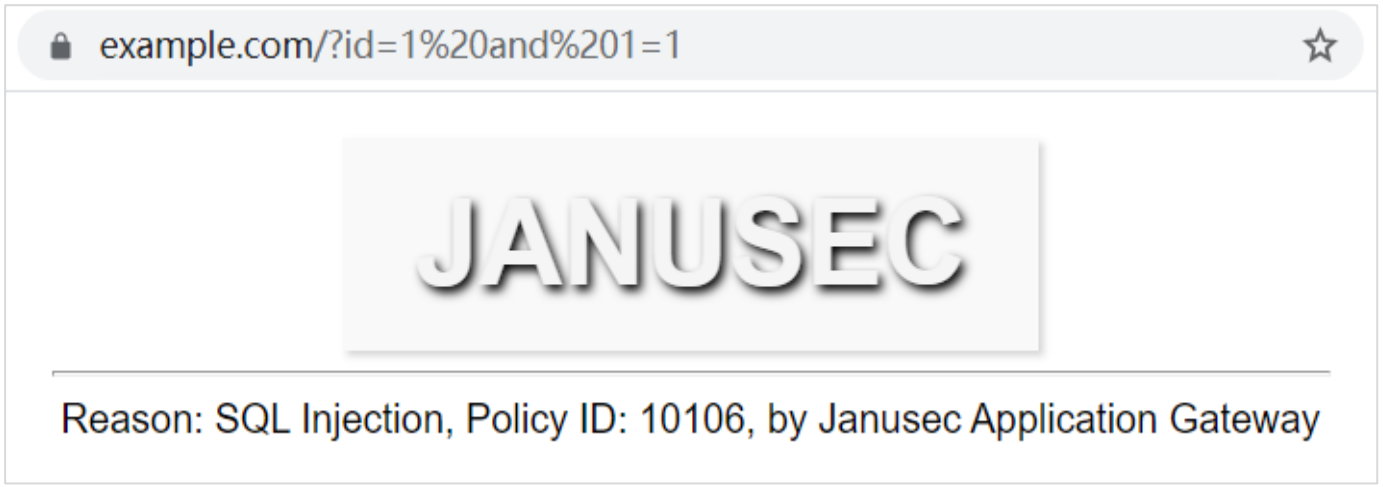
- 用户IP获取方式：默认 REMOTE_ADDR ，当网关流量来自CDN而不是直接来自用户时，根据CDN传递IP的方式调整
- 重定向：如果启用，则http访问时状态码会返回302，重定向到https地址
- HSTS：如果启用，则只使用https，不使用http，建议对安全要求较高的网站启用
- WAF：拦截恶意请求（SQL注入、XSS等）
- 5秒盾：仅限人类访问，强力拦截CC攻击或爬虫工具（影响网站被搜索引擎收录，默认不开启）
- 身份认证：访问应用网站需要先经过身份认证
- CSP：内容安全策略，协助防止跨站脚本攻击
- 应用负责人：默认当前用户
- 描述：内容不限

步骤4：验证访问

- http://www.example.com/

- https://www.example.com/
- 备注：如果使用自签证书测试，可通过点击Chrome浏览器URL地址左侧小锁，证书->详细信息->复制到文件（example.com.cer），双击cer文件导入到“受信任的根证书颁发机构”，重启Chrome浏览器

步骤5：验证WAF（基本配置完成）

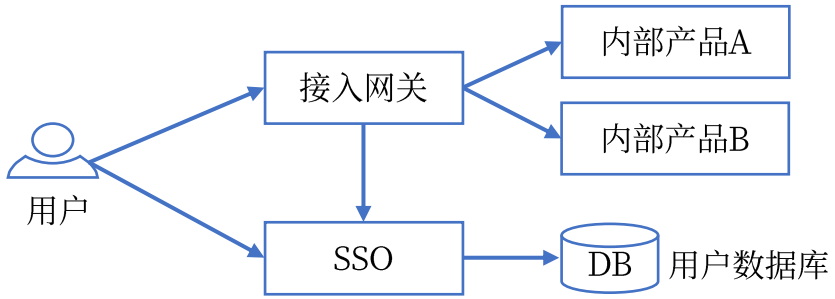


- SQL注入漏洞测试：
- https://www.example.com/?id=1 and 1=1
- 备注：%20为空格字符的编码，手工输入时只需输入空格

- 数据泄露测试
- https://www.example.com/.svn/entries
- 备注： 常见的场景是开发人员发布时连同源码一起发布了，常见的源码目录有 /.svn/ 或 /.git/ 等

FAQ（1）：网关是否支持身份认证?

答：支持。
应用网关支持直接集成身份认证，保护无身份认证的内部应用（需在 全局设置->身份认证 中启用/配置，第三方认证中的配置参见产品手册）。



可选的身份认证机制：

- 企业微信扫码
- 钉钉扫码
- 飞书扫码
- Lark扫码
- LDAP+认证器双因子认证
- CAS 2.0 协议

FAQ（2）：网关是否能够防御CC攻击?

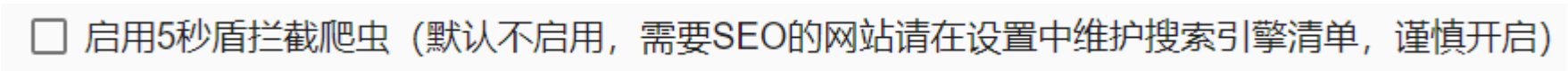
答：可以。
一方面，应用网关可以基于访问频率拦截高频访问请求（设置两道防线，可同时拦截快速、慢速CC攻击）；
另一方面，在应用设置中还可以为每一个应用单独启用5秒盾（强制等待5秒后才能浏览网页，利用工具无法执行JavaScript的特性，仅限人类通过浏览器访问，强力拦截CC攻击或爬虫工具并封禁其IP地址）。

（1）WAF管理 -> 全局CC防护规则：

CC防护参数说明：

- 统计时间窗：默认100毫秒 （对应的第二道防线的时间窗为1500毫秒）
- 最大请求数：一个统计时间窗内同一来源的最大请求数
- 超限锁定：禁止访问的时长，默认900秒（即15分钟）
- 触发动作：默认BLOCK（拦截并与nftables联动封锁IP地址）；还可以选择CAPTCHA（验证码）、旁路等机制

（2）应用管理 -> 应用配置：



FAQ（3）：网关是否支持直接发布静态内容?

答：支持。

假设我们希望使用 /static/ 二级目录来发布静态内容（位于网关服务器的/var/www/html/ 目录下），可以在应用的路由配置中新增一条路由规则

路由配置说明（点击路由规则右侧的加号）：

- 请求路由：/static/
- 路由类型：Static_Website
- 默认文件：index.html （当省略文件名时，默认访问该文件）
- 绝对路径：/var/www/html/

FAQ（4）：能否自行定制网站导航?

答：支持。

当用户使用尚未配置的域名（或直接使用IP地址）访问应用网关时，网关默认会访问 /usr/local/janusec/static/welcome/index.html ；
您可以修改定制该文件，也可以将一个完整的包含其他文件（如脚本/样式/图片）的静态网站放在 /usr/local/janusec/static/welcome/ 目录下面。

Thank you!

https://www.janusec.com/