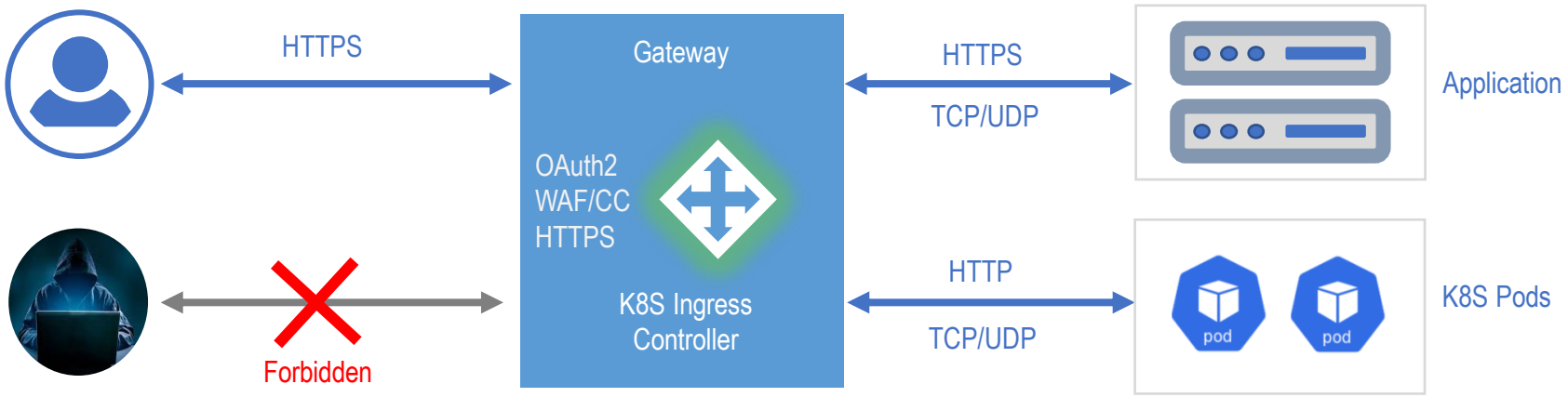
JANUSEC应用网关一体化安全解决方案

JANUSEC应用网关提供快捷、安全的应用发布



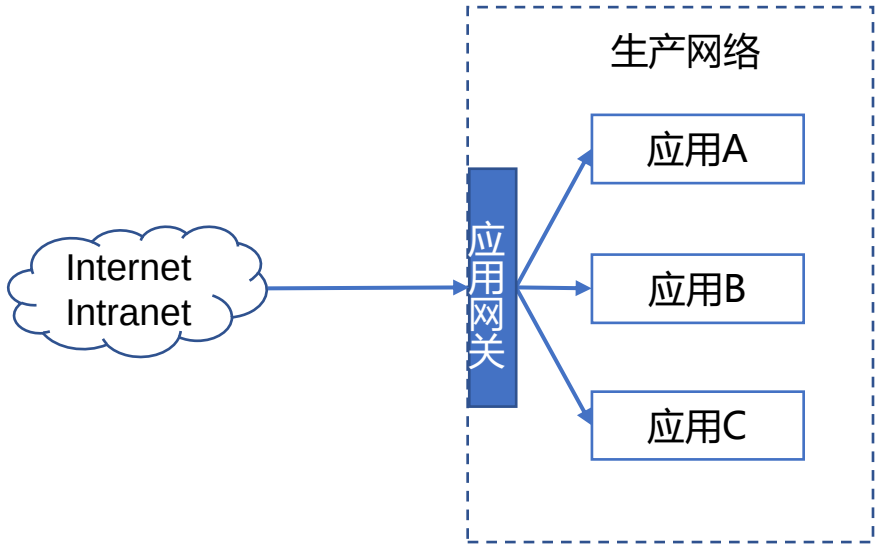
全站HTTPS接入

安全审查（WAF/CC）
安全加持（身份认证）
负载均衡（内容加速）

受保护的后端业务

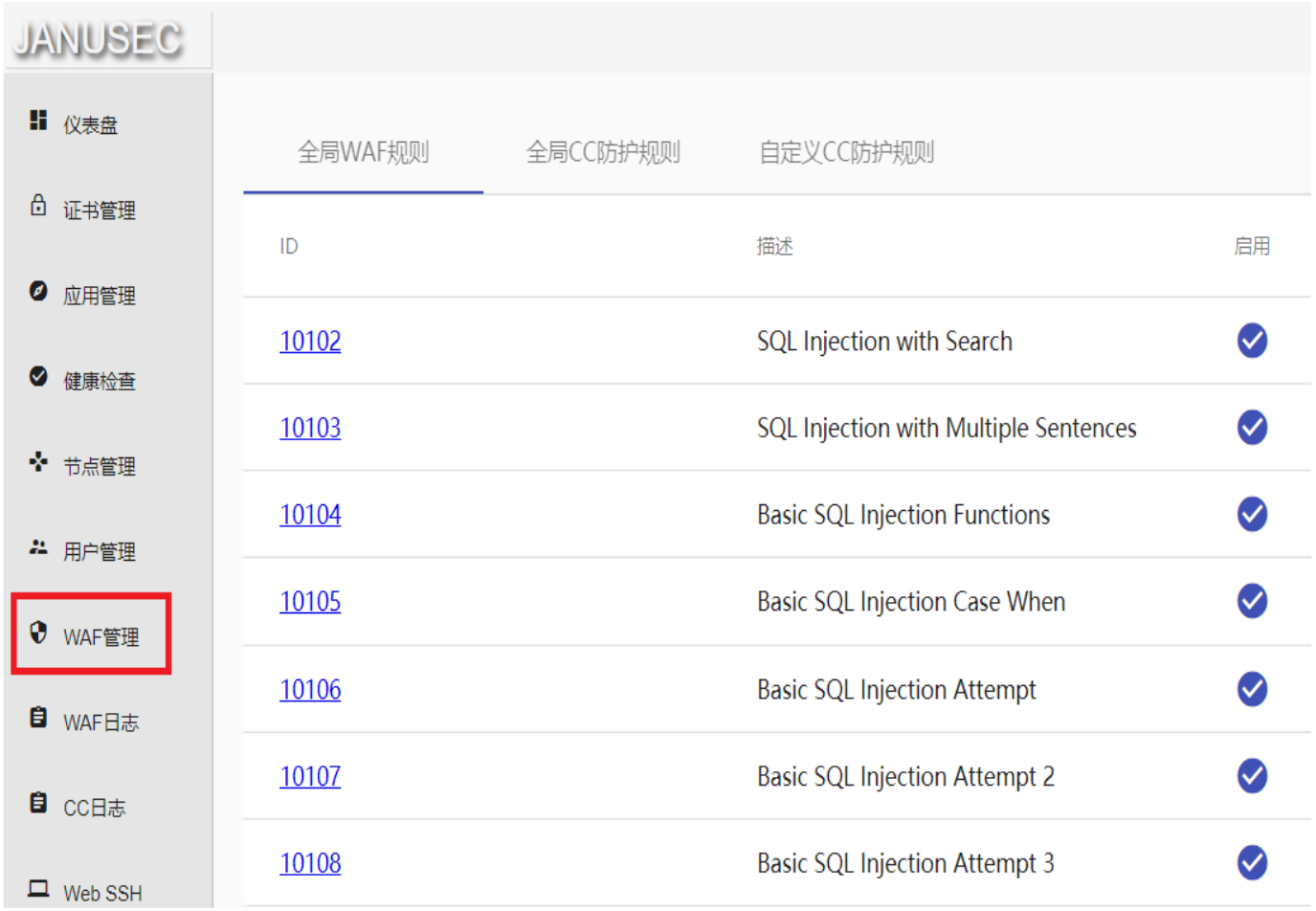
特性1：业务快速发布上线（通过Web界面配置完成）

Web化应用配置

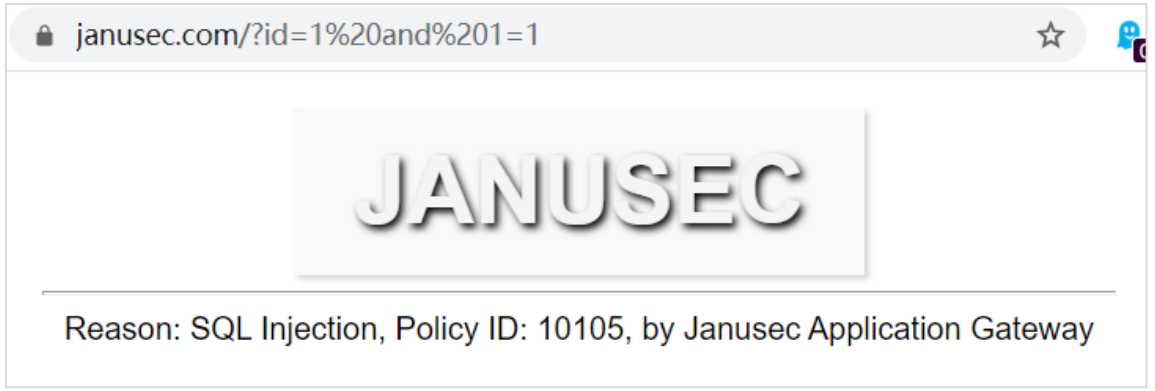


快速发布，提升效率，降低成本

特性2：内置WAF，防黑客入侵



Web化管理WAF规则



效果图：拦截SQL注入

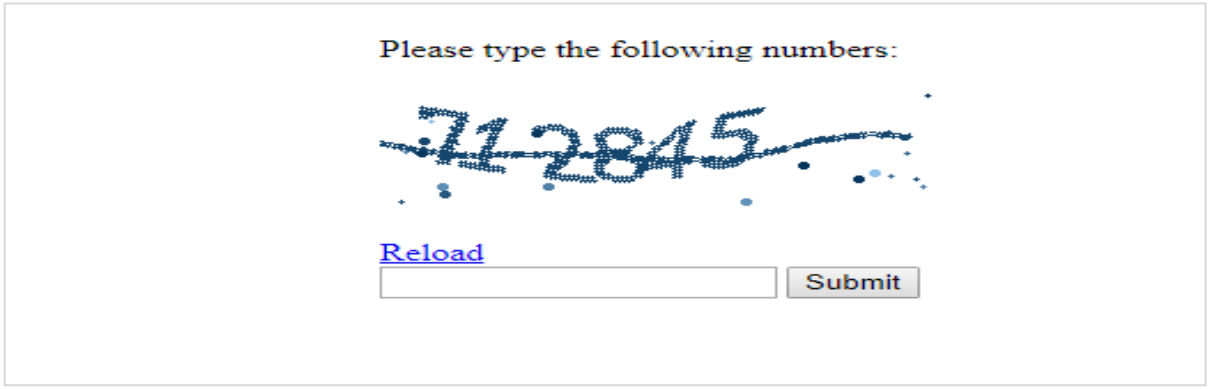
效果图：拦截敏感信息泄露

特性3：内置CC，防黑客攻击，与防火墙或验证码联动

Web化CC规则配置

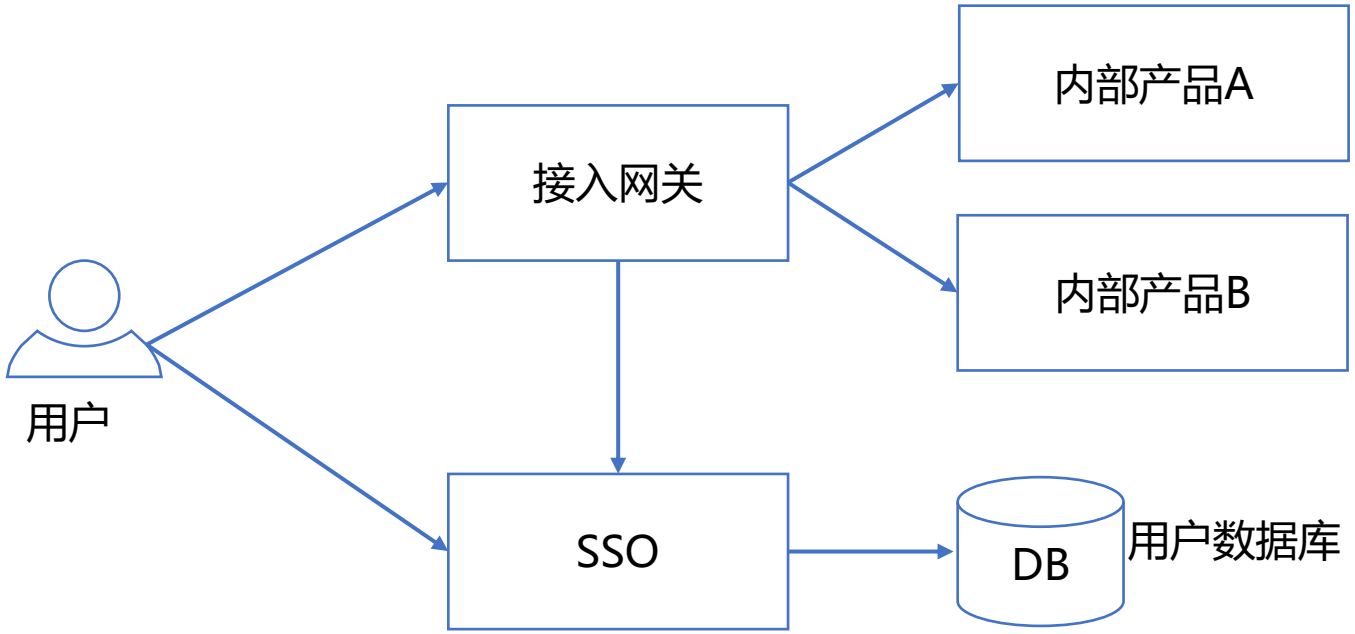
```
[root@CentOS8X ]# nft list ruleset
table inet janusec {
        set blocklist {
                type ipv4_addr
                flags timeout
                elements = { 192.168.100.1 timeout 5m expires 3m50s968ms }
        }

        chain input {
                type filter hook input priority 0; policy accept;
                @nh,96,32 @blocklist drop
        }
}
[root@CentOS8X ]#
```

效果图：主机防火墙nftables生效，攻击IP被封，自动解封



效果图：验证码生效（配置成验证码时）

特性4：身份认证（直接在应用网关上开启，保护无身份认证的内部应用）

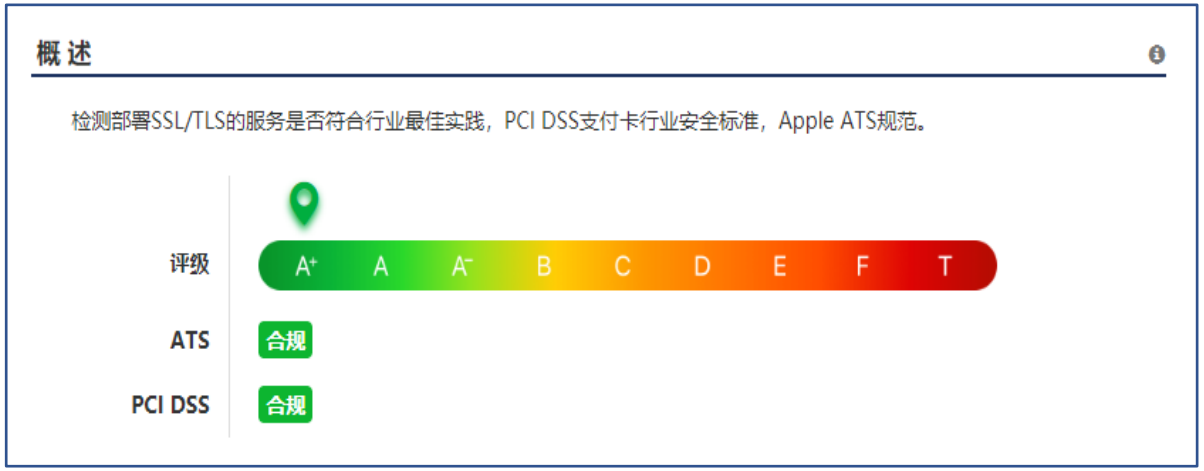


可选的身份认证机制：

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

特性5：全站HTTPS质量保障，私钥统一加密存储

业务不用持有数字证书，下拉选择证书即可

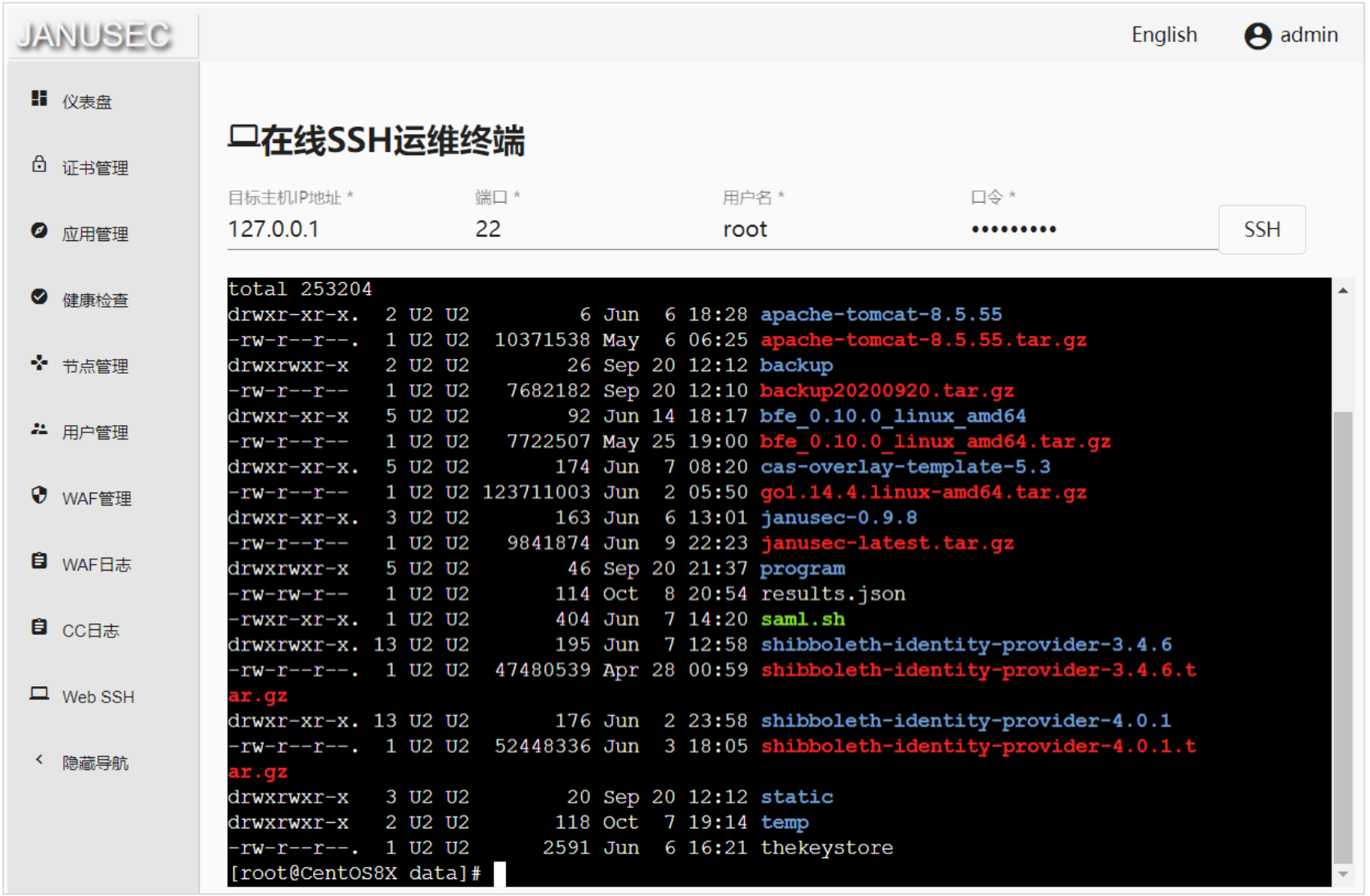


HTTPS安全质量检测结果

网关提供的HTTPS安全保障：

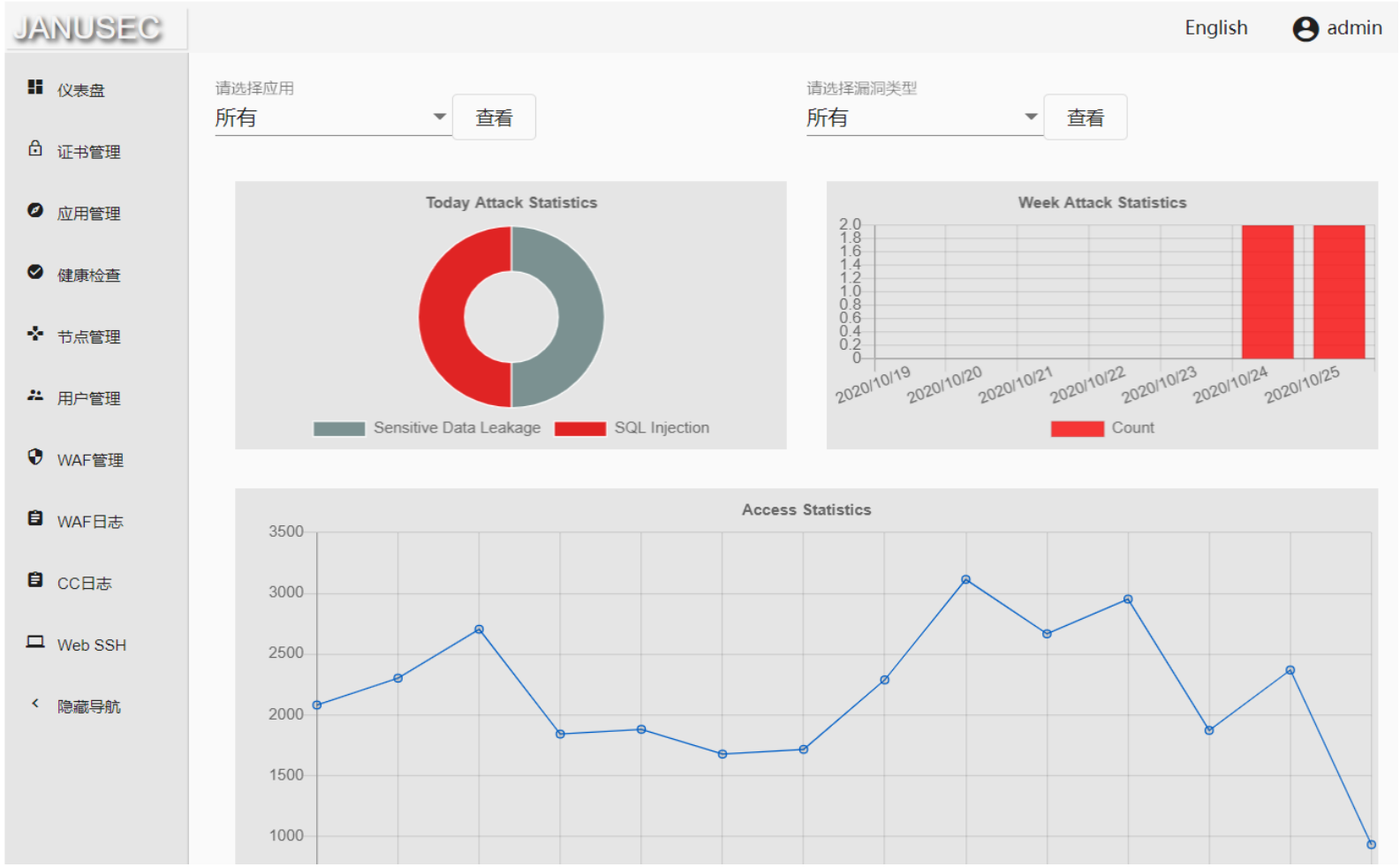
- ❑ 禁用不安全的SSL/TLS版本，使用TLS 1.2或以上版本
- ❑ 选用前向安全算法（主密钥泄露时不影响到历史通信记录的安全）
- ❑ 一键启用HSTS (浏览器默认HTTPS)或自动跳转HTTPS(301跳转)
- ❑ 私钥统一在应用网关加密存储，防止各业务随意存放带来泄露隐患

特性6：内置安全运维通道（基于浏览器，关联员工ID和SSH账号，可审计）



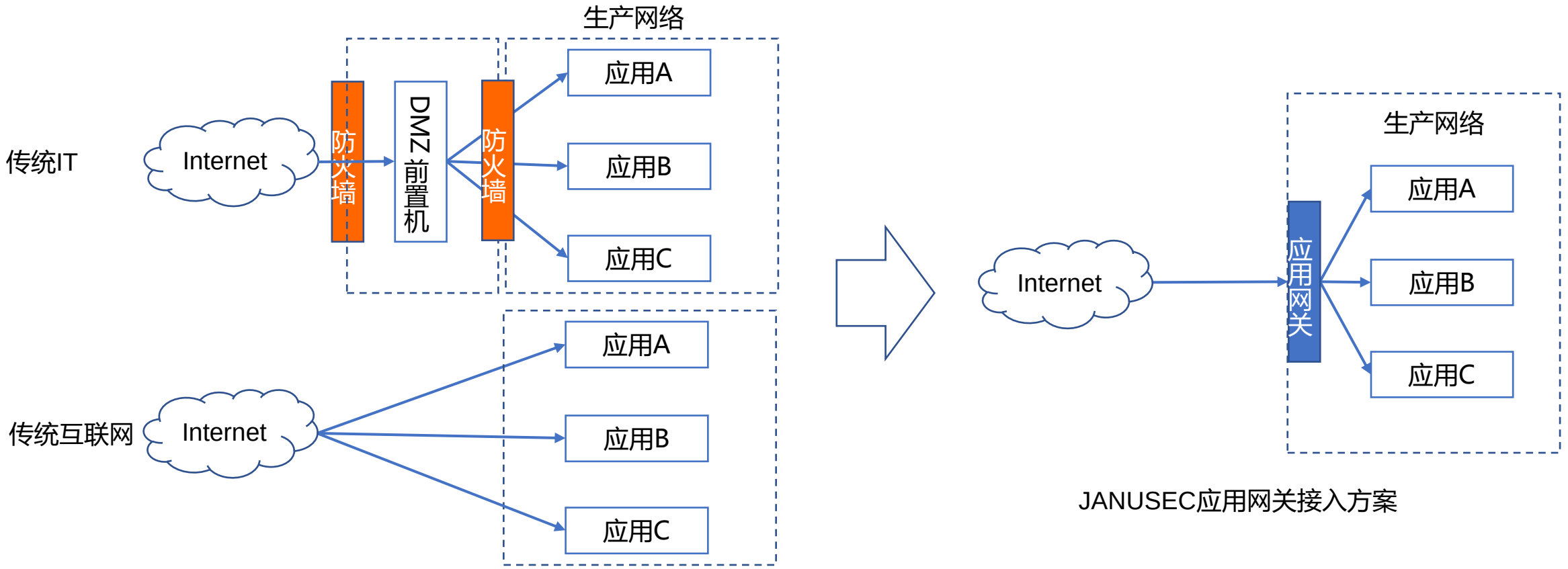
通过浏览器即可登录目标服务器，通道安全可控，日志关联到员工ID

其他特性



- 统计Dashboard
  - WAF拦截统计
  - 访问统计
- 负载均衡
  - 多节点
  - 静态内容加速
- 后端服务器健康检查
  - 自动屏蔽离线服务器
  - 自动检测与恢复转发
- 内容安全策略（CSP）

典型使用场景（1）：简化发布流程与防火墙管理

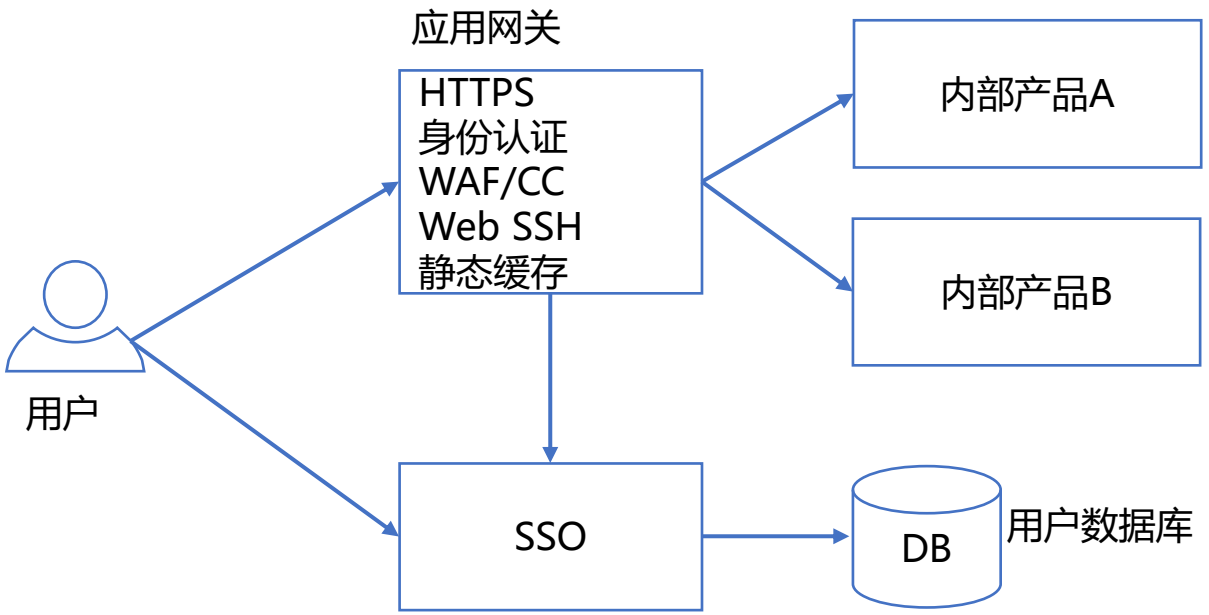


JANUSEC应用网关接入方案

特性	传统IT	传统互联网	JANUSEC应用网关
上线发布	• 前置机物理服务器部署或转发服务器配置	• 服务器通过外网网卡直接对外发布	• 通过Web界面，简单高效
防火墙管理	• 防火墙策略申请	• 不需申请防火墙策略（或需要登记）	• 不需要
预防高危端口	• 较少出现误开高危端口的情况	• 容易出现误开高危端口的情况	• 不会误开高危端口（业务只配置内网网卡）

传统发布模式与JANUSEC发布模式对比

典型使用场景（2）：整合身份认证/HTTPS/安全防御/安全运维/负载均衡



- 适用于企业内部推广全站HTTPS
- 为内部缺乏身份认证机制的业务批量开启身份认证
- 保护业务免受Web入侵&CC攻击
- 提供便捷可审计的安全运维通道
- 提供负载均衡与内容加速（多节点部署）

Thank you!

https://www.janusec.com/