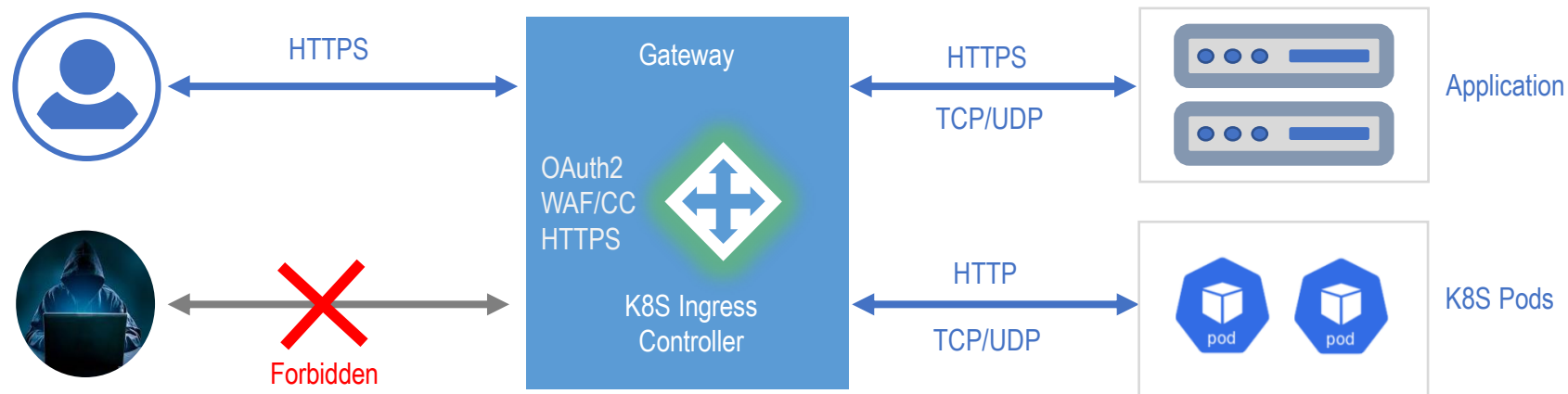


# JANUSEC应用网关一体化安全解决方案

# JANUSEC应用网关提供快捷、安全的应用发布

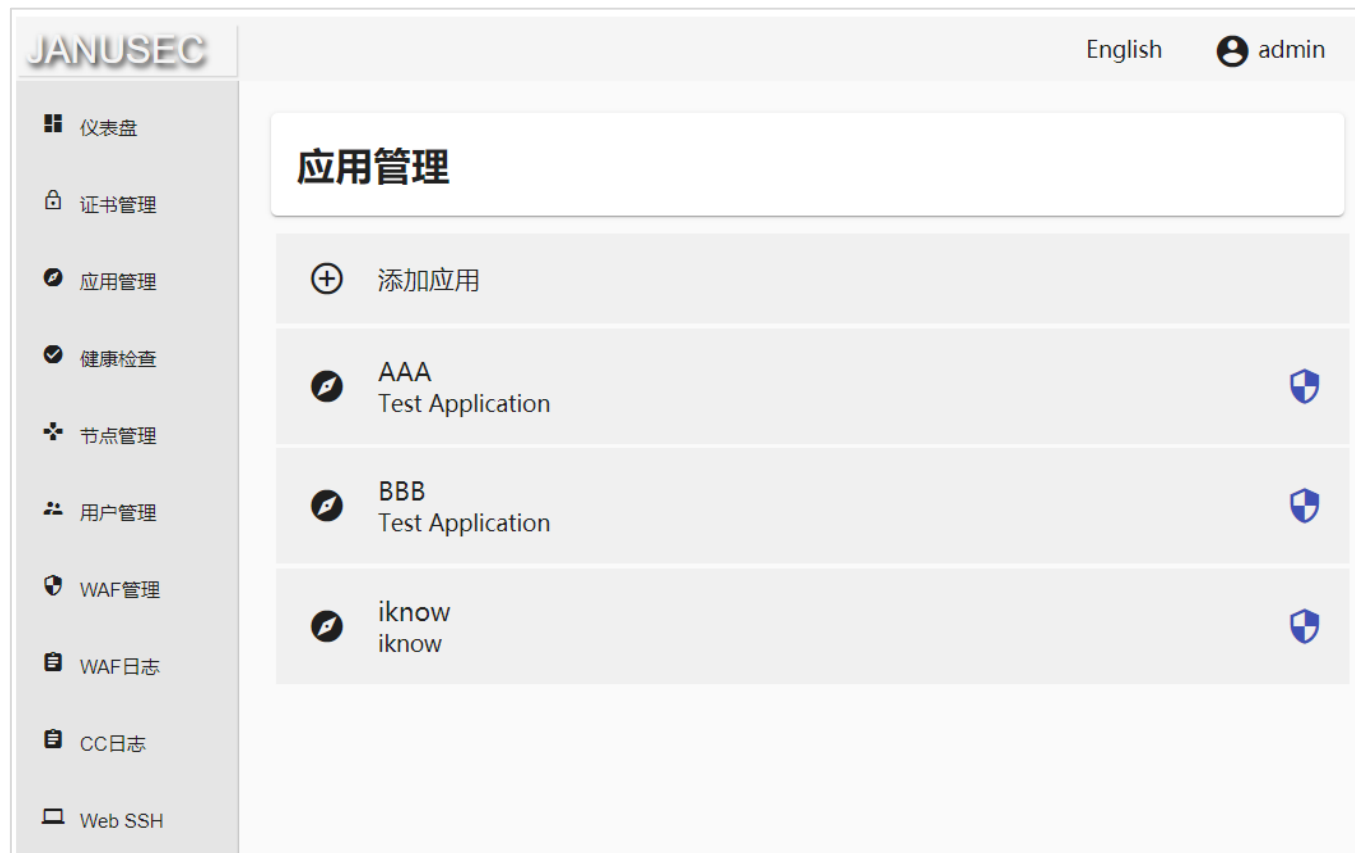


全站HTTPS接入

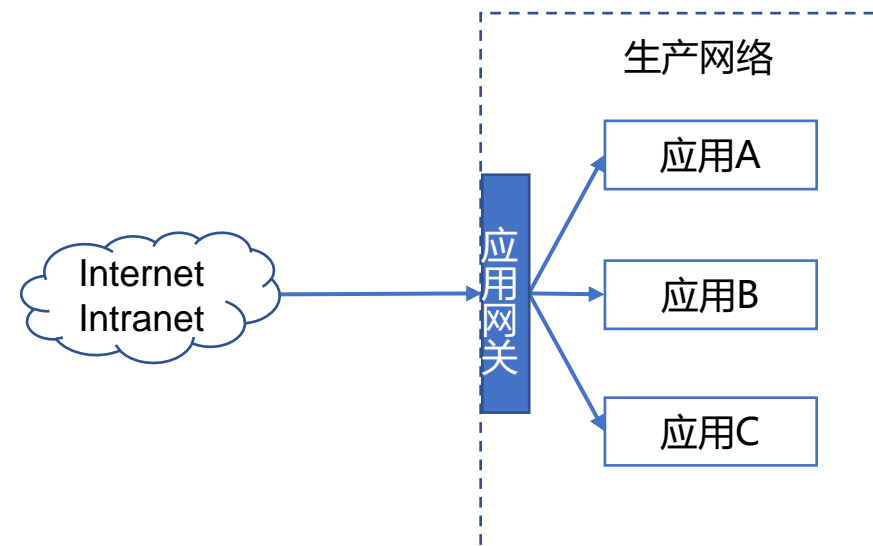
安全审查 (WAF/CC)  
安全加持 (身份认证)  
负载均衡 (内容加速)

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

JANUSEC			
	全局WAF规则	全局CC防护规则	自定义CC防护规则
	ID	描述	启用
<a href="#">10102</a>	SQL Injection with Search	<input checked="" type="checkbox"/>	
<a href="#">10103</a>	SQL Injection with Multiple Sentences	<input checked="" type="checkbox"/>	
<a href="#">10104</a>	Basic SQL Injection Functions	<input checked="" type="checkbox"/>	
<a href="#">10105</a>	Basic SQL Injection Case When	<input checked="" type="checkbox"/>	
<a href="#">10106</a>	Basic SQL Injection Attempt	<input checked="" type="checkbox"/>	
<a href="#">10107</a>	Basic SQL Injection Attempt 2	<input checked="" type="checkbox"/>	
<a href="#">10108</a>	Basic SQL Injection Attempt 3	<input checked="" type="checkbox"/>	

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



The screenshot shows the JANUSEC web interface. The top navigation bar includes the logo 'JANUSEC', the language 'English', and the user 'admin'. The left sidebar contains various management options: 仪表盘, 证书管理, 应用管理, 健康检查, 节点管理, 用户管理, WAF管理, WAF日志, CC日志, and Web SSH. The main content area is titled '全局CC防护规则 (优先级小于自定义规则)'. It features a table with columns for '统计时间窗 (默认100毫秒)', '时间窗内最大请求数量 (默认5...)', '超限锁定秒数 (默认7200)', and '触发动作(阻断/旁路/验证码/放行)'. The table contains one row with values: 100, 5, 300, and BLOCK. Below the table are four checkboxes: '单独统计每个URL地址的访问次数 (默认选中, 当只需要统计无差别的全站访问次数时, 不勾选)', '单独统计每个User-Agent的访问次数 (默认不勾选)', '单独统计每个不同的Cookie串 (默认不勾选, 当Cookie中使用了时间戳或Cookie会经常变化时, 不勾选)', and '启用该规则 (默认选中)'. A '保存' button is located at the bottom left of the configuration area.

统计时间窗 (默认100毫秒) *	时间窗内最大请求数量 (默认5...)	超限锁定秒数 (默认7200) *	触发动作(阻断/旁路/验证码/放行)
100	5	300	BLOCK

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 }
  }

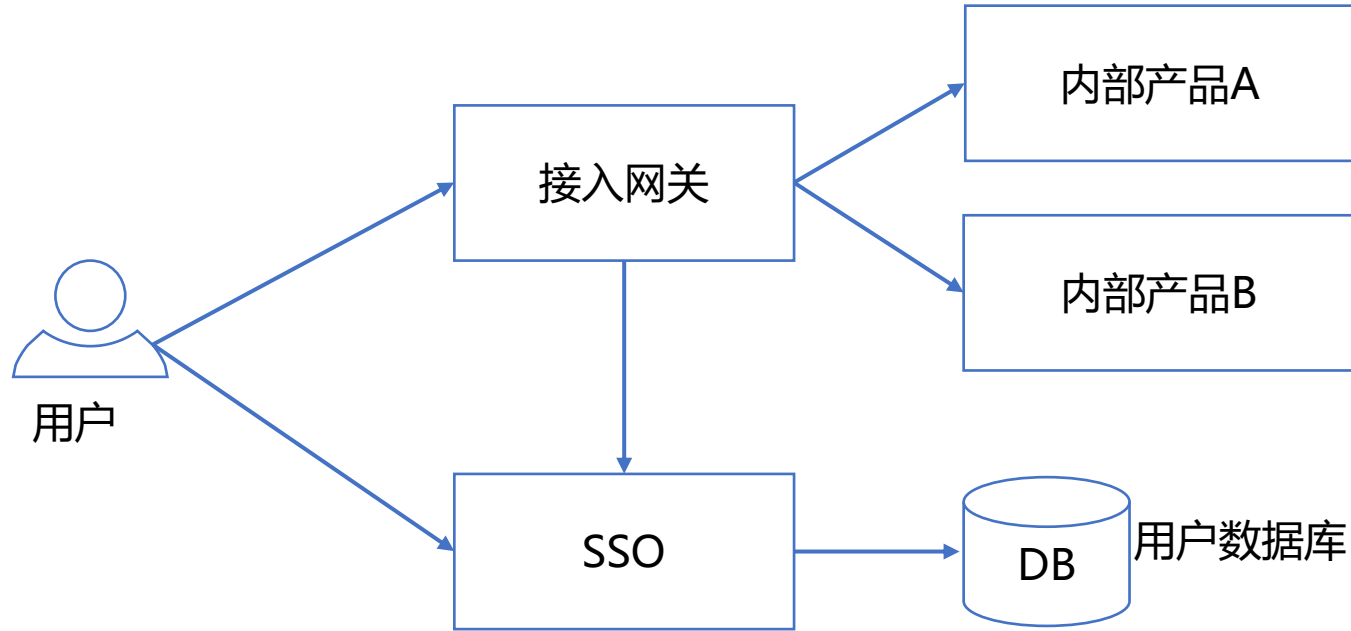
  chain input {
    type filter hook input priority 0; policy accept;
    @nh,96,32 @blocklist drop
  }
}
[root@CentOS8X ~]#
```

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）

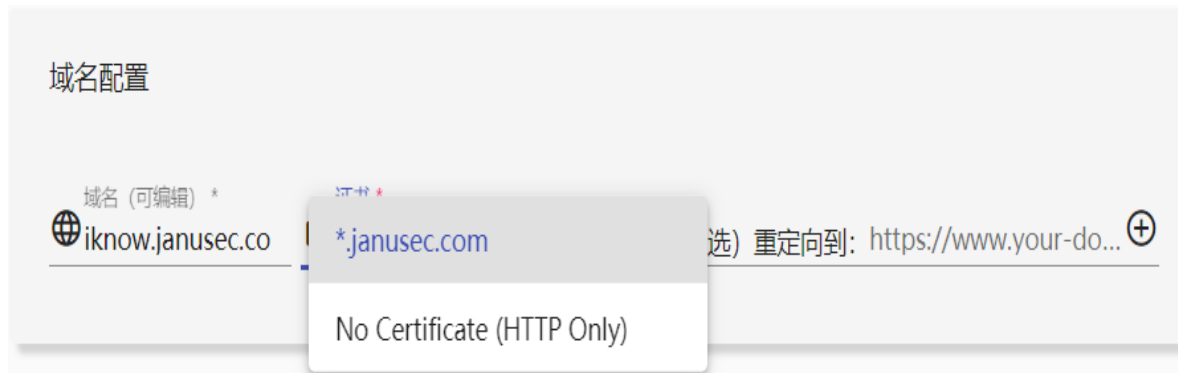
# 特性4：身份认证（直接在应用网关上开启，保护无身份认证的内部应用）



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）

JANUSEC English admin

## 在线SSH运维终端

目标主机IP地址 \* 端口 \* 用户名 \* 口令 \*

127.0.0.1 22 root .....

SSH

```
total 253204
drwxr-xr-x. 2 U2 U2      6 Jun  6 18:28 apache-tomcat-8.5.55
-rw-r--r--. 1 U2 U2    10371538 May  6 06:25 apache-tomcat-8.5.55.tar.gz
drwxrwxr-x 2 U2 U2      26 Sep 20 12:12 backup
-rw-r--r-- 1 U2 U2    7682182 Sep 20 12:10 backup20200920.tar.gz
drwxr-xr-x 5 U2 U2      92 Jun 14 18:17 bfe_0.10.0_linux_amd64
-rw-r--r-- 1 U2 U2    7722507 May 25 19:00 bfe_0.10.0_linux_amd64.tar.gz
drwxr-xr-x 5 U2 U2      174 Jun  7 08:20 cas-overlay-template-5.3
-rw-r--r-- 1 U2 U2   123711003 Jun  2 05:50 go1.14.4_linux-amd64.tar.gz
drwxr-xr-x 3 U2 U2      163 Jun  6 13:01 janusec-0.9.8
-rw-r--r-- 1 U2 U2    9841874 Jun  9 22:23 janusec-latest.tar.gz
drwxrwxr-x 5 U2 U2      46 Sep 20 21:37 program
-rw-rw-r-- 1 U2 U2      114 Oct  8 20:54 results.json
-rwxr-xr-x 1 U2 U2      404 Jun  7 14:20 saml.sh
drwxrwxr-x 13 U2 U2     195 Jun  7 12:58 shibboleth-identity-provider-3.4.6
-rw-r--r-- 1 U2 U2   47480539 Apr 28 00:59 shibboleth-identity-provider-3.4.6.t
ar.gz
drwxr-xr-x 13 U2 U2     176 Jun  2 23:58 shibboleth-identity-provider-4.0.1
-rw-r--r-- 1 U2 U2   52448336 Jun  3 18:05 shibboleth-identity-provider-4.0.1.t
ar.gz
drwxrwxr-x 3 U2 U2      20 Sep 20 12:12 static
drwxrwxr-x 2 U2 U2      118 Oct  7 19:14 temp
-rw-r--r-- 1 U2 U2     2591 Jun  6 16:21 thekeystore
[root@CentOS8X data]#
```

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

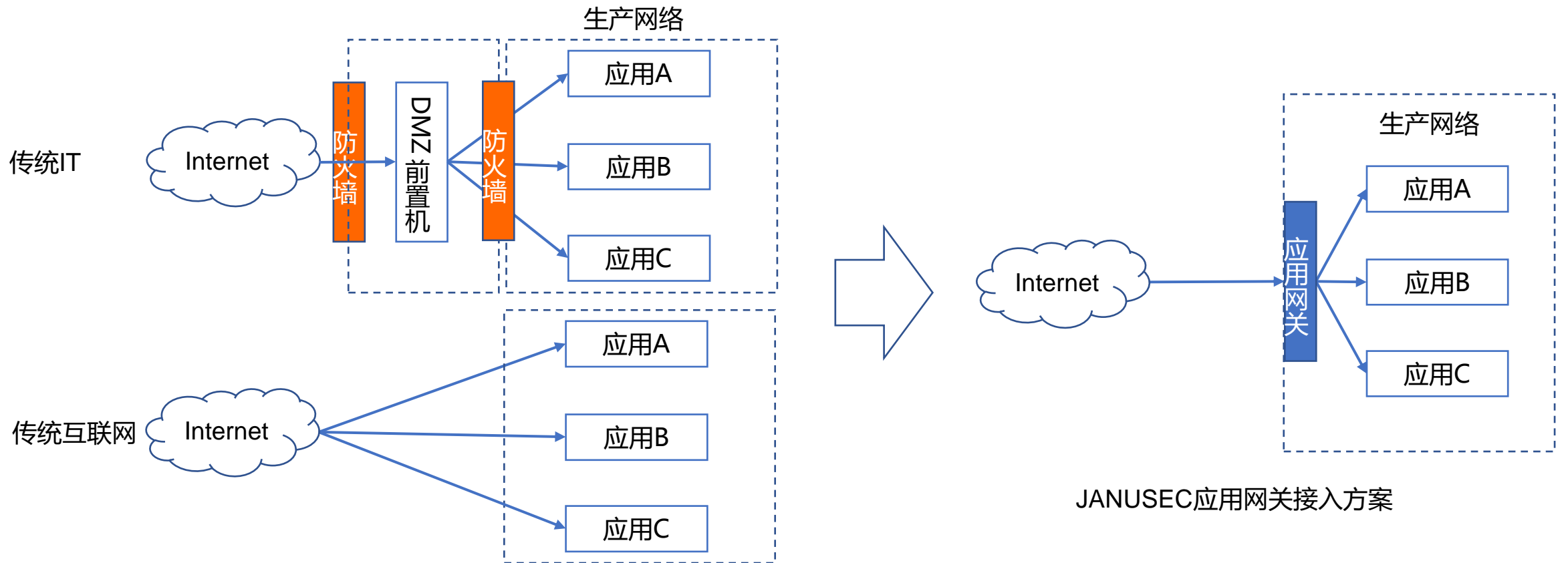
- 多节点
- 静态内容加速

## 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

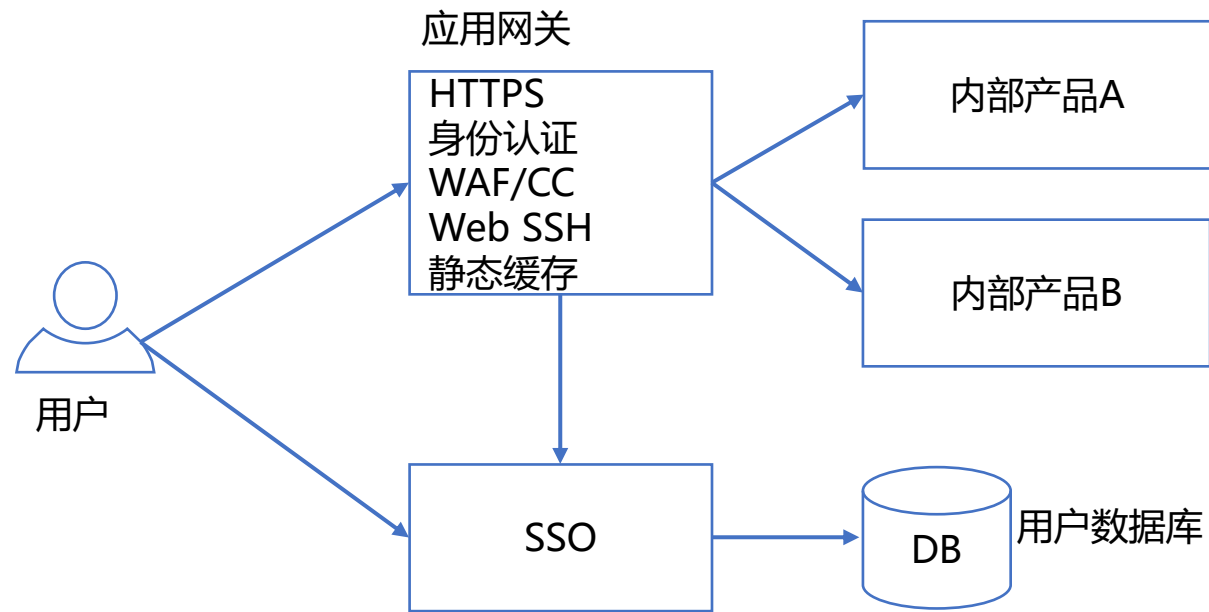


JANUSEC应用网关接入方案

特性	传统IT	传统互联网	JANUSEC应用网关
上线发布	<ul style="list-style-type: none"> <li>前置机物理服务器部署或转发服务器配置</li> </ul>	<ul style="list-style-type: none"> <li>服务器通过外网网卡直接对外发布</li> </ul>	<ul style="list-style-type: none"> <li>通过Web界面，简单高效</li> </ul>
防火墙管理	<ul style="list-style-type: none"> <li>防火墙策略申请</li> </ul>	<ul style="list-style-type: none"> <li>不需申请防火墙策略（或需要登记）</li> </ul>	<ul style="list-style-type: none"> <li>不需要</li> </ul>
预防高危端口	<ul style="list-style-type: none"> <li>较少出现误开高危端口的情况</li> </ul>	<ul style="list-style-type: none"> <li>容易出现误开高危端口的情况</li> </ul>	<ul style="list-style-type: none"> <li>不会误开高危端口（业务只配置内网网卡）</li> </ul>

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/>