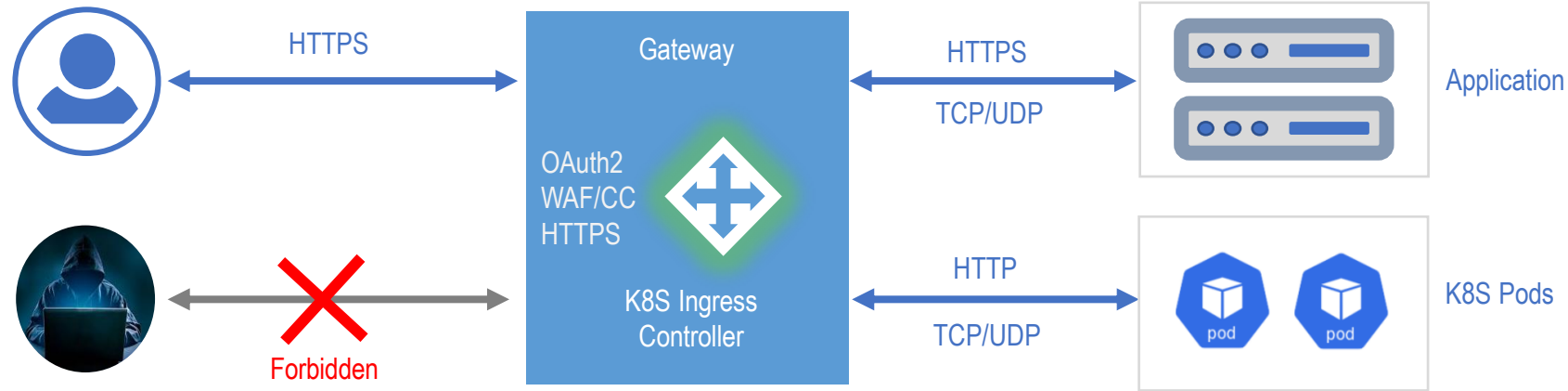


Janusec Application Gateway

©JANUSEC 2023

JANUSEC Provide Fast and Secure Application Delivery

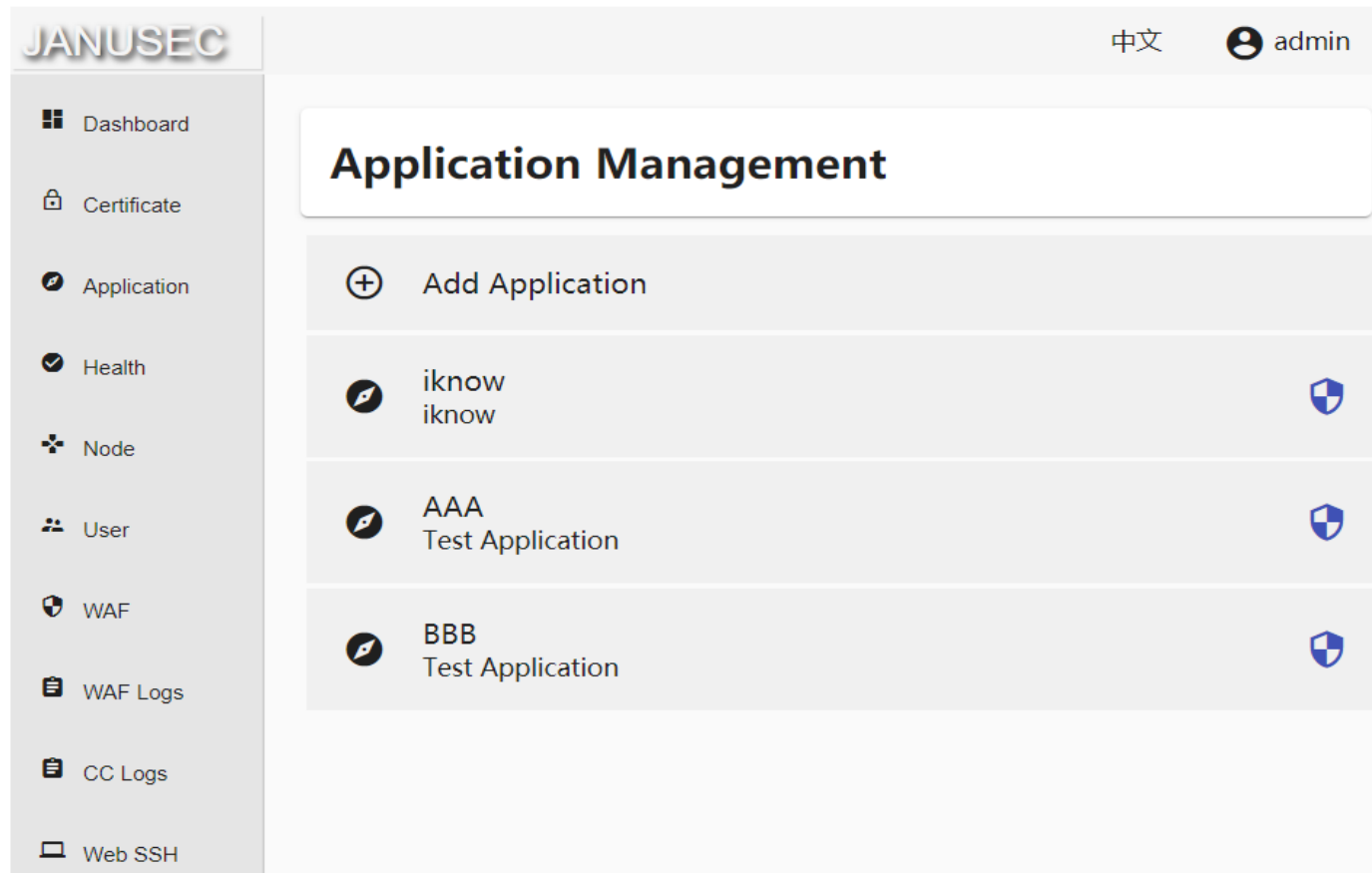


Full HTTPS

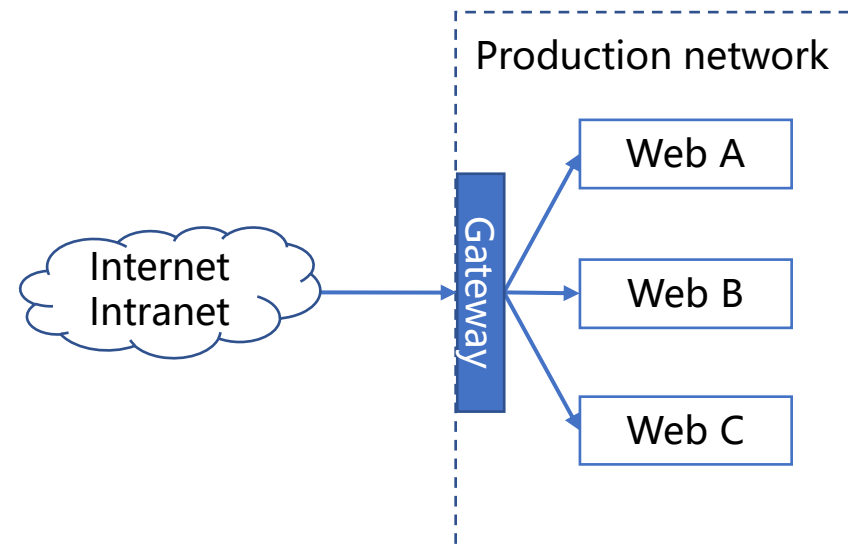
Security Denfense (WAF/CC)
Security Improvement
(Authentication)
Load Balance (Content Acceleration)

Protected
Backend

Feature 1: Fast Delivery (Web UI)

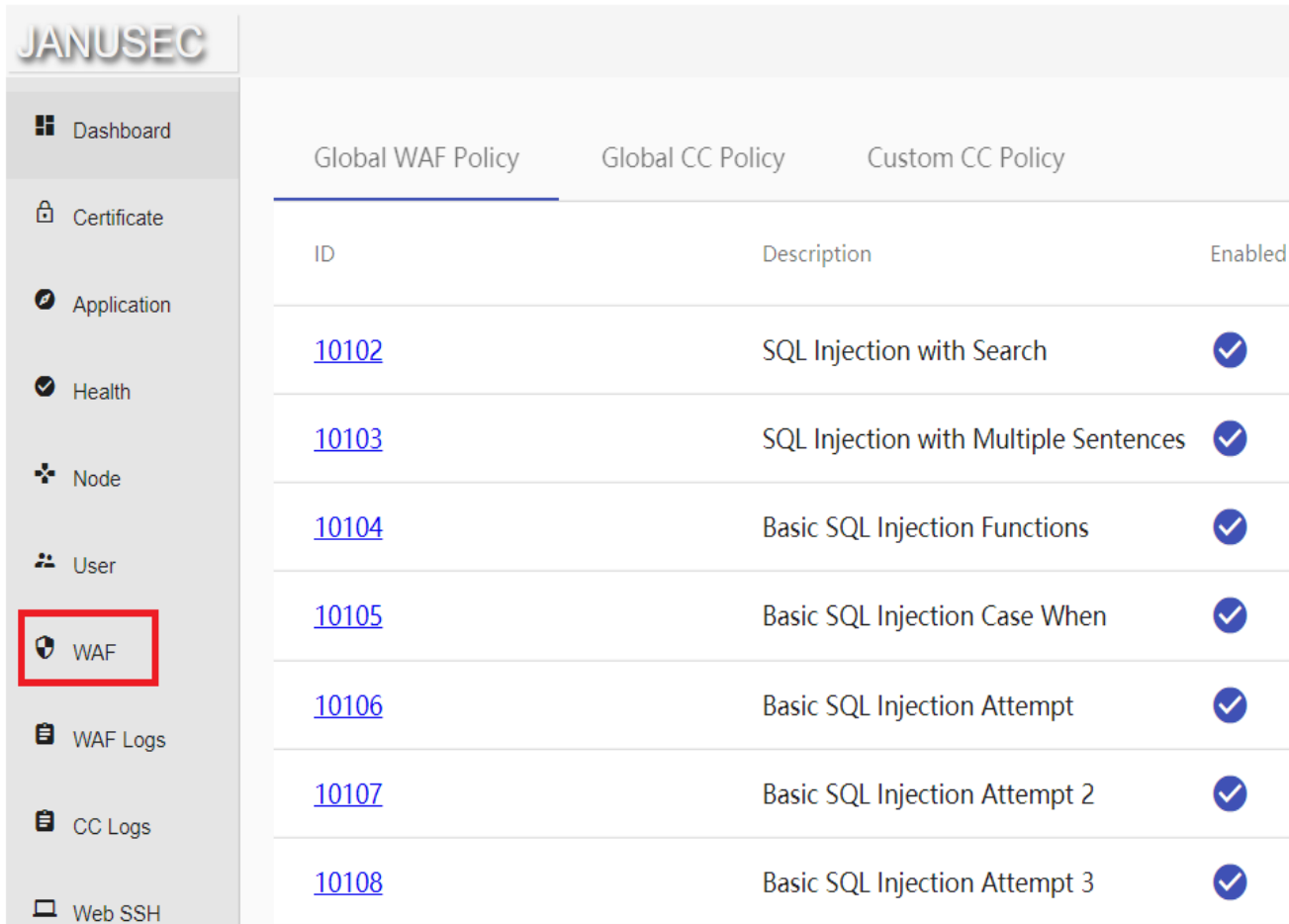


Web-based Configuration UI



Quick release, improve efficiency and reduce costs

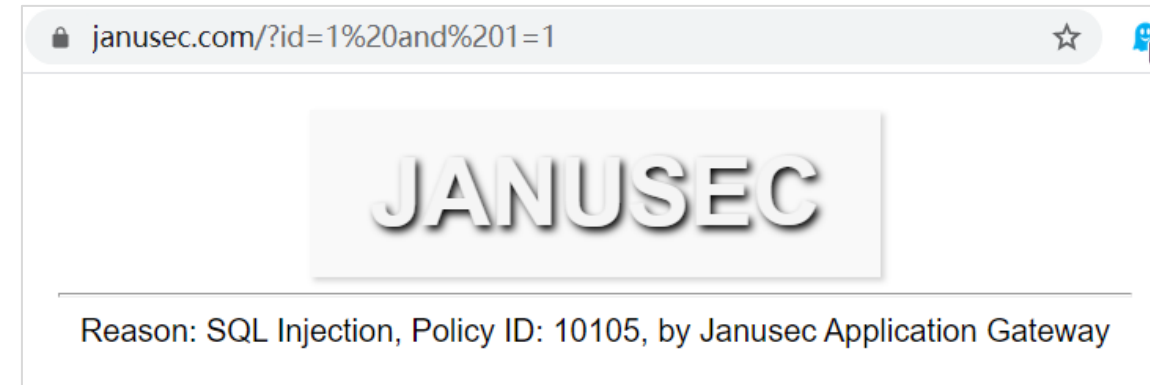
Feature 2: Built-in WAF, anti-hacking



The screenshot shows the JANUSEC management console. On the left is a sidebar with navigation items: Dashboard, Certificate, Application, Health, Node, User, WAF (highlighted with a red box), WAF Logs, CC Logs, and Web SSH. The main content area is titled 'Global WAF Policy' and contains a table of WAF policies.

| ID | Description | Enabled |
|-----------------------|---------------------------------------|---------|
| 10102 | SQL Injection with Search | ✓ |
| 10103 | SQL Injection with Multiple Sentences | ✓ |
| 10104 | Basic SQL Injection Functions | ✓ |
| 10105 | Basic SQL Injection Case When | ✓ |
| 10106 | Basic SQL Injection Attempt | ✓ |
| 10107 | Basic SQL Injection Attempt 2 | ✓ |
| 10108 | Basic SQL Injection Attempt 3 | ✓ |

WAF Policies

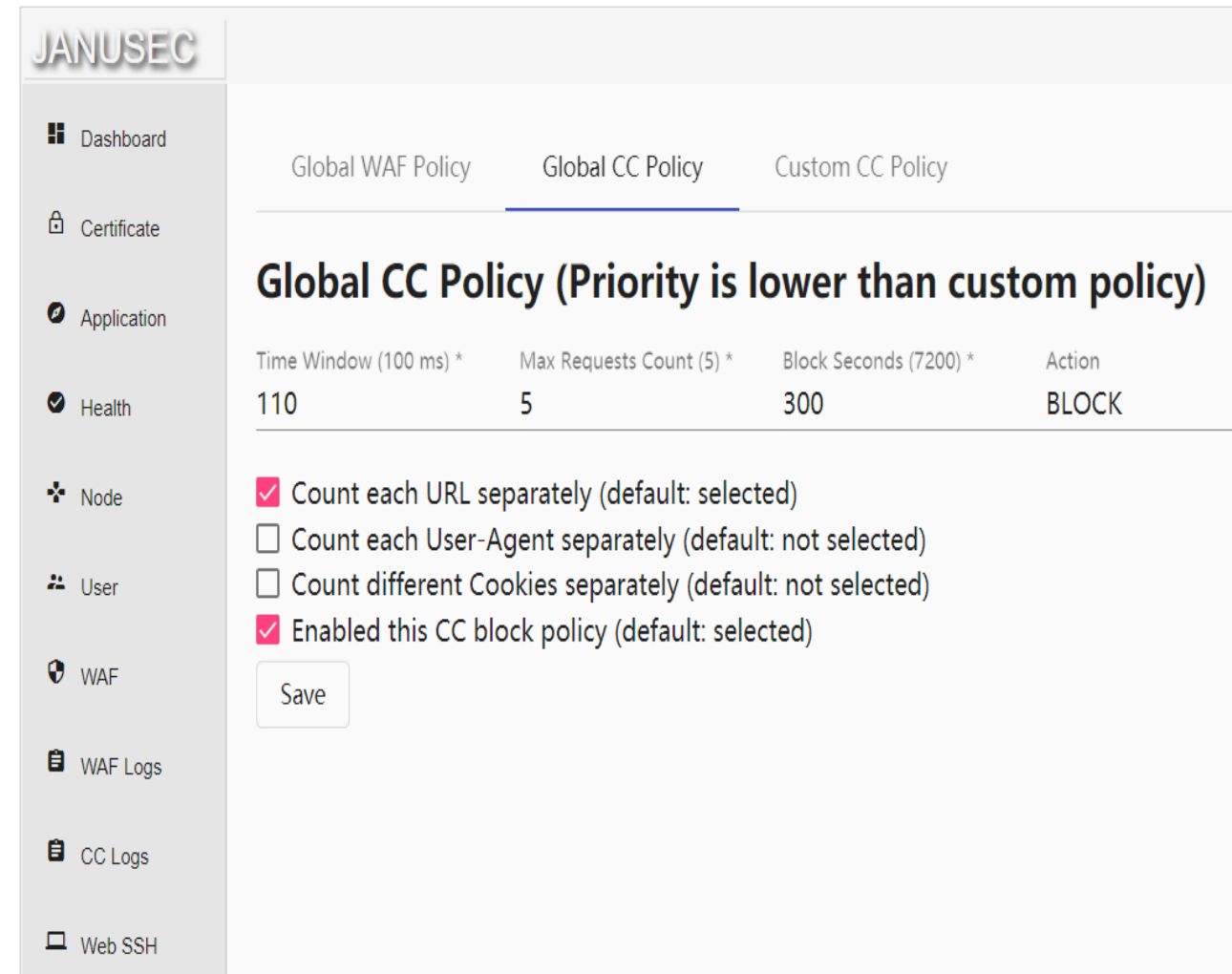


Intercept SQL injection



Intercept Sensitive Information Leakage

Feature 3: Built-in CC, Prevent attacks, link with firewall or CAPTCHA



The screenshot shows the JANUSEC web interface. On the left is a sidebar with navigation items: Dashboard, Certificate, Application, Health, Node, User, WAF, WAF Logs, CC Logs, and Web SSH. The main content area has three tabs: Global WAF Policy, Global CC Policy (selected), and Custom CC Policy. The title is "Global CC Policy (Priority is lower than custom policy)". Below the title is a table with the following data:

| Time Window (100 ms) * | Max Requests Count (5) * | Block Seconds (7200) * | Action |
|------------------------|--------------------------|------------------------|--------|
| 110 | 5 | 300 | BLOCK |

Below the table are four checkboxes:

- Count each URL separately (default: selected)
- Count each User-Agent separately (default: not selected)
- Count different Cookies separately (default: not selected)
- Enabled this CC block policy (default: selected)

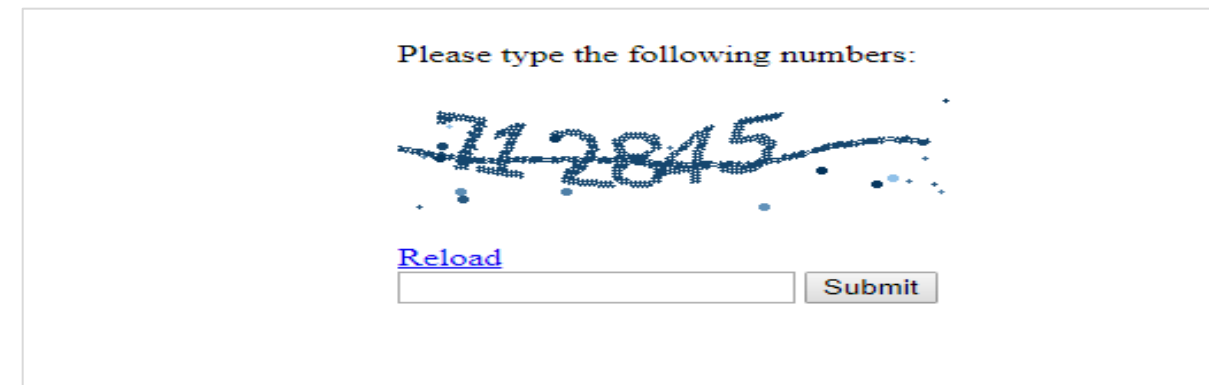
A "Save" button is located at the bottom left of the configuration area.

CC Policy Configuration

```
[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 ~]#
```

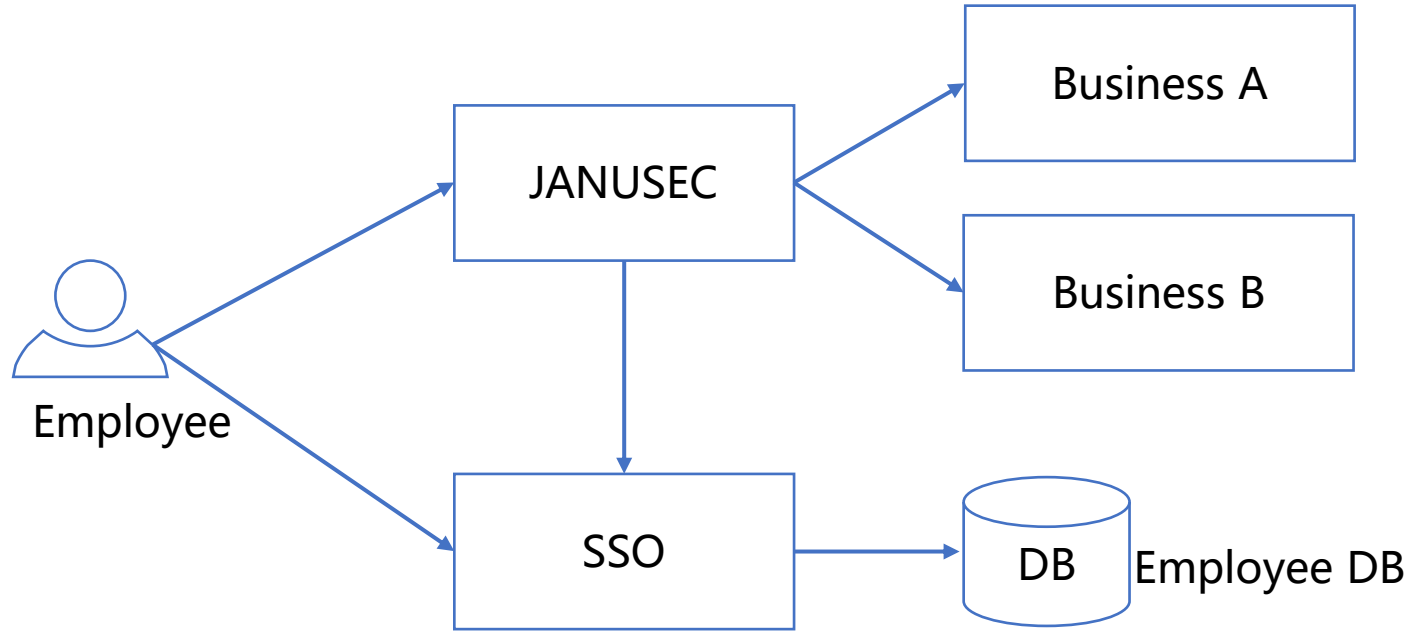
nftables takes effect, the attacking IP is blocked and will be automatically unblocked (Optional)



The screenshot shows a CAPTCHA interface. At the top, it says "Please type the following numbers:". Below this is a distorted image of the number "712845". At the bottom, there is a "Reload" link, an input field, and a "Submit" button.

CAPTCHA Demo (Optional)

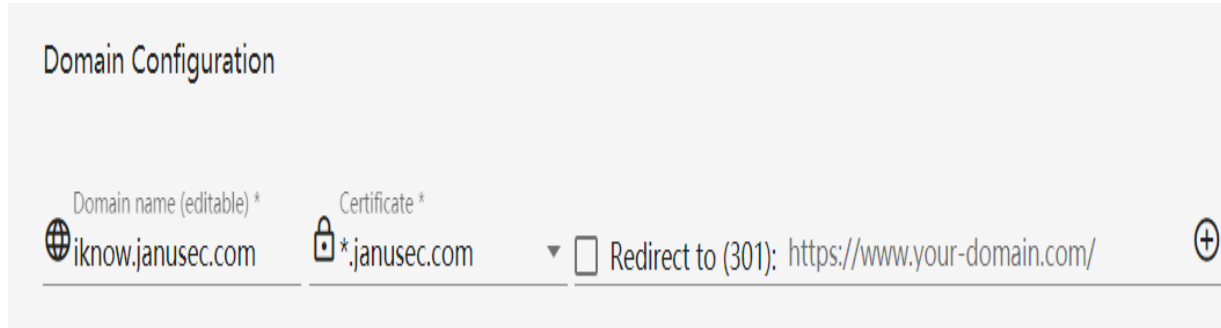
Feature 4: Authentication (Protect Internal Web Apps)



Optional Authentication Mechanism:

- WeCom Scan Code
- Dingtalk Scan Code
- Feishu Scan Code
- LDAP+Authenticator 2FA
- ...

Feature 5: HTTPS quality assurance, private key encrypted storage



Business does not need to hold a digital certificate, just drop down to select the certificate

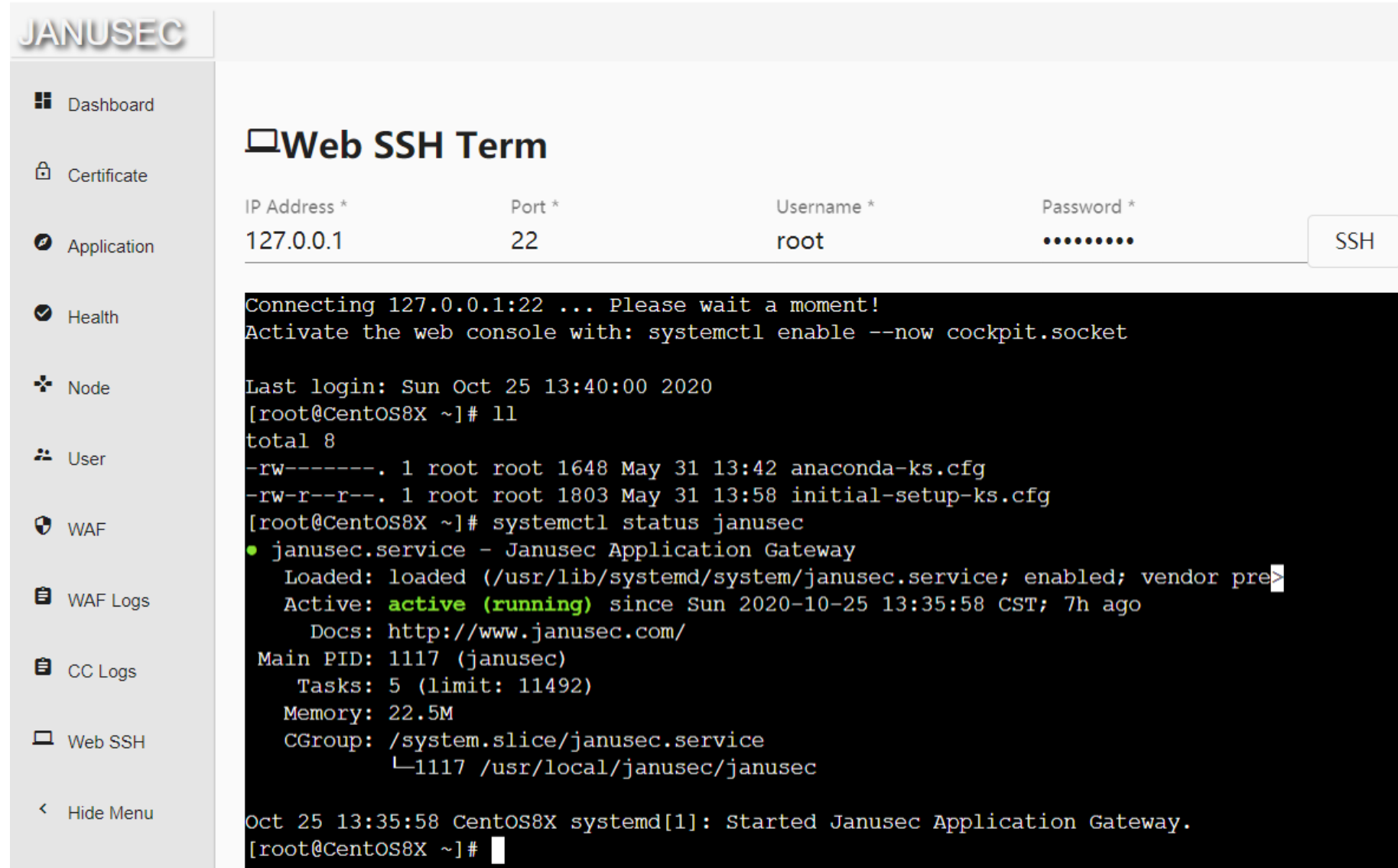


HTTPS Security Check Result

Security guarantee provided by JANUSEC:

- ❑ Disable insecure SSL/TLS versions, use TLS 1.2 or above
- ❑ Use forward security algorithm (when the master key is leaked, the security of historical communication records will not be affected)
- ❑ One-click to enable HSTS (browser default HTTPS) or automatically redirect to HTTPS (301 redirect)
- ❑ The private key is encrypted and stored in JANUSEC to prevent the hidden danger of leakage caused by the random storage of various businesses

Feature 6: Built-in Web SSH (record employee ID, auditable)



The screenshot displays the JANUSEC web interface. On the left is a sidebar menu with options: Dashboard, Certificate, Application, Health, Node, User, WAF, WAF Logs, CC Logs, Web SSH, and Hide Menu. The main content area is titled "Web SSH Term". It features a form with four input fields: "IP Address *" (127.0.0.1), "Port *" (22), "Username *" (root), and "Password *" (masked with dots). An "SSH" button is positioned to the right of the password field. Below the form is a terminal window with a black background and white text. The terminal output shows the connection process, a prompt to activate the web console, the last login time, file permissions, and the status of the janusec service, which is active and running.

JANUSEC

Dashboard
Certificate
Application
Health
Node
User
WAF
WAF Logs
CC Logs
Web SSH
Hide Menu

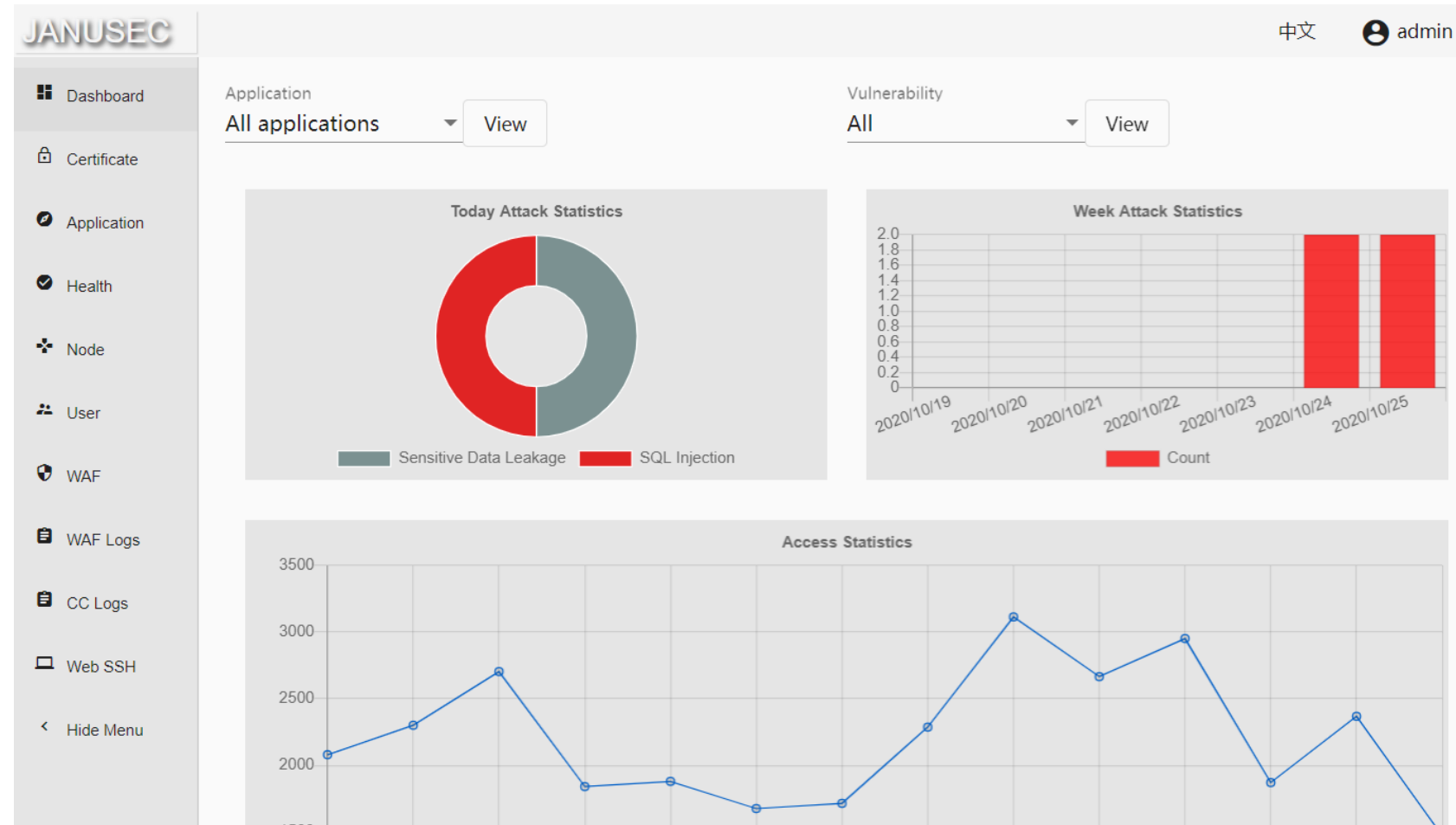
Web SSH Term

| IP Address * | Port * | Username * | Password * | |
|--------------|--------|------------|------------|-----|
| 127.0.0.1 | 22 | root | | SSH |

```
Connecting 127.0.0.1:22 ... Please wait a moment!  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sun Oct 25 13:40:00 2020  
[root@CentOS8X ~]# ll  
total 8  
-rw-----. 1 root root 1648 May 31 13:42 anaconda-ks.cfg  
-rw-r--r--. 1 root root 1803 May 31 13:58 initial-setup-ks.cfg  
[root@CentOS8X ~]# systemctl status janusec  
● janusec.service - Janusec Application Gateway  
   Loaded: loaded (/usr/lib/systemd/system/janusec.service; enabled; vendor pre  
   Active: active (running) since Sun 2020-10-25 13:35:58 CST; 7h ago  
     Docs: http://www.janusec.com/  
   Main PID: 1117 (janusec)  
     Tasks: 5 (limit: 11492)  
    Memory: 22.5M  
     CGroup: /system.slice/janusec.service  
            └─1117 /usr/local/janusec/janusec  
  
Oct 25 13:35:58 CentOS8X systemd[1]: Started Janusec Application Gateway.  
[root@CentOS8X ~]#
```

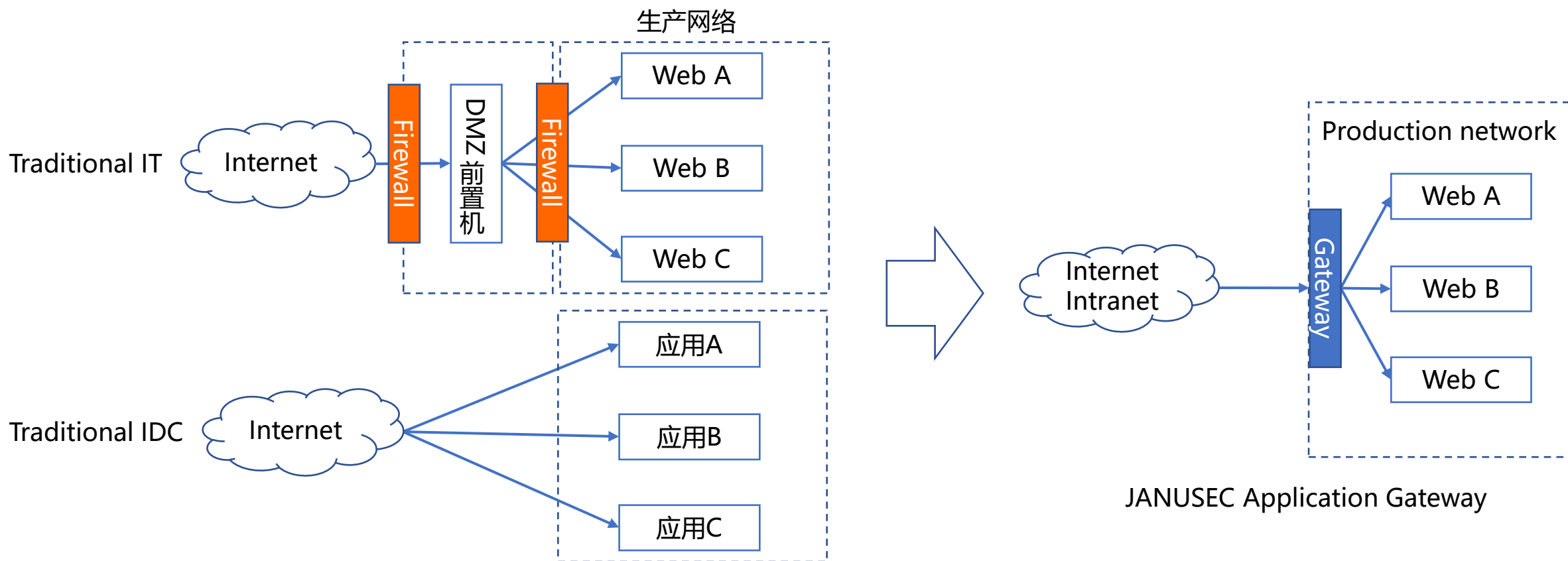
You can log in to the target server through a browser, the channel is safe and controllable, and the log is associated with the employee ID

Other Features



- Dashboard
 - WAF Statistics
 - Access Statistics
- Load Balance
 - Multiple Nodes
 - Content Acceleration
- Hosts Health Check
 - Stop Forward to Offline Hosts
 - Automatically Detect and Resume Forwarding
- Content Security Policy (CSP)

Typical Scenario (1): Simplify publishing process and firewall management

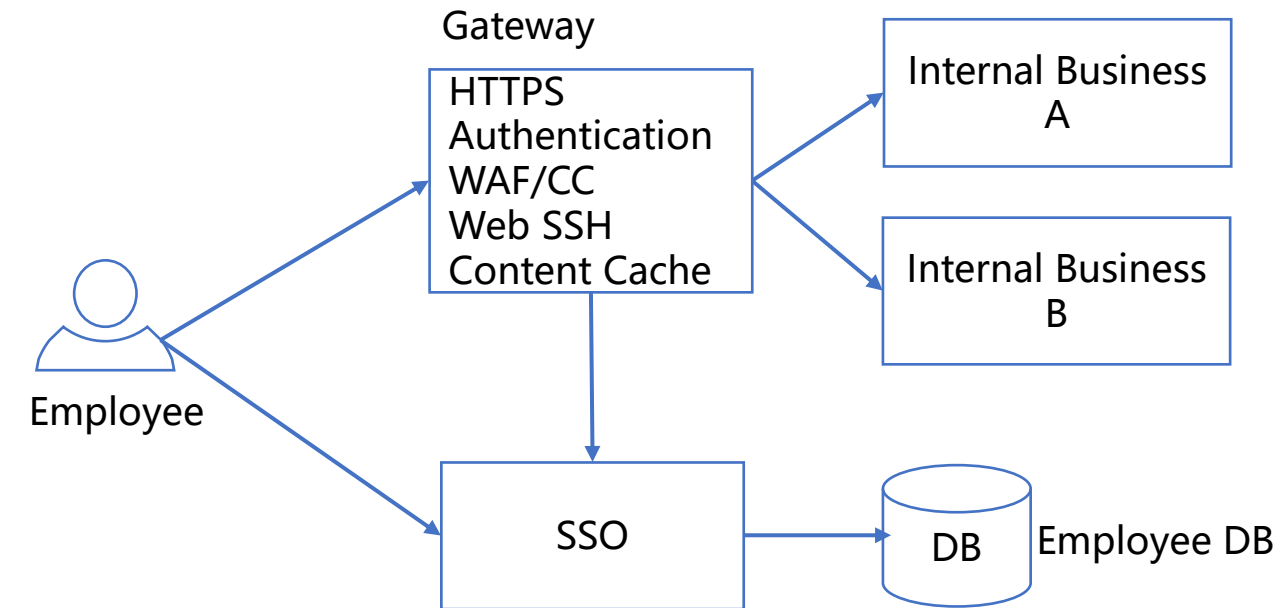


JANUSEC Application Gateway

| Feature | Traditional IT | Traditional IDC | JANUSEC Application Gateway |
|-----------------|---|--|--|
| Publishing | <ul style="list-style-type: none"> Front-end physical server deployment or forwarding server configuration | <ul style="list-style-type: none"> The server publishes directly to the outside through the external network interface card | <ul style="list-style-type: none"> Simple and efficient through Web UI |
| Firewall | <ul style="list-style-type: none"> Apply for firewall policy | <ul style="list-style-type: none"> No need to apply for Firewall policy (or need to register) | <ul style="list-style-type: none"> Not needed |
| High risk ports | <ul style="list-style-type: none"> Rarely open high-risk ports by mistake | <ul style="list-style-type: none"> Prone to accidentally open high-risk ports | <ul style="list-style-type: none"> Will not open high-risk ports by mistake (only internal network interface card is configured for business) |

Comparison of traditional publishing model and JANUSEC publishing model

Typical Scenario (2): Integrated Authentication, HTTPS, Security defense, Web SSH, Load balancing



- ❑ Applicable to the internal promotion of the whole site HTTPS
- ❑ Open authentication in batches for businesses that lack internal authentication mechanisms
- ❑ Protect business from web intrusion & CC attacks
- ❑ Provide convenient and auditable Web SSH channels
- ❑ Provide load balancing and content acceleration (multi-node deployment)

Thank you!

<https://www.janusec.com/>