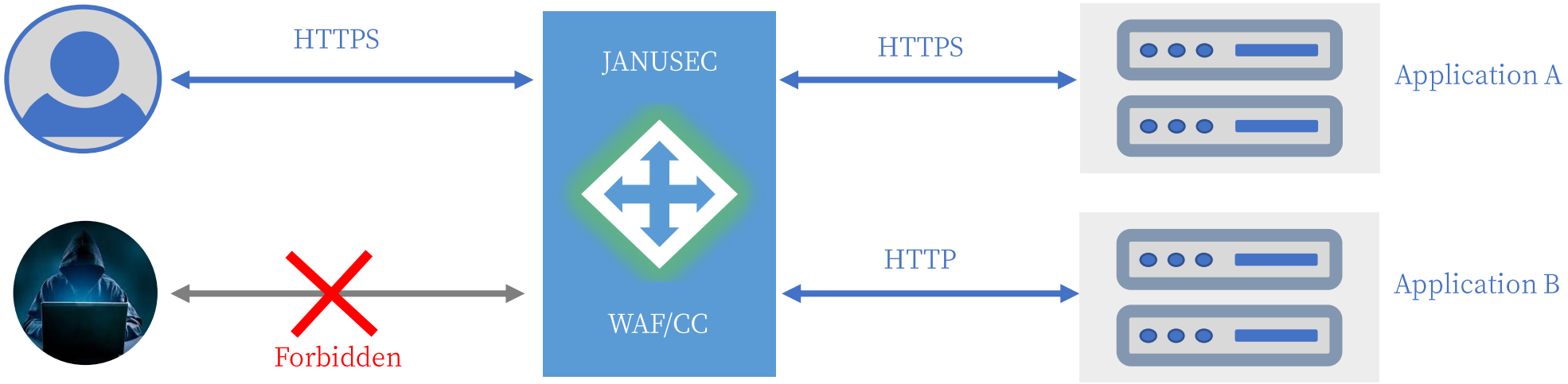
Janusec Application Gateway

JANUSEC Provide Fast and Secure Application Delivery

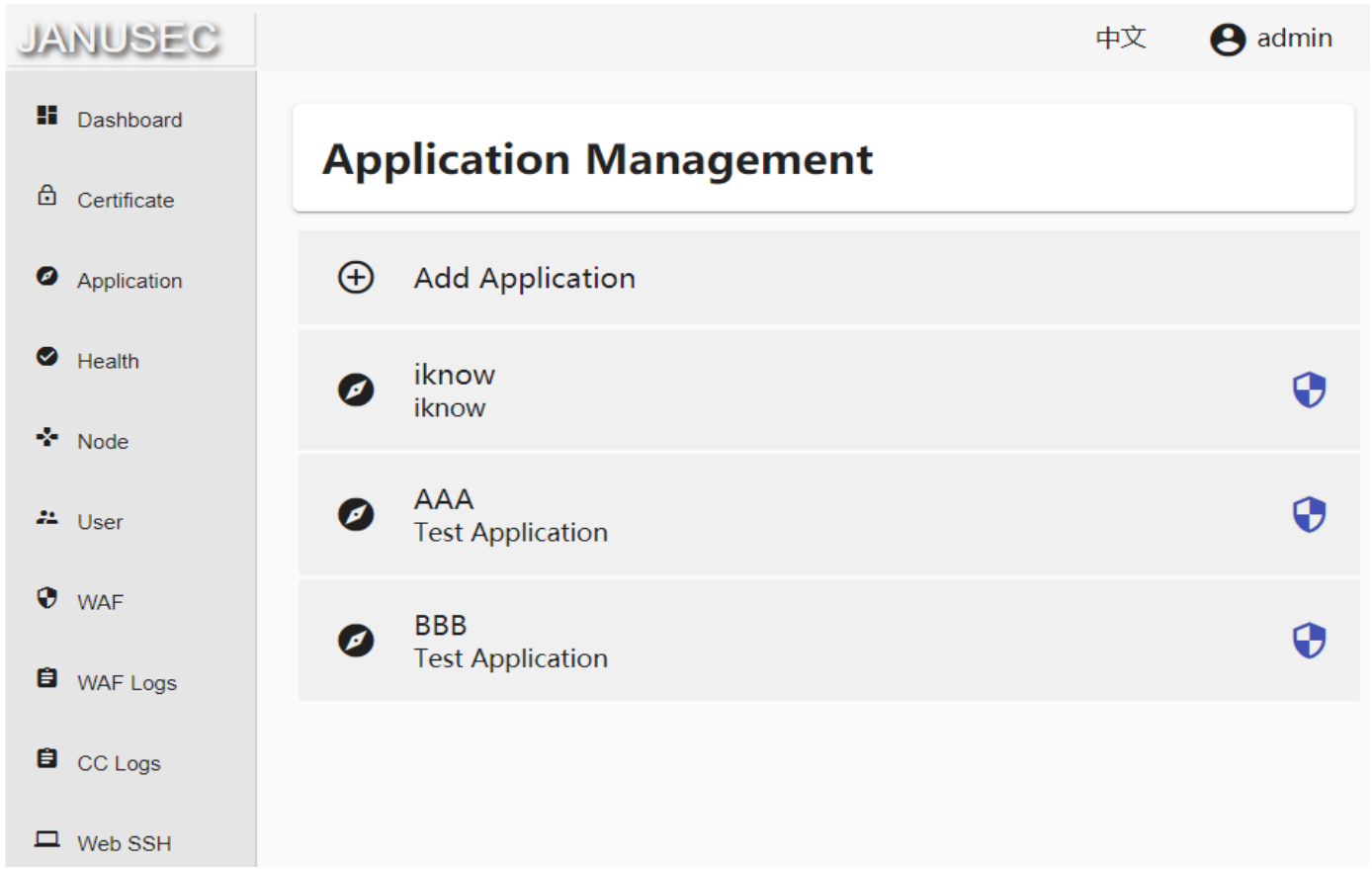


Full HTTPS

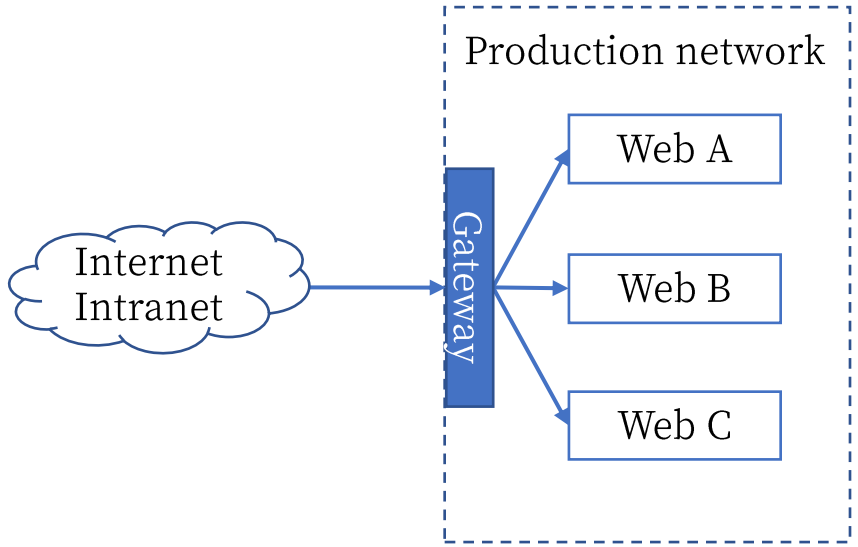
Security Denfense (WAF/CC)
Security Improvement
(Authentication)
Load Balance (Content Acceleration)

Protected
Backend

Feature 1: Fast Delivery (Web UI)

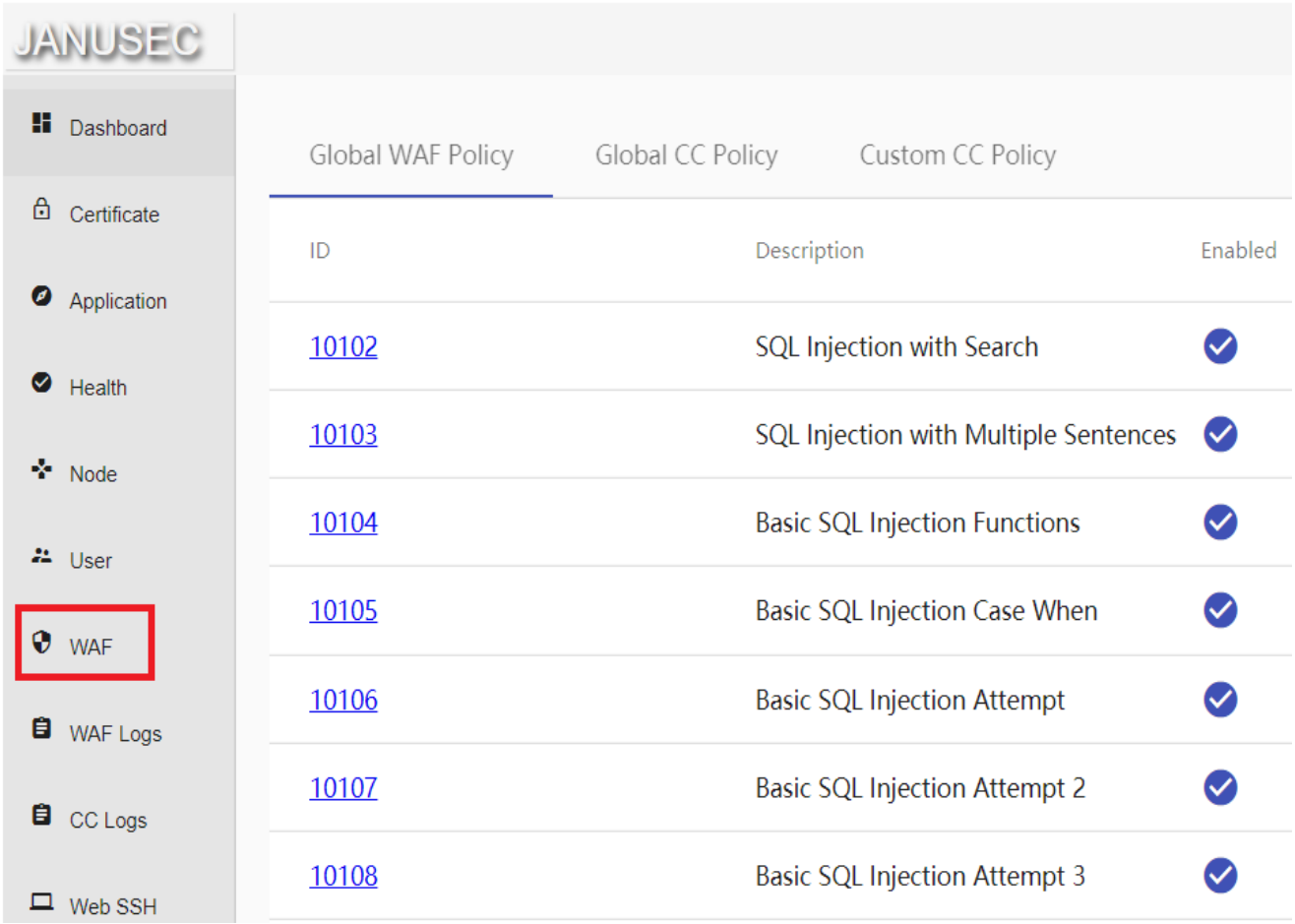


Web-based Configuration UI

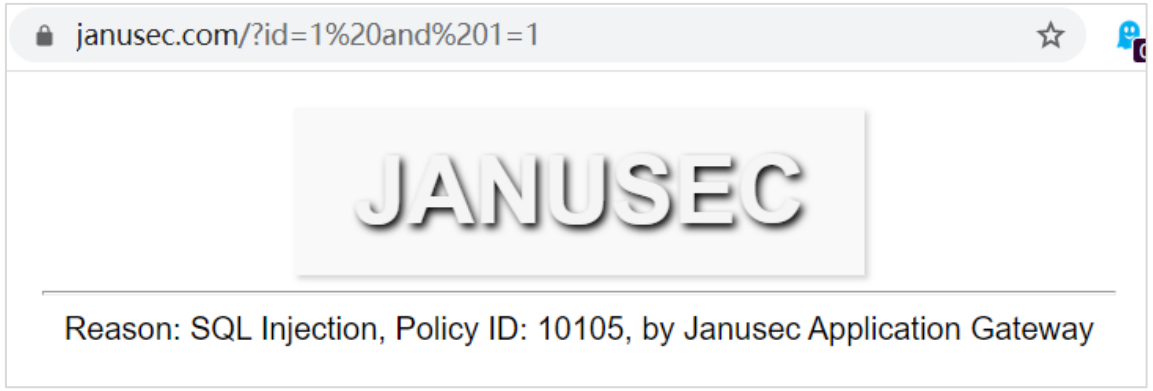


Quick release, improve efficiency and reduce costs

Feature 2: Built-in WAF, anti-hacking



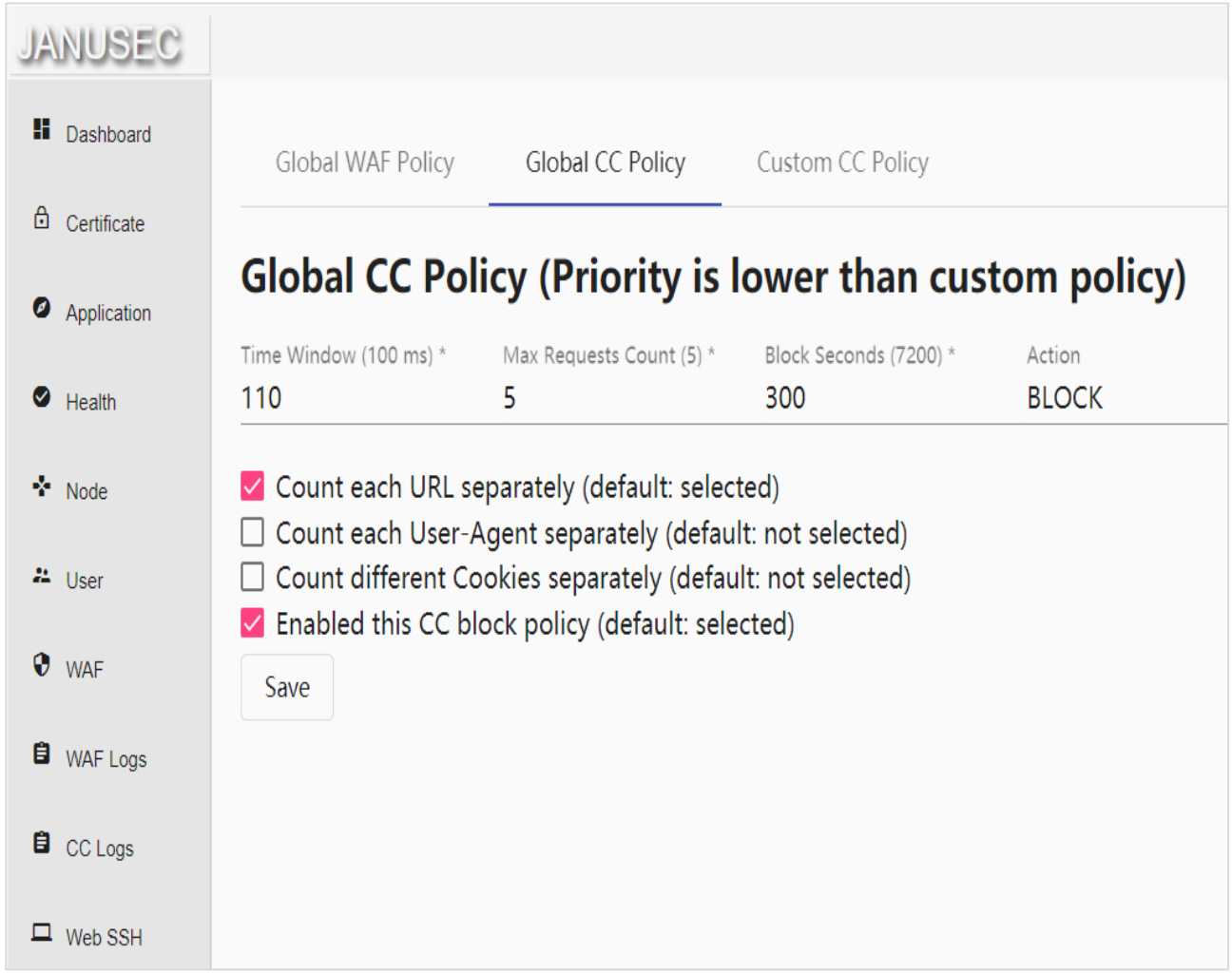
WAF Policies



Intercept SQL injection

Intercept Sensitive Information Leakage

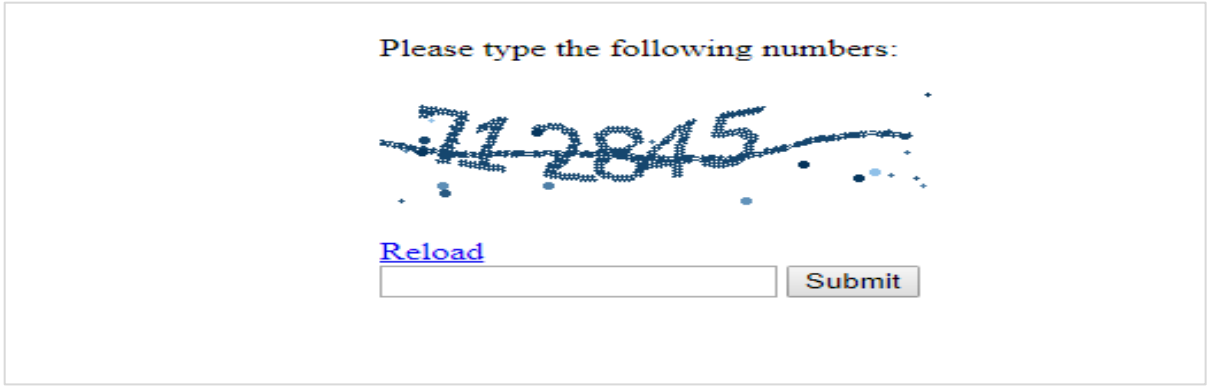
Feature 3: Built-in CC, Prevent attacks, link with firewall or CAPTCHA



CC Policy Configuration

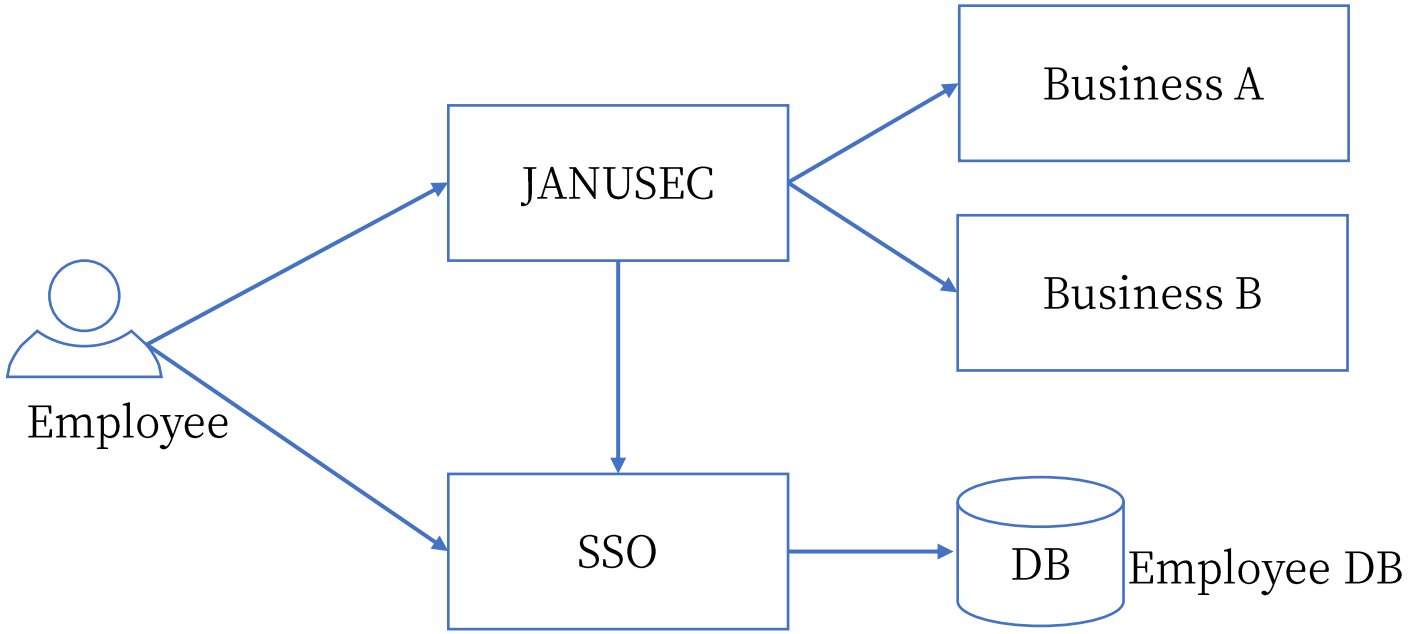
```
[root@CentOS8X U2]# nft list ruleset
table inet janusec {
        set blocklist {
                type ipv4_addr
                flags timeout
                elements = { 192.168.100.1 timeout 5m expires 3m50s968ms }
        }

        chain input {
                type filter hook input priority 0; policy accept;
                @nh,96,32 @blocklist drop
        }
}
[root@CentOS8X U2]#
```

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



CAPTCHA Demo (Optional)

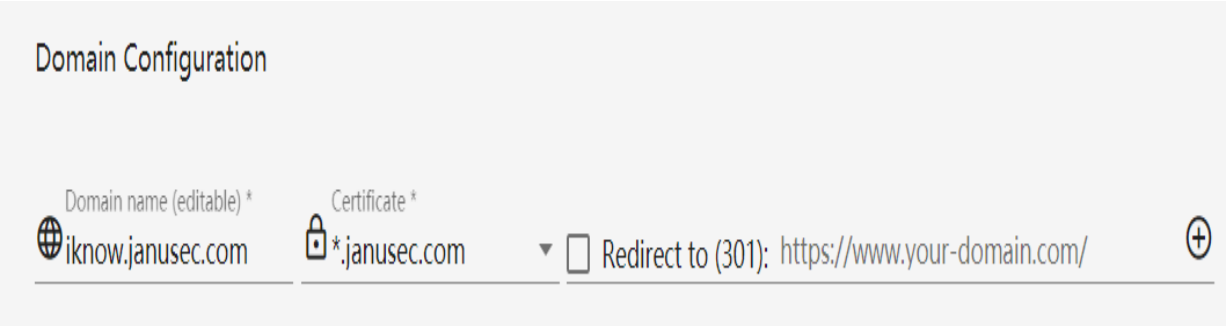
Feature 4: Authentication (Protect Internal Web Apps)



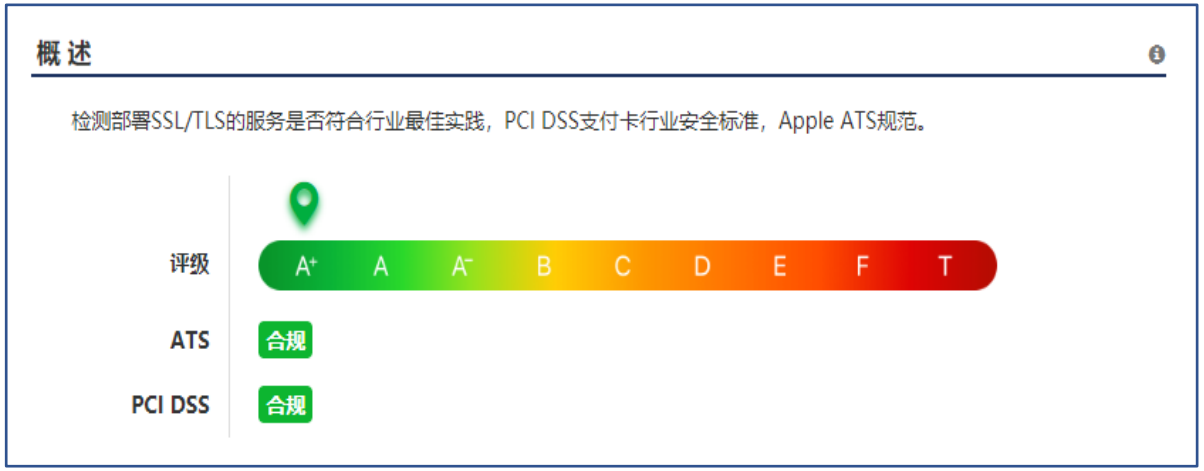
Optional Authentication Mechanism:

- 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

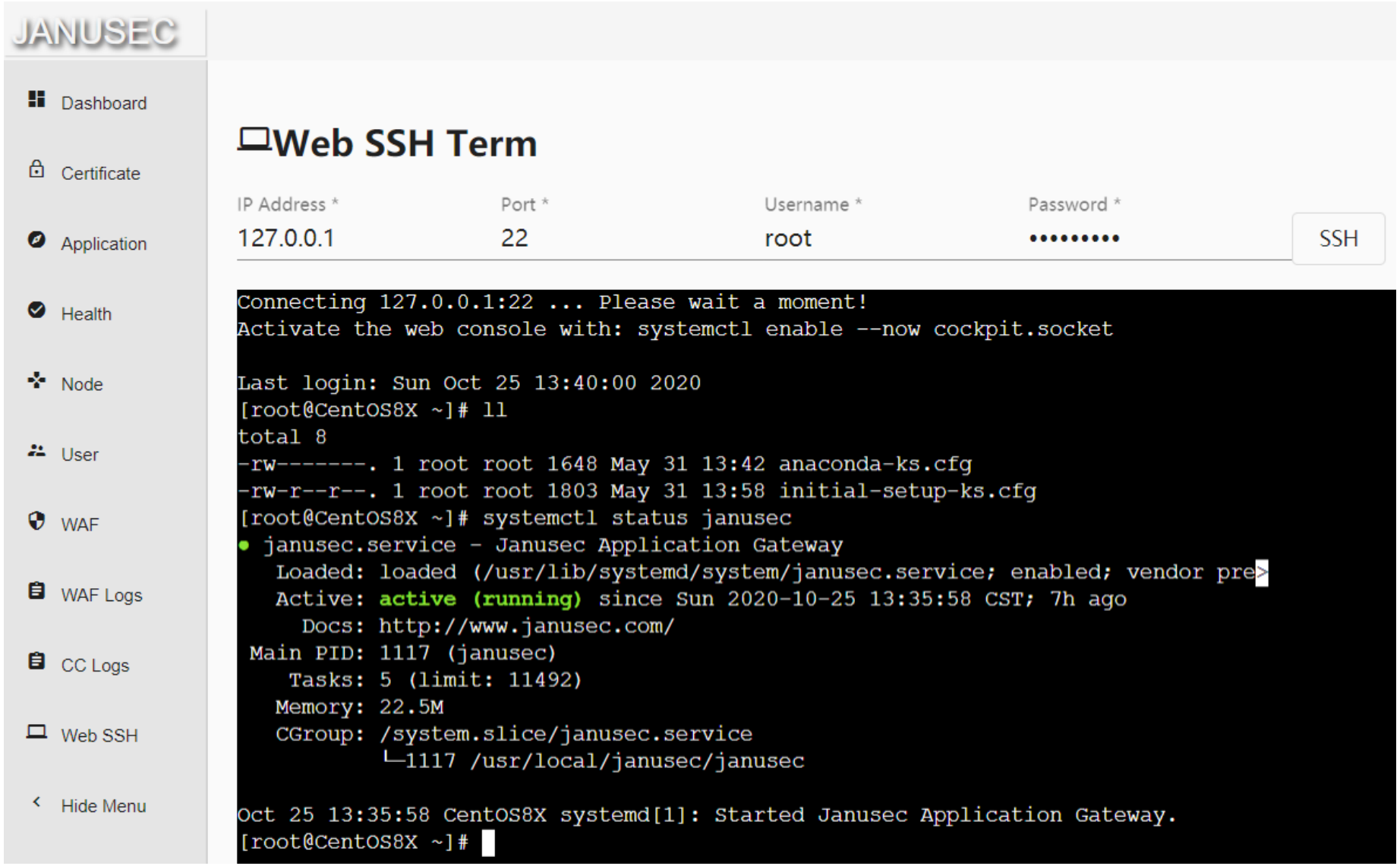


HTTPS Security Check Result

Security guarantee provided by JANUSEC:

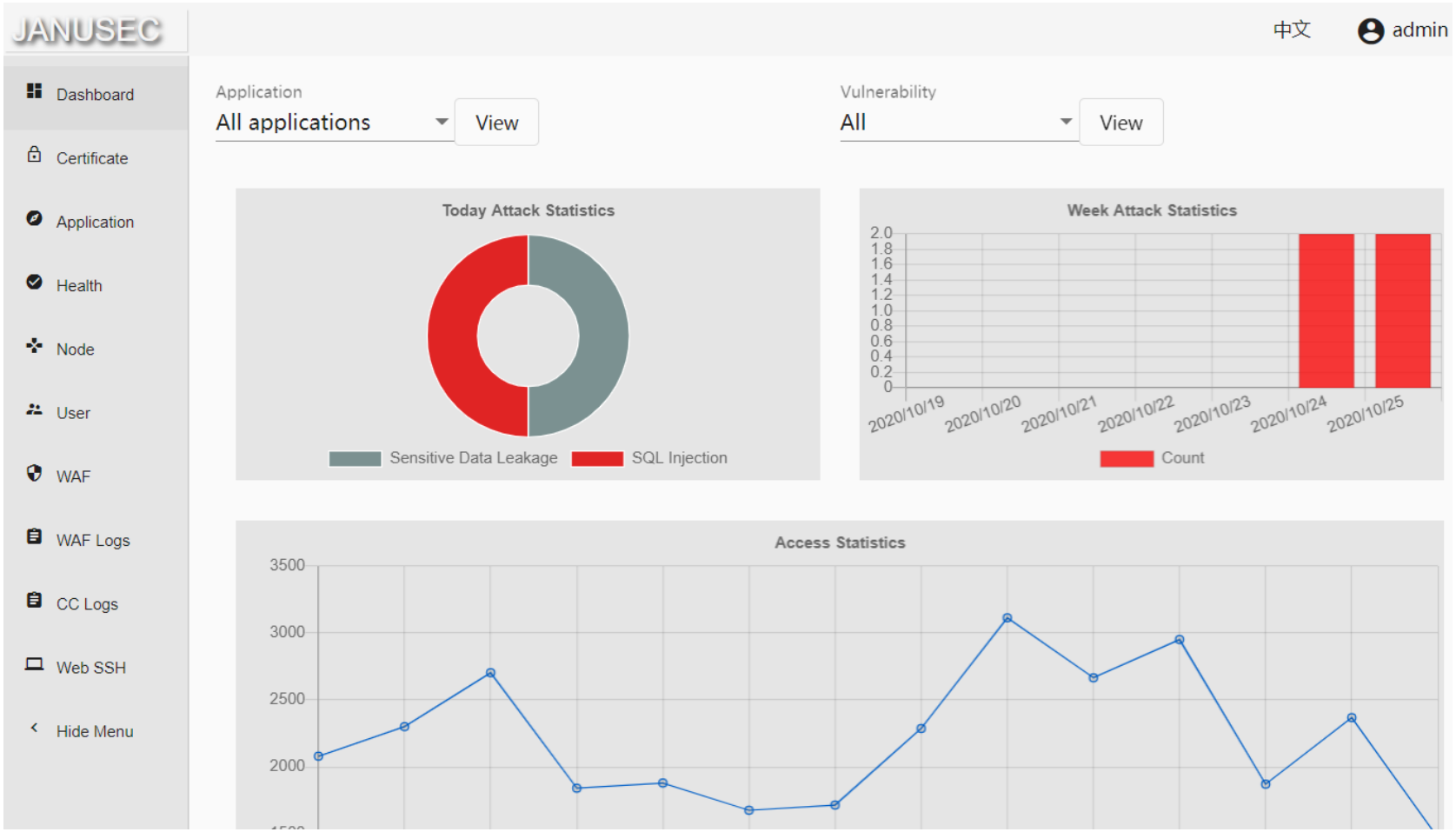
- ❑ Disable insecure SSL/TLS versions, use TLS 1.2 or above
- ❑ Use forward security algorithm (when the master key is leaked, the security of historical communication records will not be affected)
- ❑ One-click to enable HSTS (browser default HTTPS) or automatically redirect to HTTPS (301 redirect)
- ❑ 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)



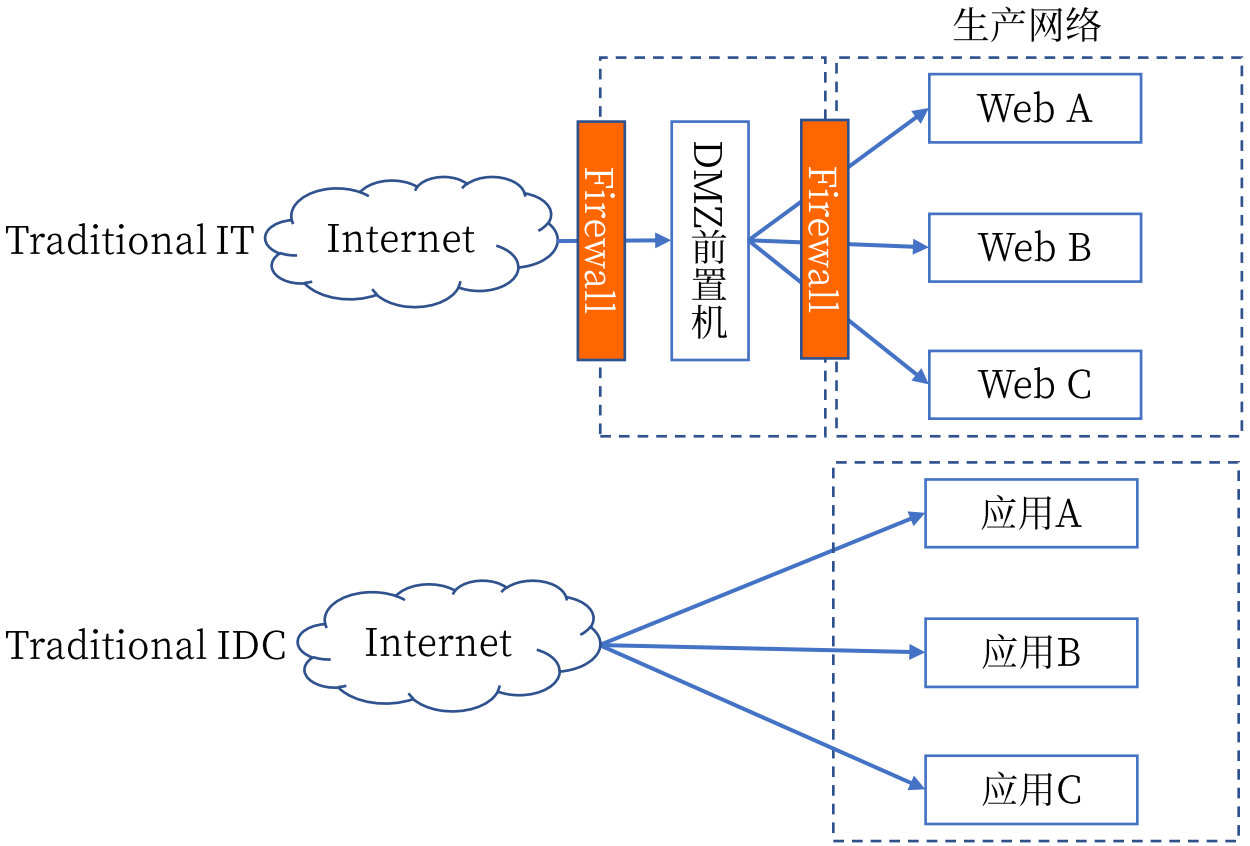
You can log in to the target server through a browser, the channel is safe and controllable, and the log is associated with the employee ID

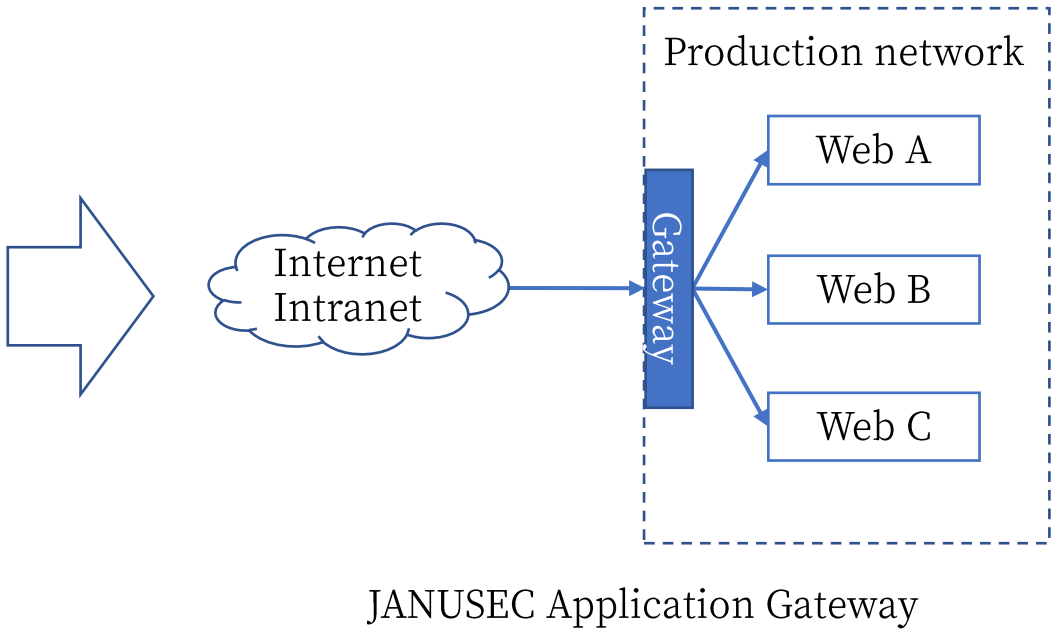
Other Features



- ❑ 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



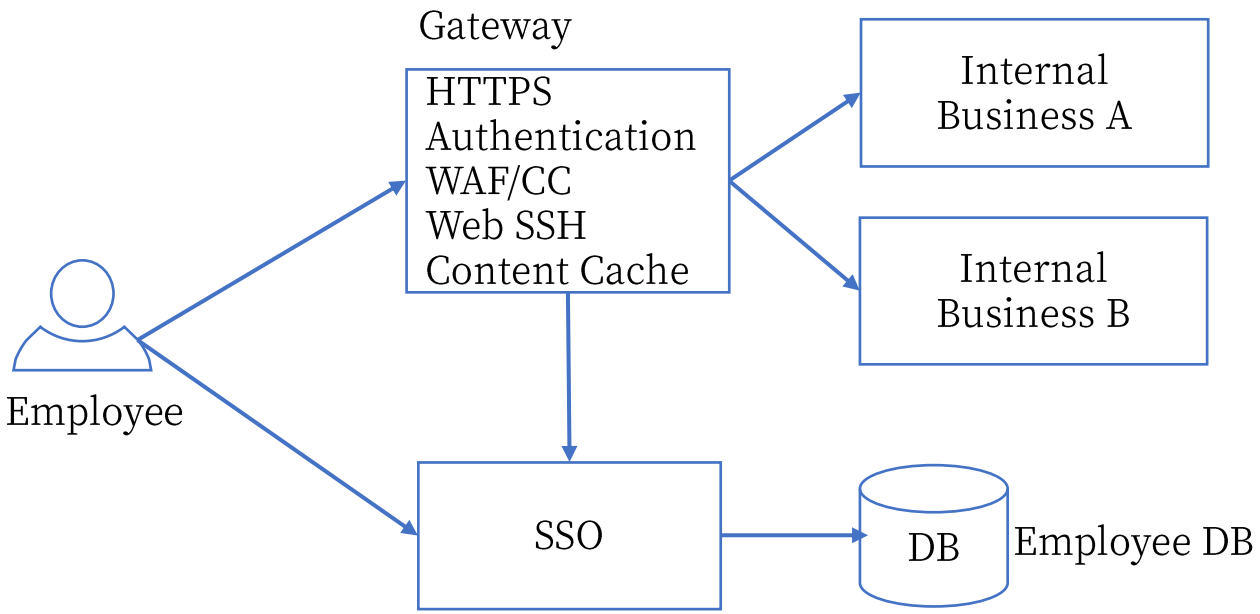


JANUSEC Application Gateway

Feature	Traditional IT	Traditional IDC	JANUSEC Application Gateway
Publishing	• Front-end physical server deployment or forwarding server configuration	• The server publishes directly to the outside through the external network interface card	• Simple and efficient through Web UI
Firewall	• Apply for firewall policy	• No need to apply for Firewall policy (or need to register)	• Not needed
High risk ports	• Rarely open high-risk ports by mistake	• Prone to accidentally open high-risk ports	• 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/