Bluedon-WAF

Contents

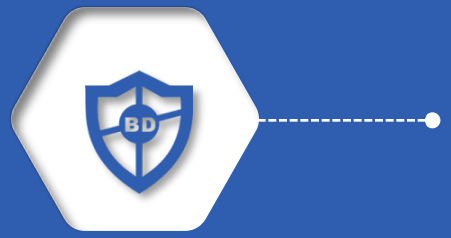
Product Portfolio

蓝盾 BLUEDON 智慧安全领导者 蓝盾股份:300297

Application security products

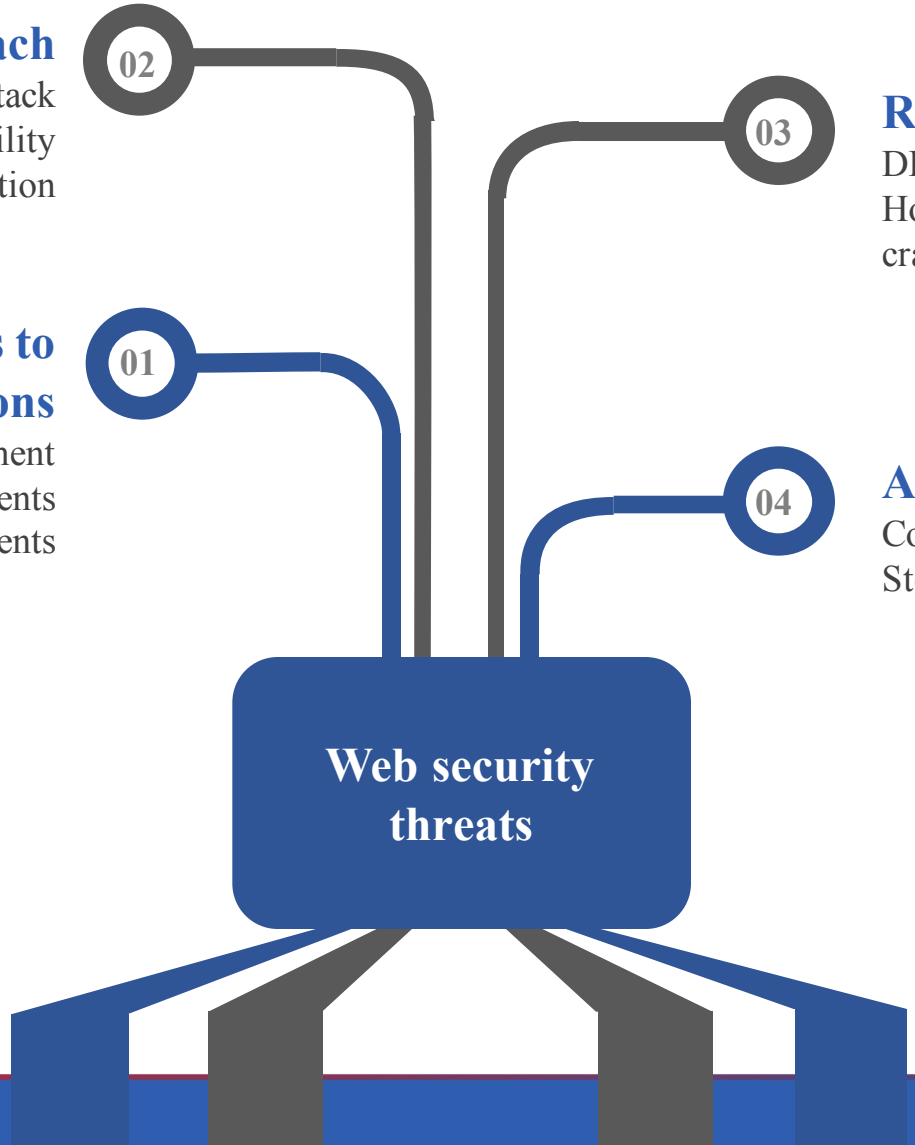
- Bluedon-WAF

- Bluedon webpage defacement prevention system



Background

Background



Data breach
Hacker attack
Exploitation of a third-party vulnerability
SQL injection

Resources and financial loss
DDOS attack, CC attack
Hot link
crawler

Reputation loss to enterprises/institutions
Webpage defacement
XSS/CSRF—attack clients
Malicious code—attack clients

APT attack
Control server to intrude into intranet
Stealing sensitive data

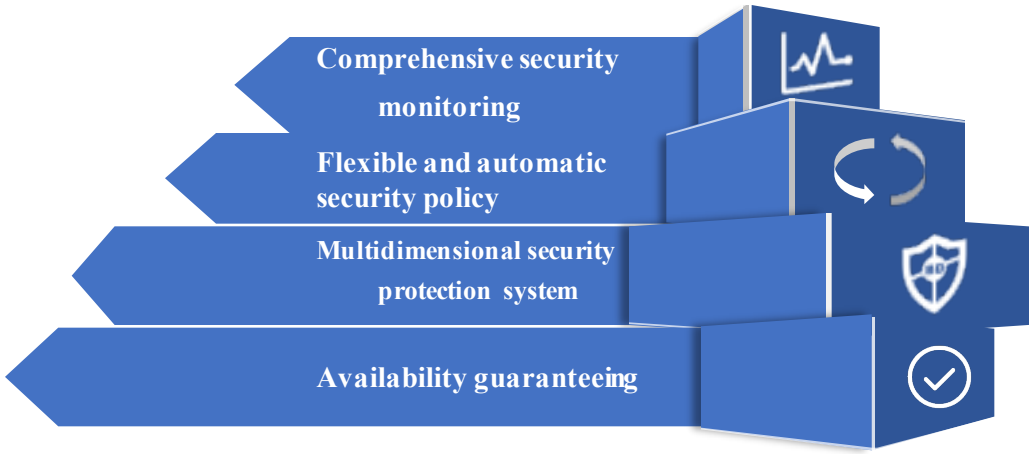
Product Introduction

Web Application Firewall that can realize self-learning dynamic modeling

Bluedon Web Application Firewall

Web application firewall:

- Comprehensive security monitoring
- Self-learning security policy
- Multidimensional security protection system
- Availability guaranteeing



Multidimensional security protection system

Multidimensional security protection system

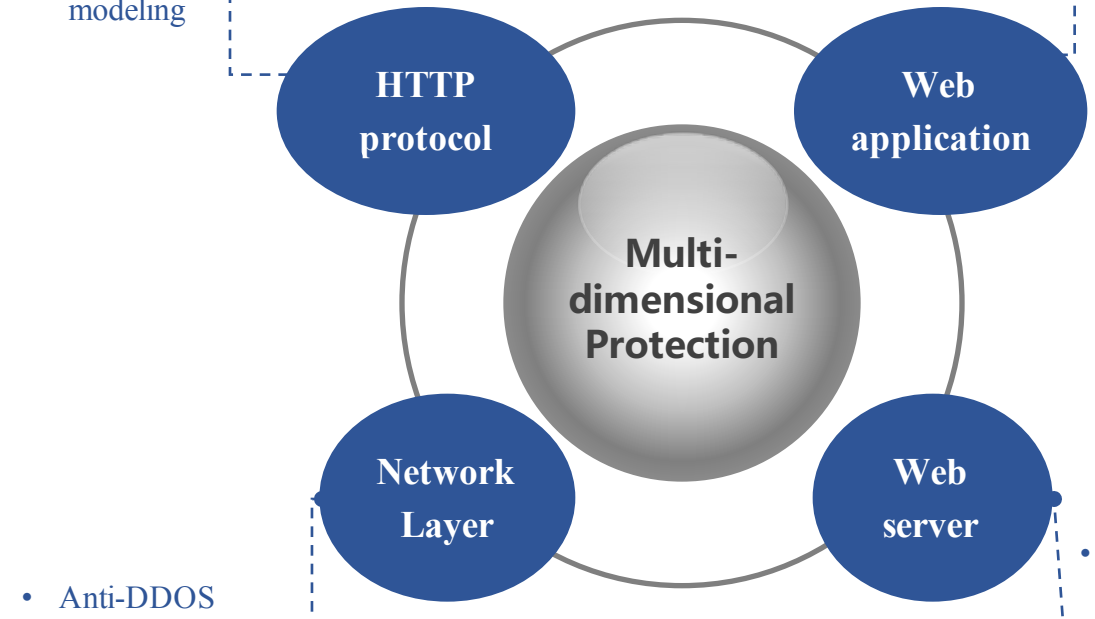
Establish protection means from dimensions including Network Layer, HTTP protocol layer, Web Sever layer and Web application layer and form an integrated prevention system.

Network Layer: anti-DDOS attack, web access control;

HTTP protocol layer: HTTP protocol compliance check and self-learning modeling;

Web Server layer: server information hiding, crawler prevention, vulnerability scanning;

Web application layer: over 2000 web attack rules, SQL injection, XSS etc.



- HTTP protocol compliance check
- Self-learning dynamic modeling

- Over 2000 web attack prevention rules
- Defend against web attacks like SQL injection and XSS.

- Anti-DDOS attack
- Web access control

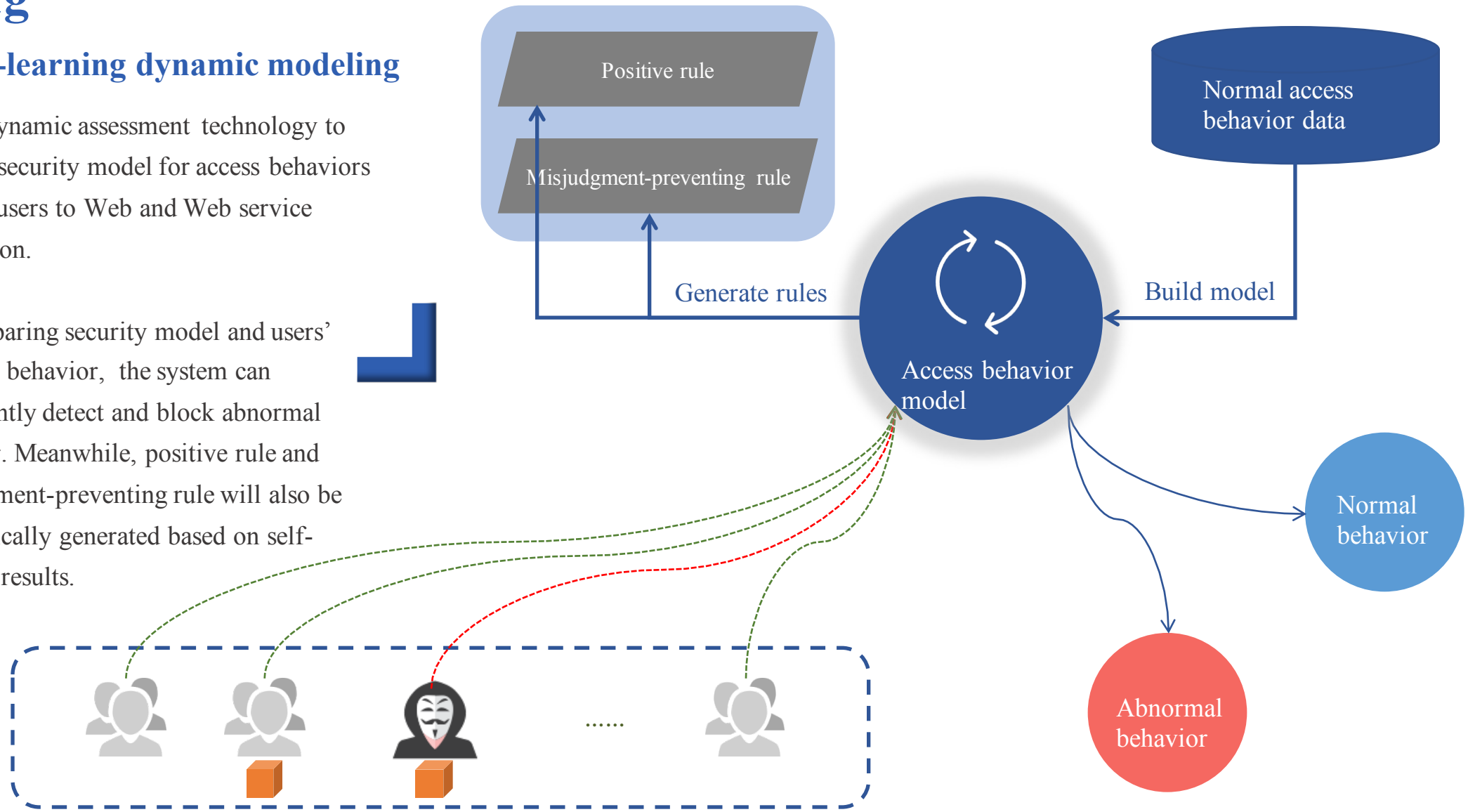
- Server information hiding
- Hot link and crawler prevention
- Vulnerability scanning

Automatic security policy and self-learning dynamic modeling

Self-learning dynamic modeling

Adopt dynamic assessment technology to create a security model for access behaviors of legal users to Web and Web service application.

By comparing security model and users' practical behavior, the system can intelligently detect and block abnormal behavior. Meanwhile, positive rule and misjudgment-preventing rule will also be automatically generated based on self-learning results.



Flexible security policy and its hierarchical configuration

Hierarchical configuration of security policy

Security policies are configured based on 3 levels:

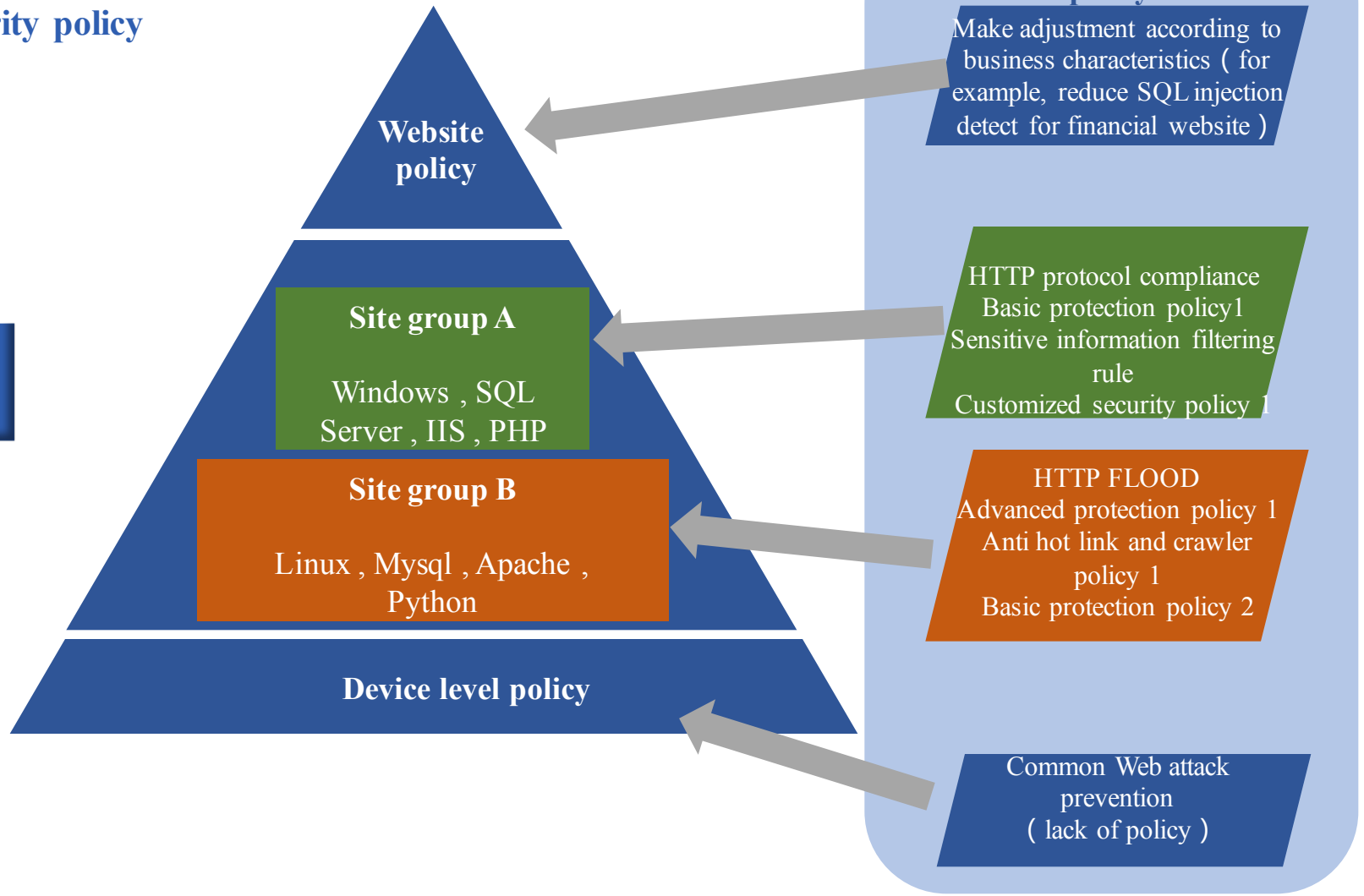
Device level policy, which applies to the whole WAF device;

Site group level policy, which applies to certain site group;

Website level policy, which applies to certain website;

Rules can be inherited among different levels;

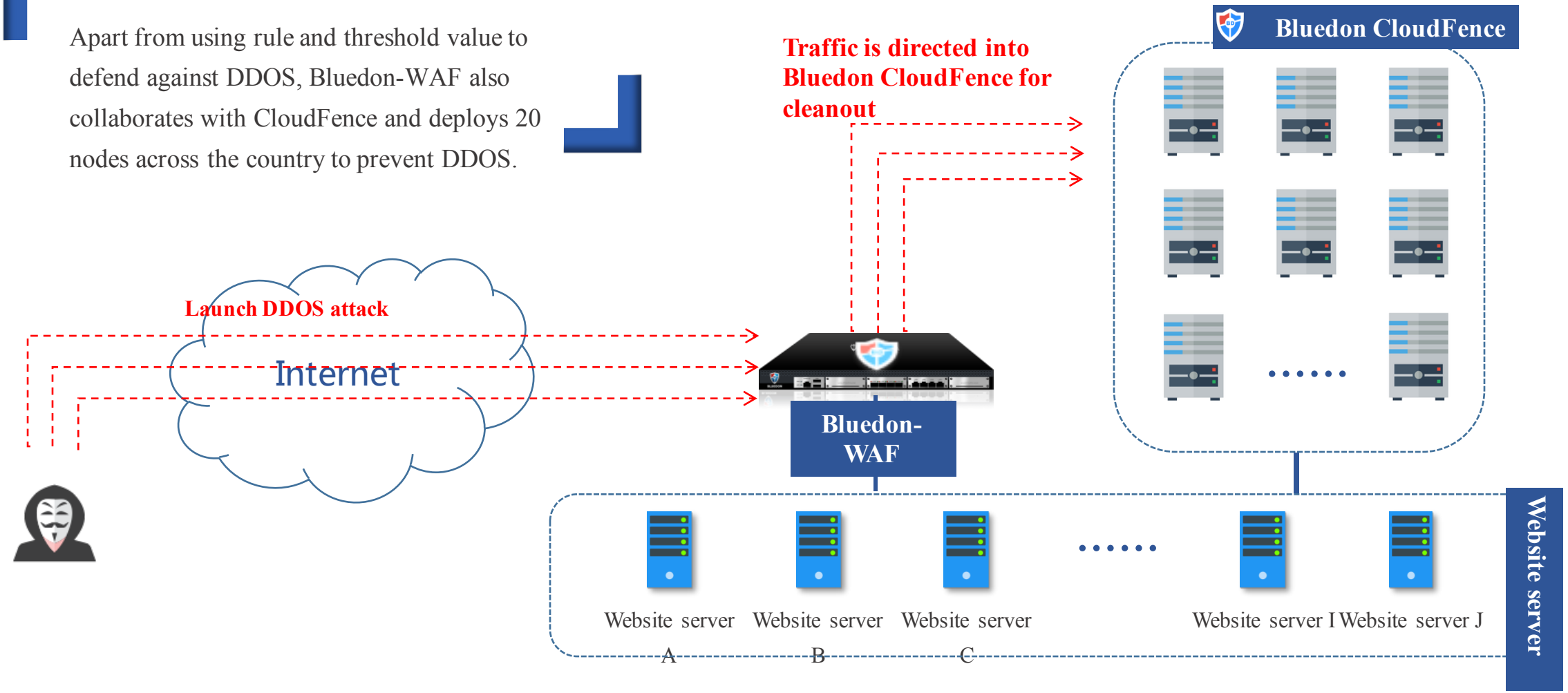
Rules can be detailed for specific website.



Availability guaranteeing and collaborative defense against DDOS

Collaborative defense against DDOS attack

Apart from using rule and threshold value to defend against DDOS, Bluedon-WAF also collaborates with CloudFence and deploys 20 nodes across the country to prevent DDOS.

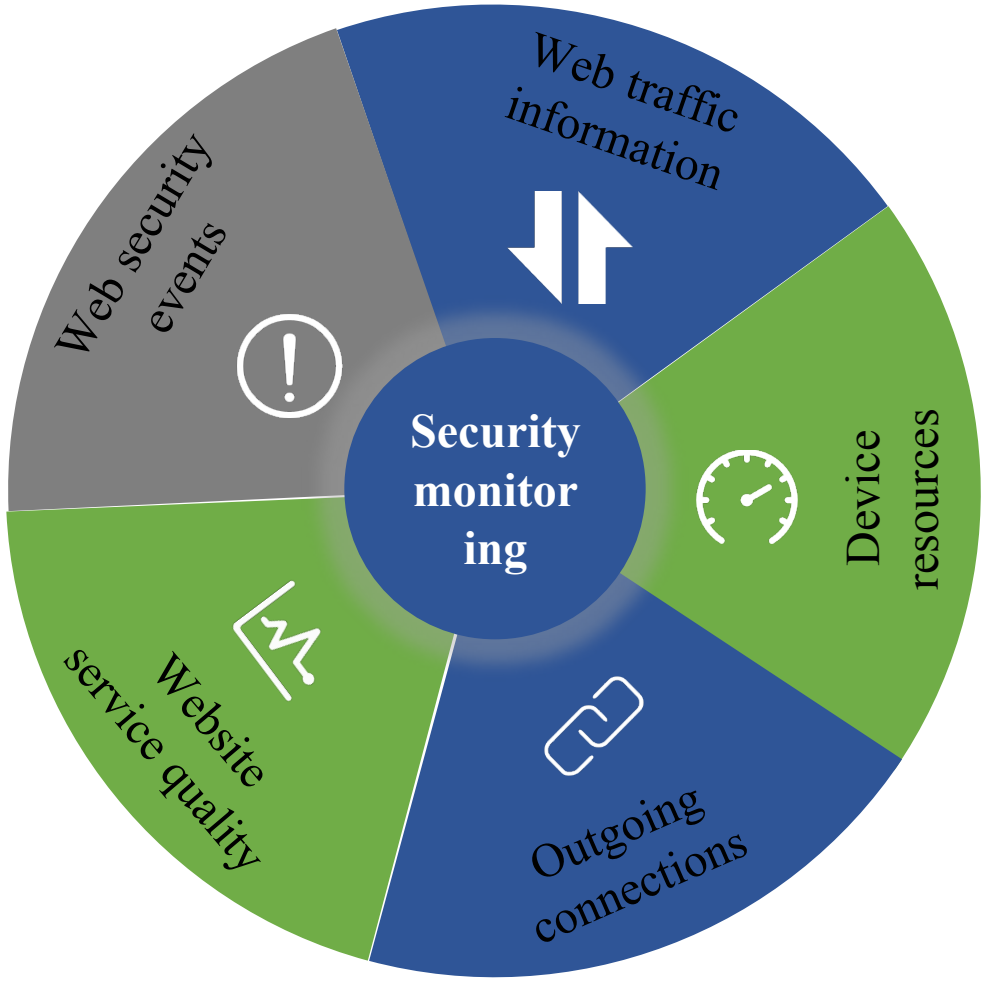


Security monitoring

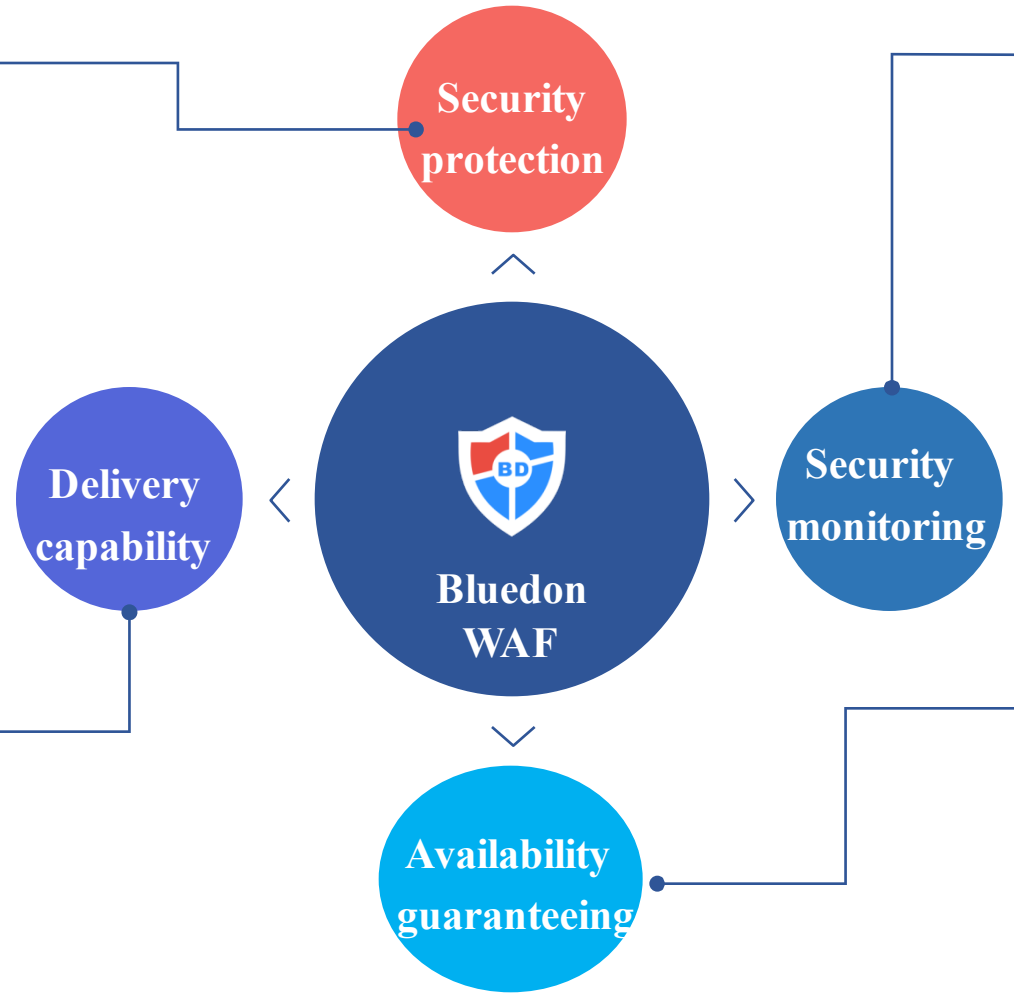
Security monitoring

Comprehensive security monitoring helps users get to know web security condition and service quality in real time:

- Real-time monitoring of Web security events
- Monitoring of Web traffic
- Monitoring of device's resources
- Monitoring of outgoing connections
- Monitoring of website service quality



Basic functions



Security protection
- Web attack prevention
- Self-learning modeling
- Webpage defacement prevention
- Sensitive information filtration
- Server information hiding
- Abnormal traffic detection
- HTTP protocol compliance
- Web access control

Security monitoring
- Real-time monitoring of security events
- Connections and traffic state of web application
- Usage of device resources
- Monitoring of outgoing connections
- Monitoring of website service quality

Delivery capability
- Cache acceleration
- Automatic load balancing
- Inspection of server state
- Hot Standby

Availability guaranteeing
- DDOS attack prevention
- Web vulnerability scanning
- Monitoring of server state
- Crawler and hot link prevention
- Website access statistics

Advantages

蓝盾 BLUEDON 智慧安全领导者 蓝盾股份:300297

Comprehensive and intelligent security protection

- Multidimensional security protection system to comprehensively defend against common web attacks;
- Self-learning modeling technology to quickly identify abnormal access behavior;
- Flexible multilevel policy management to achieve fine-grained policy configuration.

High availability guaranteeing

- Collaborate with Bludedon CloudFence to defend against DDOS attack;
- Prevent hot link and crawler to protect website resources;
- Web vulnerability scanning to avoid remote control.

Bluedon-WAF

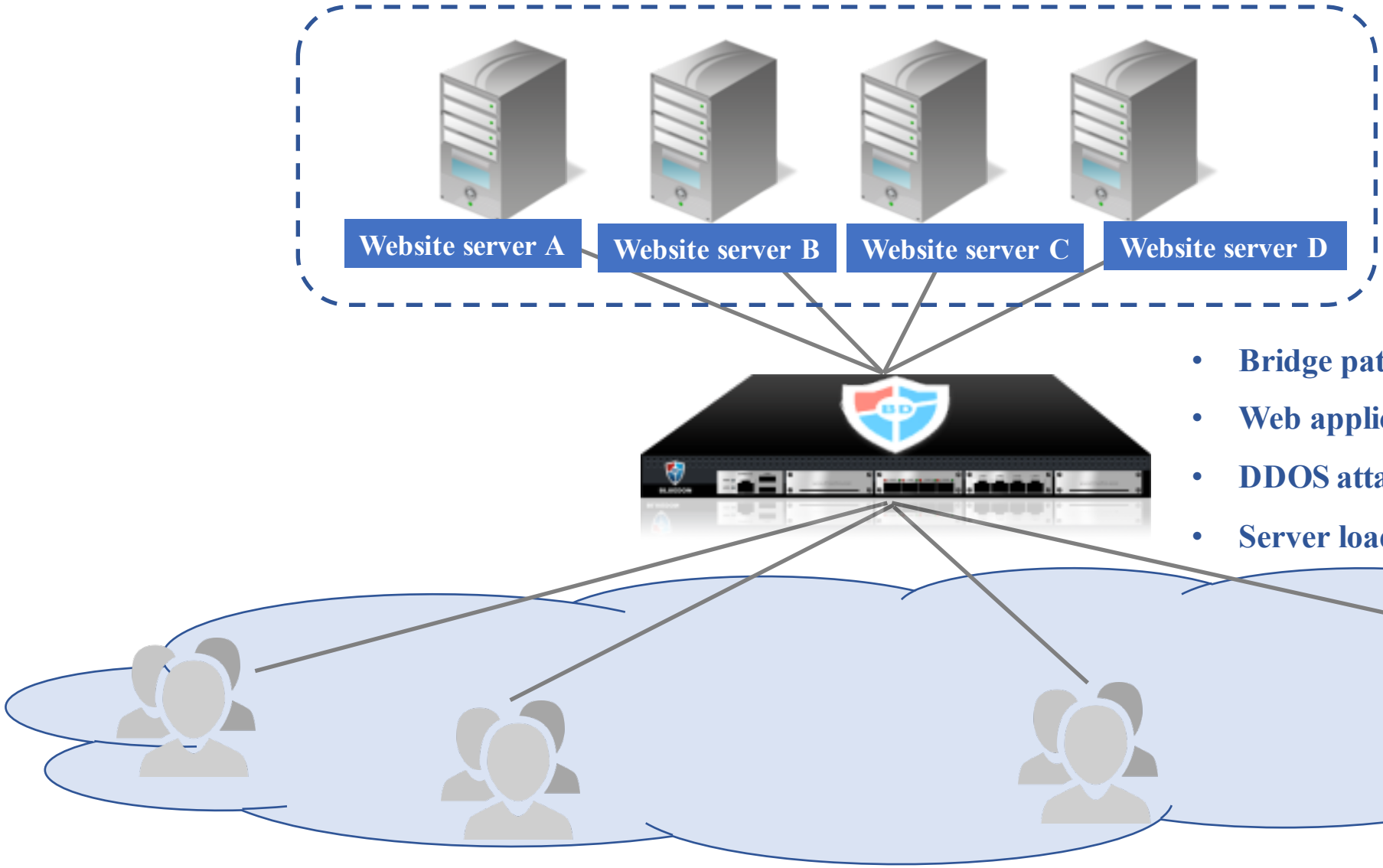
Comprehensive deliverability

- Utilize Cache technology to accelerate access to web applications;
- Load balancing technology to ensure service quality;
- Inspect server state to avoid business interruption.

Real-time monitoring and intuitive presentation

- Real-time monitoring and alert of security events;
- Real-time monitoring of network traffic and connections to timely know network state;
- Real-time monitoring of website service quality and server condition to ensure users to know about business operation in time.

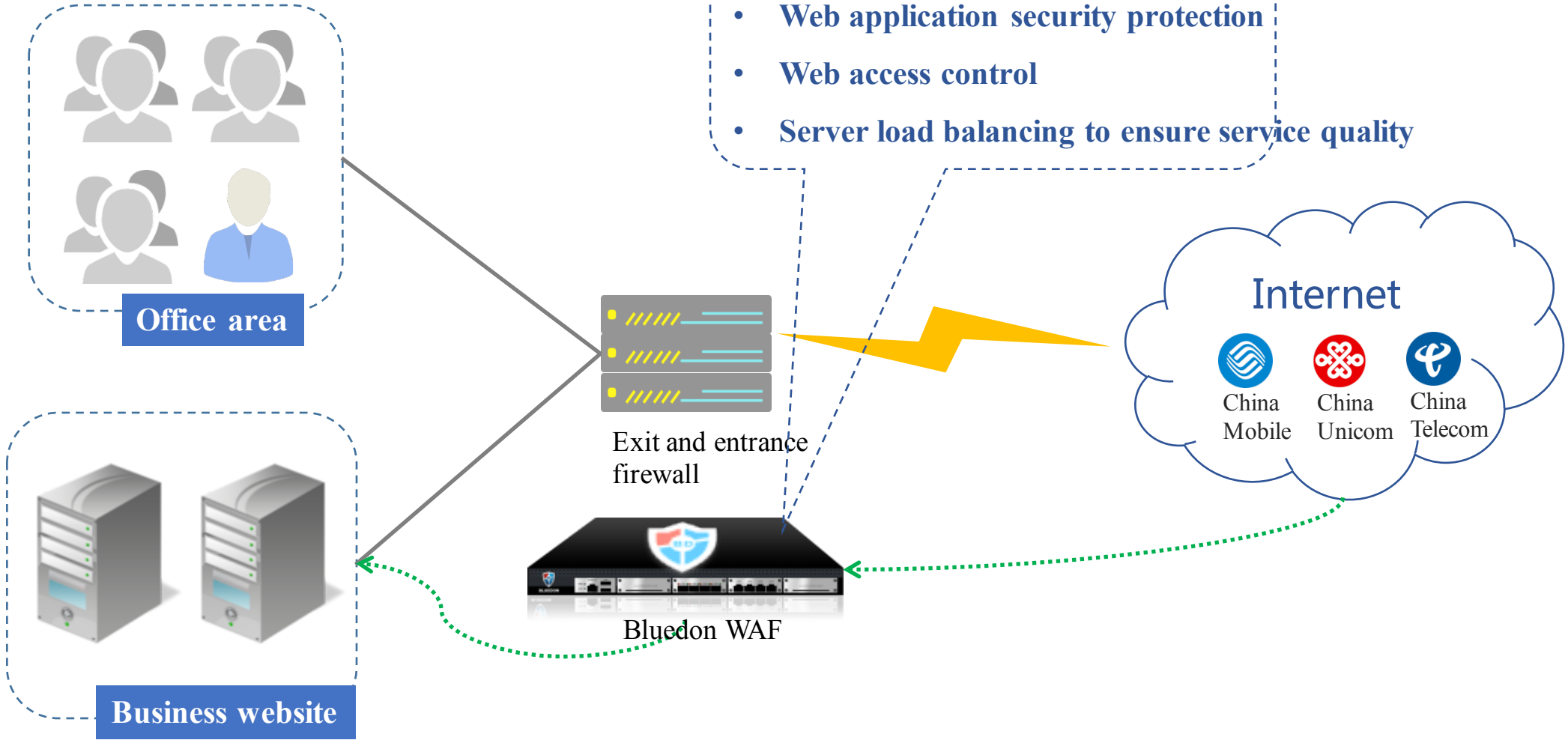
Deployment (bridging mode)



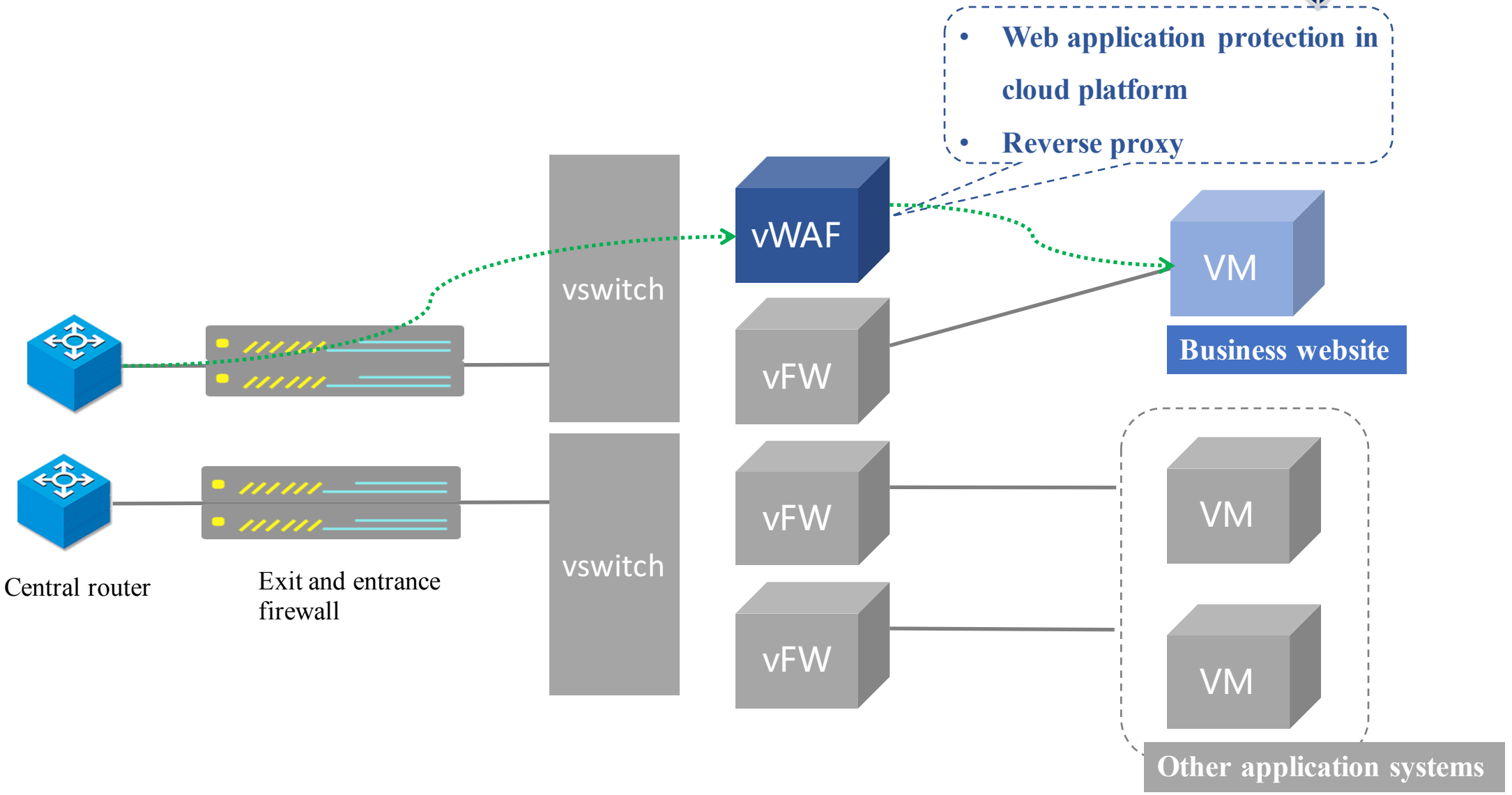
- Bridge pattern
- Web application security protection
- DDOS attack prevention
- Server load balancing to ensure service quality

Deployment (reverse proxy)

- Reverse proxy pattern
- Web application security protection
- Web access control
- Server load balancing to ensure service quality



Deployment (cloud platform)



Product Series

蓝盾 BLUEDON 智慧安全领导者 蓝盾股份:300297

BD-M Series

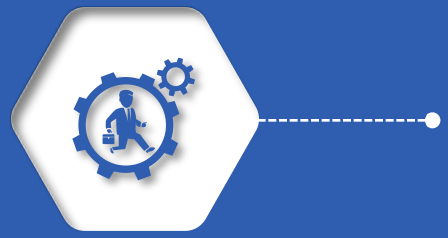
200M~850M
Suitable for SMEs

BD-G Series

1000M
Suitable for medium-sized enterprises

BD-T Series

10G
Suitable for large enterprises



Value

Value

蓝盾 BLUEDON 智慧安全领导者 蓝盾股份:300297

Improve website security

· Comprehensive web attack prevention to defend against common attacks like SQL injection and XSS;

· Information leakage prevention and strict web access control to prevent clients' information and website sensitive information from being leaked;

· Exclusive self-learning modeling technology to quickly identify abnormal behavior and automatically generate protection rules.

Improve service quality

· Collaborate with CloudFence to defend against DDOS so as to ensure service availability;

· Crawler and hot link prevention to prevent occupation of website resources

· Cache acceleration to improve access speed

· Load balancing to improve service quality and better user access experience.

Real-time security monitoring

· Real-time monitoring and alert of security events for the convenience of emergency response;

·Real-time presentation of website‘s operation status and service quality;

·Intuitive log report to guarantee easy and better understanding for users.

Thank you