Web动态防御系统在电网的应用研究

Study on Application of Web Dynamic Defense System in Power Grid

冯铭能，王　欣，梁辰恺（中讯邮电咨询设计院有限公司广东分公司，广东 广州 510627）
Feng Mingneng，Wang Xin，Liang Chenkai（China Information Technology Designing & Consulting Institute Co.，Ltd. Guangdong Branch，Guangzhou 510627，China）

摘　要：
目前电网Web应用主要通过传统WAF防火墙进行防护，传统WAF过于依赖特征库，存在误报和漏报、维护成本高等问题。基于Web动态防御系统采用先进的动态防御理念以及传统的静态特征过滤，构建“动态欺骗”+“静态防御”的防御体系，保护电网Web应用服务器免于自动化攻击，大幅降低电网企业对抗新兴安全威胁的难度，全面提升电网Web应用的安全性。

关键词：
Web应用防火墙；动态防御；智能电网
doi：10.12045/j.issn.1007-3043.2022.03.008
文章编号：1007-3043（2022）03-0042-06
中图分类号：TN918
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
At present，the Web application of the power grid is mainly protected by the traditional WAF firewall. The traditional WAF is too dependent on the feature library，which has the problems of false alarm，missing alarm and high maintenance. Based on the Web dynamic defense system，the advanced dynamic defense concept and traditional static feature filtering are adopted to build a "dynamic deception" + "static defense" defense system，which protects the power grid Web application server from automatic attacks，greatly reduces the difficulty of power grid enterprises against emerging security threats，and comprehensively improves the security of power grid Web applications.

Keywords：
Web application firewall；Dynamic defense；Smart grid

引用格式：冯铭能，王欣，梁辰恺. Web动态防御系统在电网的应用研究[J]. 邮电设计技术，2022（3）：42-47.

1 概述

近年来，Web应用的攻击事件层出不穷，2019年上半年，CNCERT监测发现并协调处置我国境内遭篡改的网站有近4万个，其中被篡改的政府网站有222个，Web安全形势不容乐观。在应对网站Web攻击中，Web应用防火墙（Web Application Firewall，WAF）提供应用层安全防护，通过对HTTP/HTTPS应用层数据的深度检测分析识别，阻断传统网络防火墙无法识别的Web应用攻击行为。传统WAF主要的功能如图1所示。

a）漏洞攻击防护：网站安全防护目前可拦截常见的Web漏洞攻击，如SQL注入、XSS跨站、获取敏感信息、利用开源组件漏洞进行攻击等常见的攻击行为。

b）自定义攻击特征：当发现有未公开的0Day漏洞，或者刚公开但未修复的NDay漏洞被利用时，WAF可以在发现漏洞到用户修复漏洞这段空档期通过自定义的正则表达式，对漏洞特征进行识别，抵挡黑客的攻击，保障网站安全。

随着Web攻击的变异升级，传统WAF过于依赖特征库，存在误报和漏报、维护成本高等问题，已无法满足日益增多的网页攻击防护需求，传统WAF主要存在

收稿日期：2022-01-20

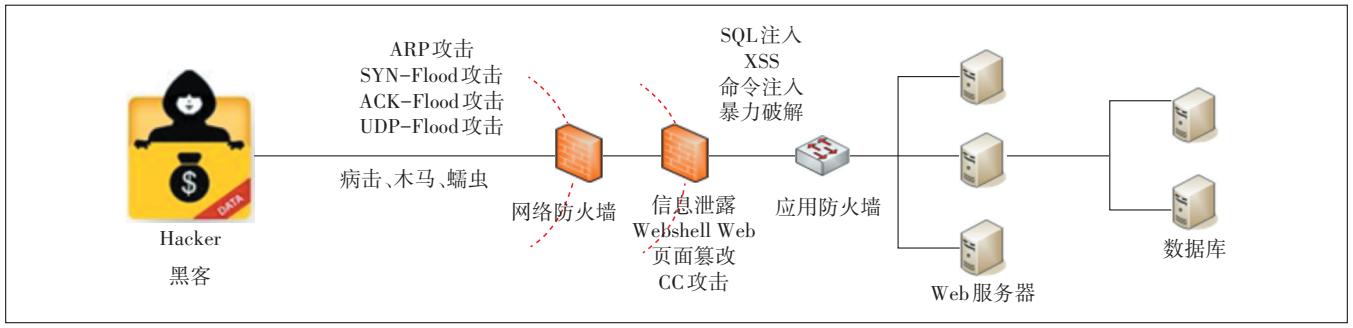

图1　WAF部署示意图

以下问题。

a）规则依赖性高：传统WAF基于特征库的防护方式，对0day攻击等新型攻击和各种自动化和程序化的恶意流量，无法有效防御，并且经常出现误判。由于WAF是基于事前的规则和签名技术，使用规则匹配引擎，WAF的好坏就取决于签名和引擎规则的质量。

b）维护复杂：由于攻击种类繁多，并且企业的互联网业务更新速度加快，传统WAF产品运维复杂，企业的安全运维成本不断攀高。部署新的Web应用后，需要投入大量的运维人员，运维人员需要掌握配置规则，人工成本高。

c）防护被动性高：由于WAF是基于事先的规则和签名技术，只能对已发现且已配置规则的攻击进行防护。

d）人员要求高：通常在Web应用程序新版本发布后，需要重新修改WAF的配置，要求维护人员必须能掌握基于新应用的规则。

传统防御方式属于战术手段，见招拆招、被动防守，治标不治本，攻击者总有办法绕过。因此Web应用防护需要从战略层面引入主动防御机制。

2 电网Web应用安全需求分析

根据国家能源局的《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范》文件要求，电力监控系统安全防护的总体原则为“安全分区、网络专用、横向隔离、纵向认证”。安全防护主要是针对电力监控系统，需重点强化边界防护，加强内部的物理、网络、主机、应用和数据安全，完善安全管理制度、机构、人员、系统建设、系统运维的管理，提高系统整体安全防护能力，保证电力监控系统及重要数据的安全。

参考《电力监控系统安全防护规定》的要求，安全防护总体方案的框架结构如图2所示。

根据要求允许非控制区内部业务系统采用B/S结构，但仅限于业务系统内部使用。允许提供纵向安全Web服务，但应当优先采用专用协议和专用浏览器的图形浏览技术，也可以采用经过安全加固且支持HTTPS的安全Web服务。

当前电网Web应用仍采用传统WAF防火墙进行防护，Web应用安全面临前所未有的挑战，传统WAF疲于应对越发复杂多变的攻击，急需引入主动的防御手段，对攻击者进行降维打击，动静结合构建战略性Web应用安全防御体系。

3 基于Web动态防御的安全防护方案

3.1 整体架构

采用先进的动态防御理念以及传统的静态特征过滤，构建“动态欺骗”+“静态防御”的防御体系可以极大地提升黑客入侵的难度和Web业务的安全防护能力，同时这种防御体系的易用性和兼容性极大地降低了安全部门的运维成本，也对业务系统提供了非常有价值的纯净的用户访问数据。“WAF+动态防御”Web应用安全总体架构如图3所示。

3.2 技术原理

动态防御技术的核心是对网页的敏感接口的URL地址进行动态变换，客户端环境和客户行为进行动态验证，并且为网页提供一次性动态Cookie令牌，具体如图4所示。

3.2.1 URL地址变换

动态防御技术通过对网页URL地址做动态封装，隐藏攻击入口，避免其成为网络攻击目标。每个用户每次请求的URL地址都是随机的，无法被预测的，并且该动态URL可配置有效次数和有效时间。这样可保障业务逻辑的正确运行并防止攻击者发出非法请

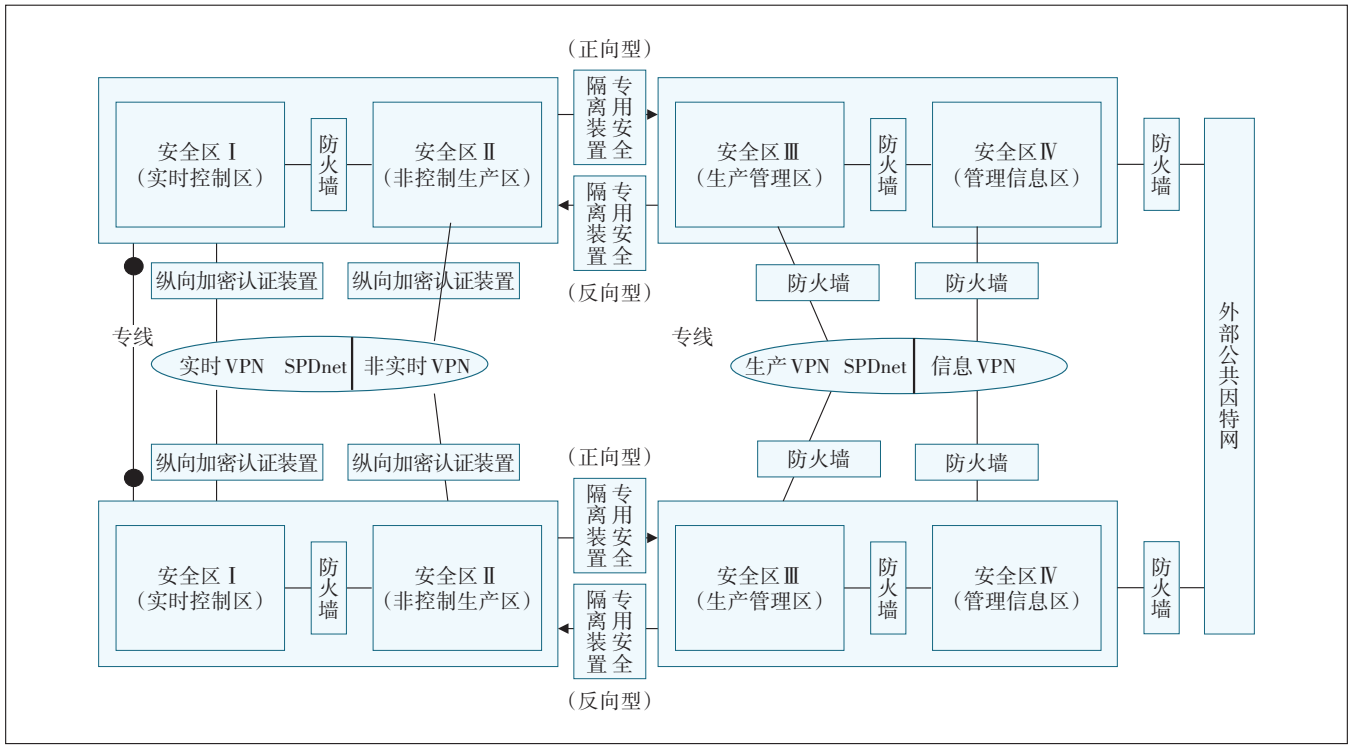

图2　电网安全防护总体方案的框架结构

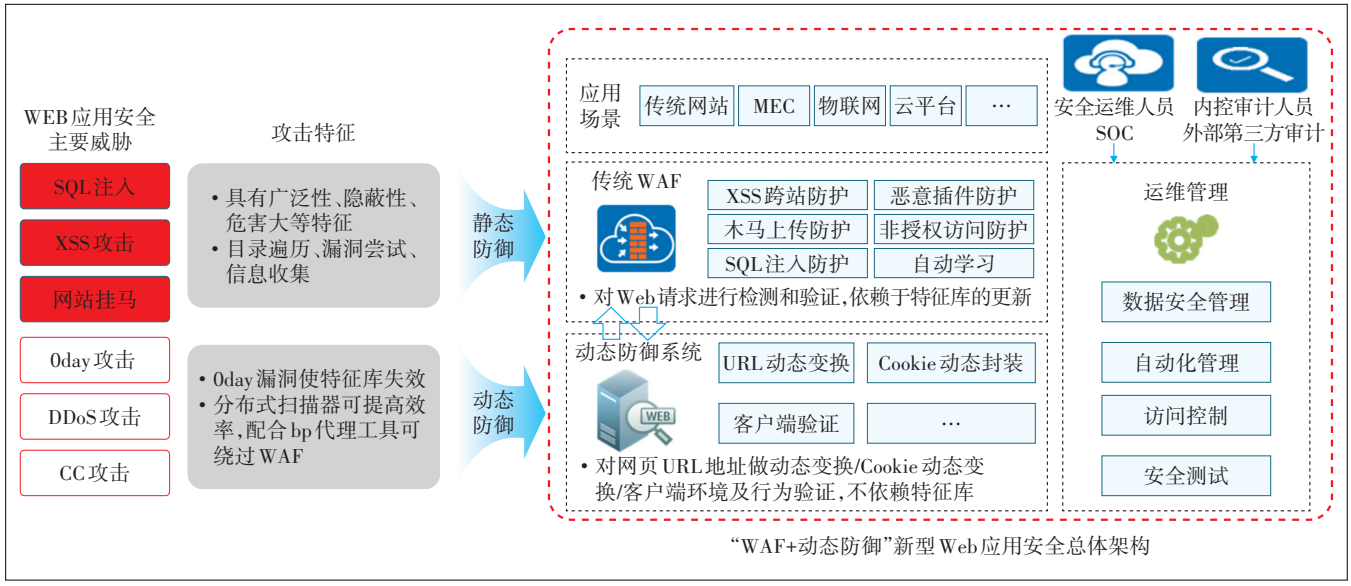

图3　“WAF+动态防御”Web应用安全总体架构

求，抵御越权访问、网页后门、重放攻击、应用层DDoS等自动化恶意攻击行为。

3.2.2 Cookie变换

动态防御技术在网页中插入一个新Cookie，动态生成新的Cookie，根据用户行为模型和二次计算来确定是正常访问还是攻击行为。通过Cookie的动态变化可以有效阻挡各种脚本和程序的攻击，提升攻击复杂度和难度，增加时间和经济成本。

3.2.3 客户端环境及行为验证

动态防御技术通过对客户端环境和行为进行校验，验证是“人”还是“自动化”，根据浏览器的特征、环境参数以及用户的行为、动作来进行判断，包括但不限于鼠标、键盘等行为。

客户端环境及行为验证方式可以有效防护各种

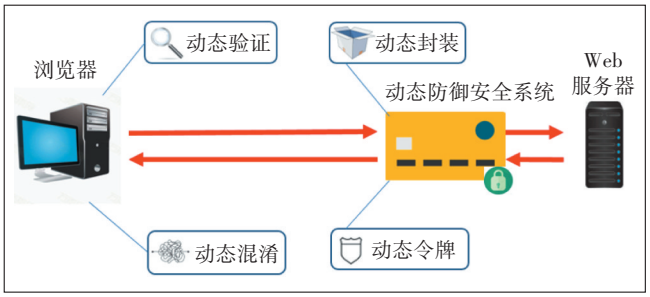

图4　动态防御系统部署示意图

攻击软件，包括常用代理调试工具、恶意插件等恶意软件，可以识别攻击者通过修改浏览器的属性冒充新用户进行攻击的行为。

3.3 部署方案

Web动态防御平台并非完全替代传统的WAF，而是在原有的WAF上增加一道防线，补齐WAF的短板。Web动态防御平台以软件安装包的形式安装在服务器上，实现负载均衡，反向代理，以及业务安全防护等功能，这样更加容易部署和管理，并且不需要对现有的应用架构做任何的改动。具体部署方式如图5所示。

3.4 效果分析

Web动态防御平台通过欺骗手段来阻止和扰乱攻击者的认知过程，对抗各种自动化攻击工具，极大地提升黑客攻击难度和成本。实验室攻防演练结果显示部署防御系统后效果非常明显，在使用Web动态防御平台的保护后，扫描工具检测不到strust2漏洞的存在，部署效果如图6所示。

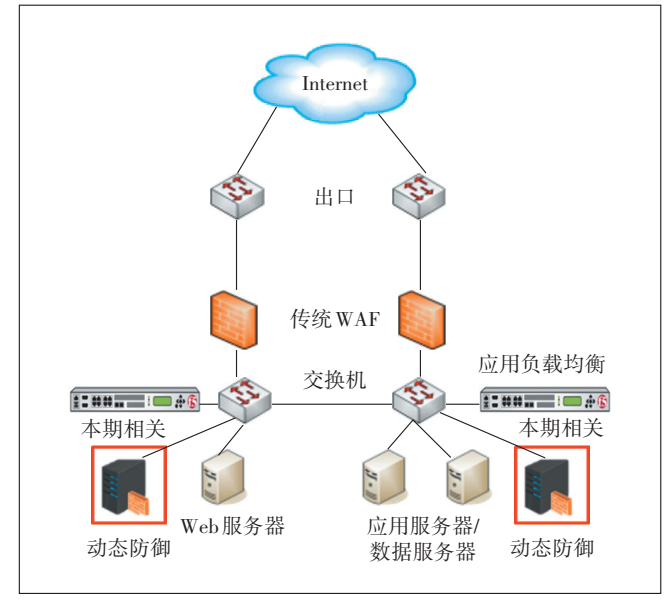

图5　“WAF+动态防御”部署示意图

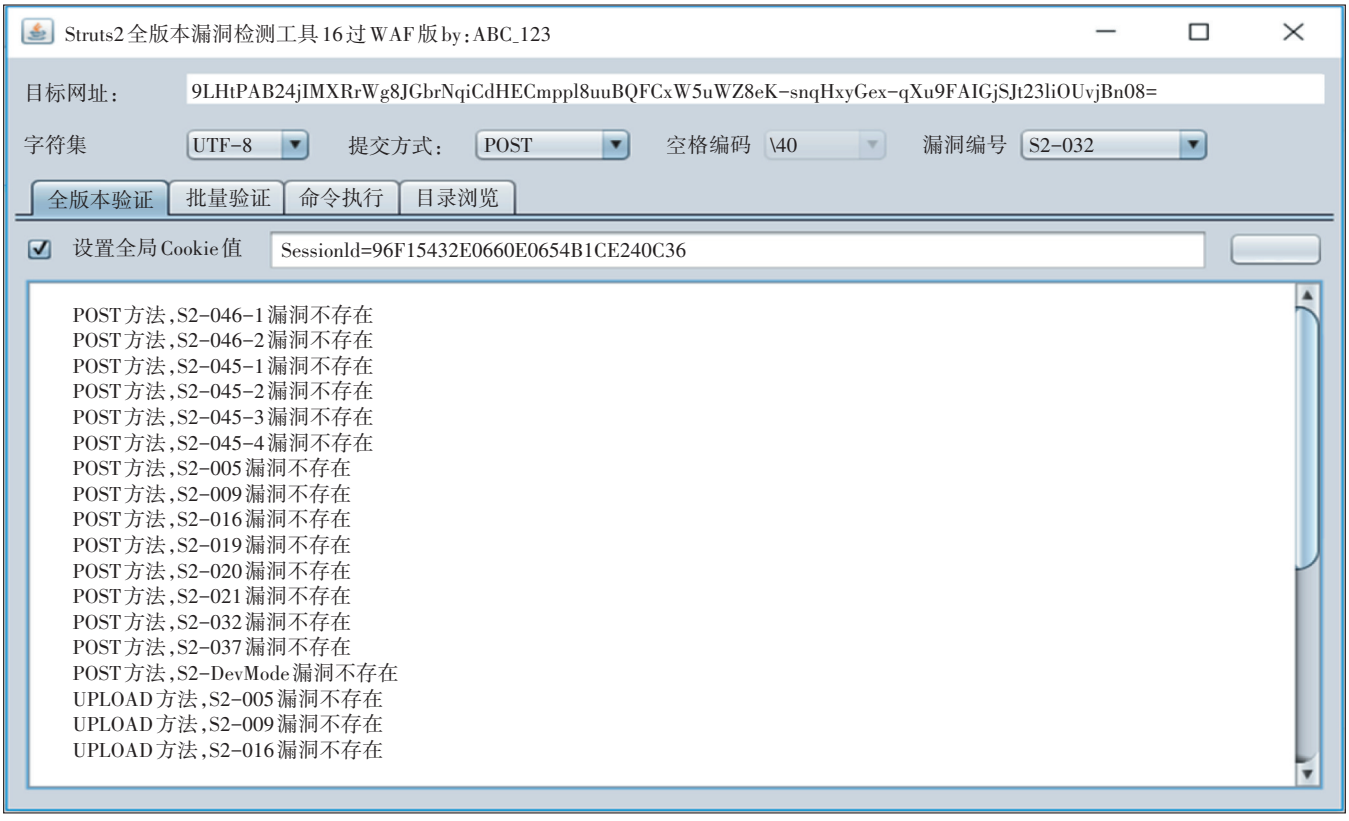

图6　部署效果分析

经过实验室和现网的真实环境测试，平台可涵盖目前已知的99%的攻击和漏洞。

4 Web动态防御电网应用场景分析

4.1 电网Web应用防护

目前电网企业运行各类Web网站，可在“WAF+动态防御”Web应用安全总体架构下，对非法的请求予以实时阻断，对各类网站进行有效防护。具体部署情况如图7所示。

4.2 电网物联网防护

随着泛在电力物联网建设不断推进，中低压配电网各类传感感知类装置快速增长，这使安全风险防范压力剧增。结合等保2.0要求，电网物联网在“WAF+动态防御”Web应用安全总体防护下，能有效对抗物

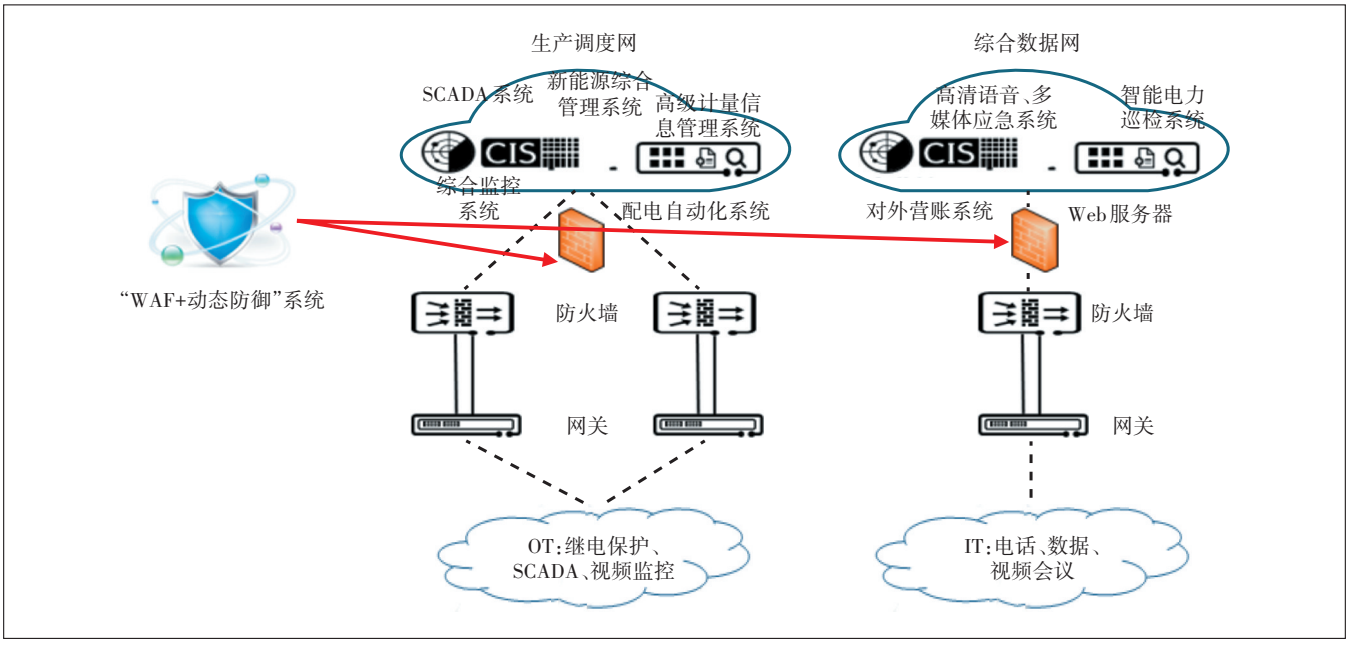

图7　电网Web应用防护

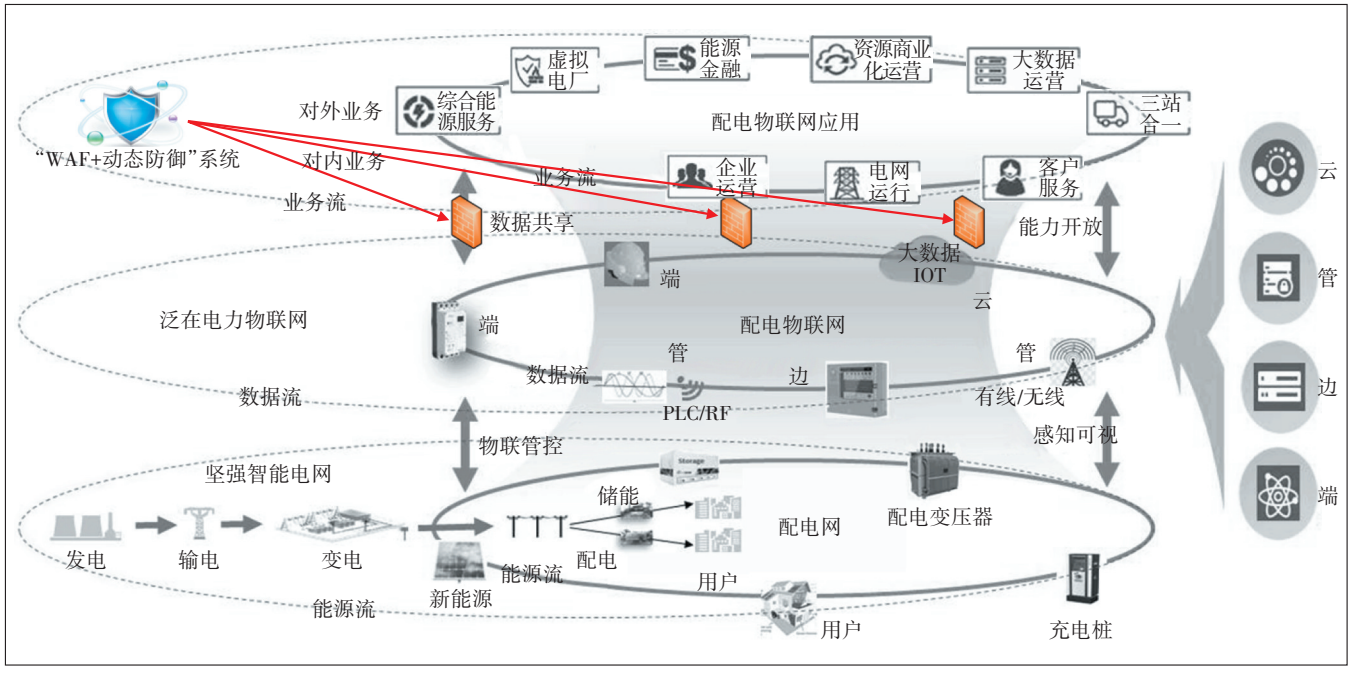

图8　电网物联网防护示意图

联网的安全威胁与挑战。具体部署位置如图8所示。

4.3 电网MEC防护

目前MEC仅部署普通防火墙进行防护，安全防护较薄弱，可以通过引入“WAF+动态防御 ”Web应用安全系统，对MEC及相关业务进行全面防护，提升安全等级，具体部署方式如图9所示。

5 Web动态防御应用价值分析

动态防御技术不需要修改任何应用服务器代码，部署于应用服务器前，即可保护应用服务器免于自动化攻击，大幅降低企业对抗新兴安全威胁的难度；同时其没有规则库、签名文件等，部署简单方便。具体的应用价值如下。

a）增强业务安全防护。动态防御技术可以有效对抗各种基于脚本和工具的自动化或半自动化的攻击，极大减少了业务在互联网上的暴露面，大大降低了业务被攻击的几率，保障互联网业务的快速发布和推广。

b）增强大数据安全防护。对后台大数据平台进行用户数据“降噪”处理，提升后台大数据对业务系统的分析效率；同时防止恶意爬取大数据后台数据的恶意行为。

c）等保2.0监管合规。可以有效应对0Day漏洞以及各种监管机构的监管合规要求，也可以在紧急情况下为企业赢得更多的安全应急响应时间。

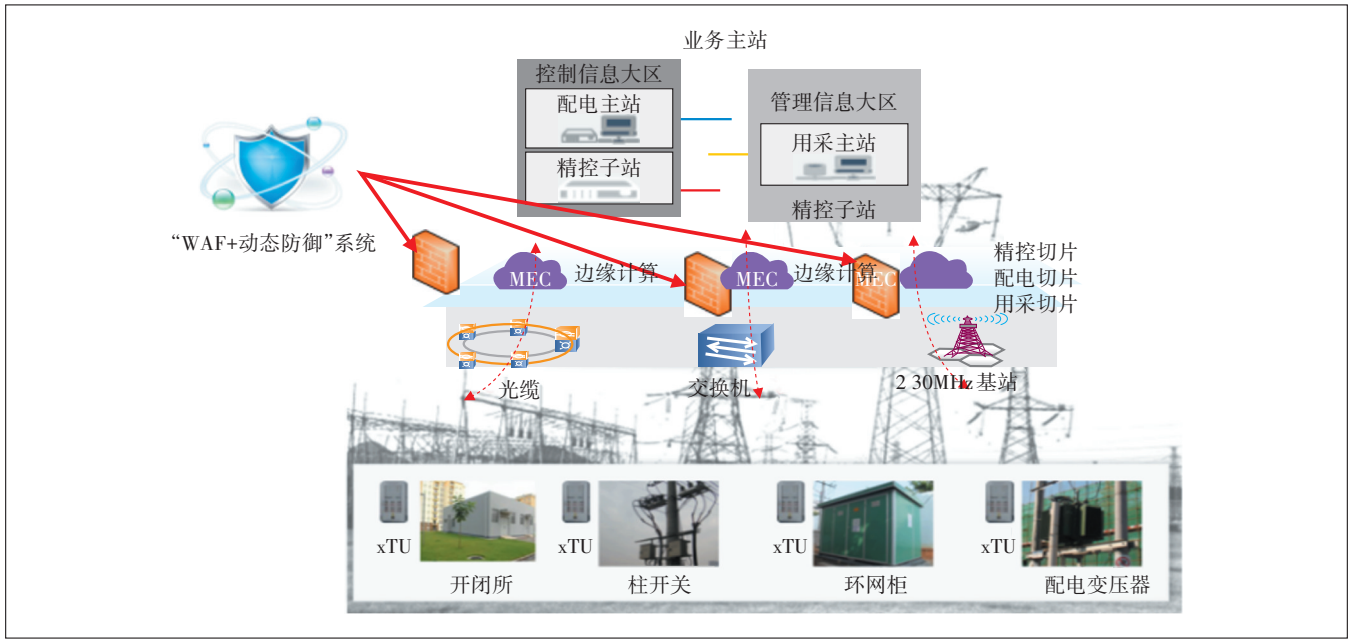

图9　电网MEC防护示意图

d）降低运维成本及人力要求：不依赖规则库的防御机制，大大降低了企业的后期安全运维成本；同时通过阻挡大量的自动化请求或攻击，可以节省网络带宽和服务器系统资源，减少企业每年在系统运维方面的投入。

6 结束语

本文根据电力监控系统安全防护总体要求，分析电网企业Web应用部署现状和存在的问题，提出在电网典型应用场景部署Web动态防御系统，构建“动态欺骗”+“静态防御”的防御体系，这样可以增加黑客入侵的难度和提升Web业务的安全防护能力，降低企业安全运维成本，全面提升电网网络安全性。

参考文献：

[1] 杨东晓，王嘉，程洋. Web应用防火墙技术及应用[M]. 北京：清华大学出版社，2019.
[2] 杨林，于全. 动态赋能网络空间防御[M]. 北京：人民邮电出版社，2018.
[3] 徐焱.Web安全攻防渗透测试实战指南[M]. 北京：电子工业出版社，2018.

作者简介：
冯铭能，高级工程师，博士，主要从事数据网、核心网、电力通信网的相关咨询设计工作；
王欣，高级工程师，，学士，主要从事数据网、核心网、电力通信网的相关咨询设计工作；
梁辰恺，助理工程师，硕士，主要从事IT、无线网、软件工程的相关咨询设计工作。