关于云防护方案的调研报告

近日，公司统一信息披露平台项目即将立项建设，为增强公司互联网信息系统的安全防护能力，妥善应对信息系统可能遭受的拒绝服务攻击、入侵攻击、恶意扫描等攻击行为，结合统一信息披露平台的安全防护需求，降低信息系统总体建设及运维成本，根据公司领导要求，我部调研了云防护服务情况，现将相关情况报告如下：

一、**安全防护需求**

根据公司统一信息披露平台的安全防护需求，结合我部在公司互联网信息系统扫描中发现的安全问题，公司互联网信息系统安全防护应具备以下能力：

1、防御常见WEB攻击、漏洞攻击、恶意扫描等攻击；

2、防御一定规模的流量攻击、CC攻击等拒绝服务攻击；

3、通过链路负载均衡满足两条运营商互联网线路的正常访问；

4、通过CDN加速等方式提高应用访问速度和稳定性。

按照证联网部提供的系统建设方案和安全产品指标要求，原有方案采取本地部署安全设备，如图1所示：

1、抗DDOS设备防护拒绝服务攻击；

2、链路负载均衡设备动态调节联通和移动两条线路的访问流量；

3、IPS设备、WAF设备防护系统攻击、WEB攻击；

4、CDN技术对网站访问进行加速。

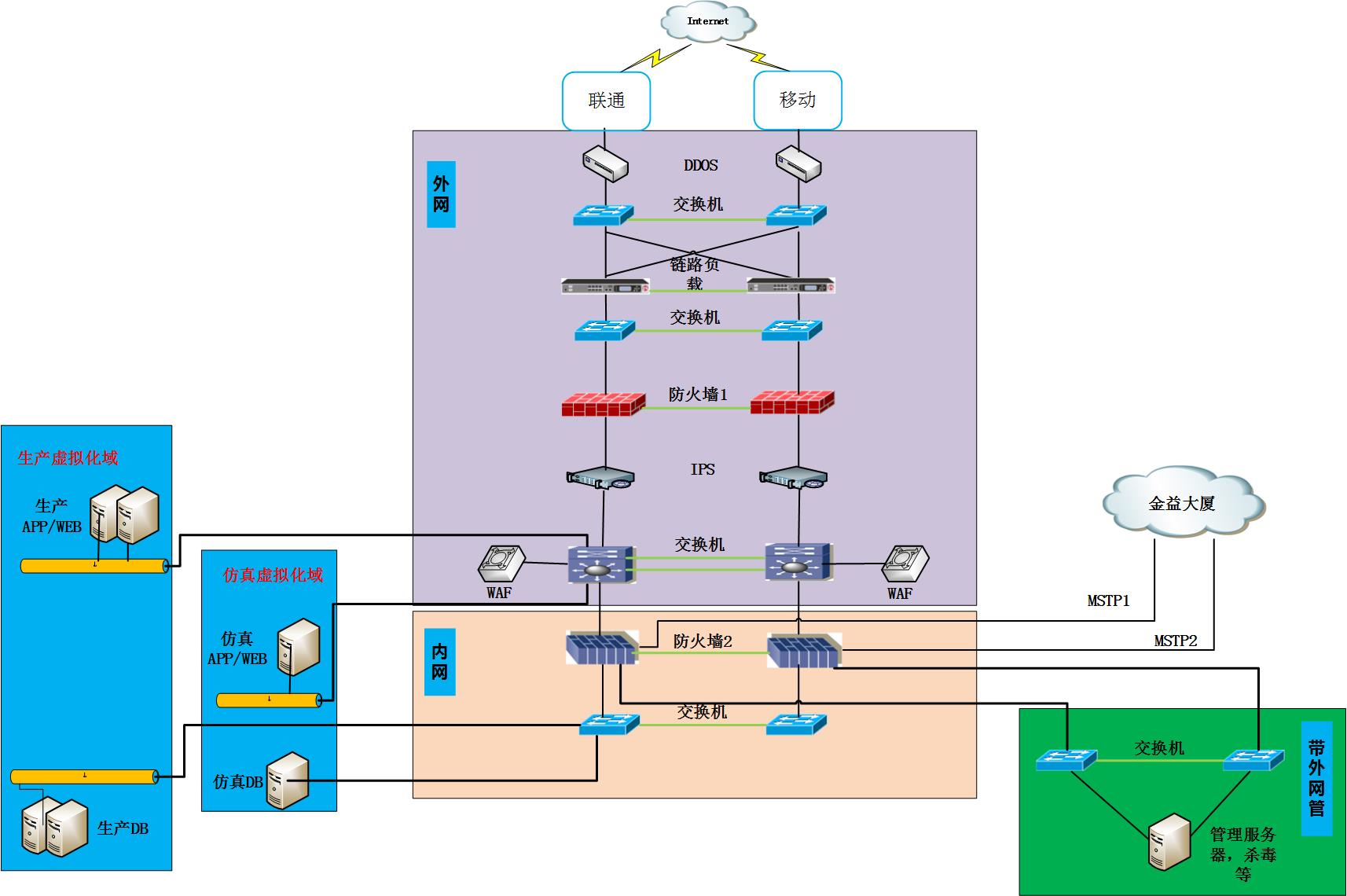


图1：本地部署设备示意图

二、云防护服务情况

云防护服务是近两年新兴的安全防护模式，服务提供方通过互联网建立大规模的防护集群，向服务使用方提供抗拒绝服务攻击防护、WEB攻击防护、CDN加速服务等安全防护。服务使用方通过修改网站的域名解析到云防护提供商的防护节点，获取对应的安全防护能力。

目前云防护服务提供的安全功能主要包括以下方面，完全能够实现我们的防护需求：

1、WEB攻击防护，可对WEB攻击手段进行防护，将过滤后的正常访问流量转发给后端服务器。

2、DDoS防护：云防护服务提供商在互联网建立多个防护中心，可发现业务流量中的攻击流量，并对流量进行清洗，将过滤后的正常访问流量转发给后端服务器。

3、链路负载均衡：云防护平台支持对用户的多条互联网线路进行轮询访问。

4、CDN加速：利用DNS多线路解析和缓存技术，智能选择响应速度最快的线路。

如采取云防护服务，服务接入示意如图2所示。只将被防护网站的域名别名记录（CNAME）指向云防护服务商的防护节点，两条互联网专线正常配置即可。

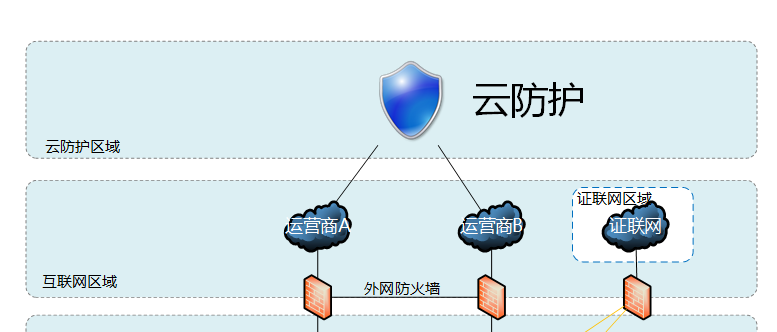


图2 云防护接入示意

我们对两种模式进行了比较（如表1所示），云防护服务在采购成本、扩展能力、线路带宽、防护技术等方面具备一定优势，更加符合我们的需求，建议选择云防护服务模式。

表1采购模式比较

|  |  |  |
| --- | --- | --- |
|  | **自行采购安全设备模式** | **租赁云防护服务模式** |
| 采购成本 | 购买全套安全设备，一次性投入成本较大 | 按服务年度付费，年度投入成本较低 |
| 扩展能力 | 扩展性差，如提升防护能力需要重新购置设备 | 扩展灵活，按需使用，向服务商购买扩展能力 |
| 部署维护 | 自行部署硬件设备，配备维护人员进行设备维护、策略调整等 | 无需本地部署设备，维护人员只需查看服务商推送的有效告警即可 |
| 网络带宽要求 | 考虑互联网大规模并发请求，线路带宽要求较大 | 只需跟服务商云节点通信，降低线路带宽要求 |
| 抗DDOS防护能力 | 出口带宽及设备性能决定，只能防御小规模攻击 | 服务商部署多个节点分担攻击流量，支持防御较大规模的流量攻击 |
| WEB攻击防护能力 | 支持用户自定义策略，但需专门人员配置维护 | 能利用服务商专业安全能力，无需用户自定义策略 |

三、云防护服务工作模式

云防护服务工作模式如图3所示：

1、公司网站侧的配置：在域名注册商处将域名解析配置为域名别名记录（CNAME）；在云防护节点处配置CNAME和防护站点IP地址对应记录；公司防火墙配置容许云防护节点访问。

2、对于使用域名访问的用户流量，用户通过域名DNS Server查询解析，获取云防护节点的IP地址；访问请求发往云防护节点；云防护节点通过安全检测、过滤后，将正常访问流量传递给公司网站；将恶意攻击流量进行过滤，起到防护作用。如图2中1-7所示。

3、对于直接访问网站IP地址的流量，公司防火墙直接拒绝访问，起到防护作用。

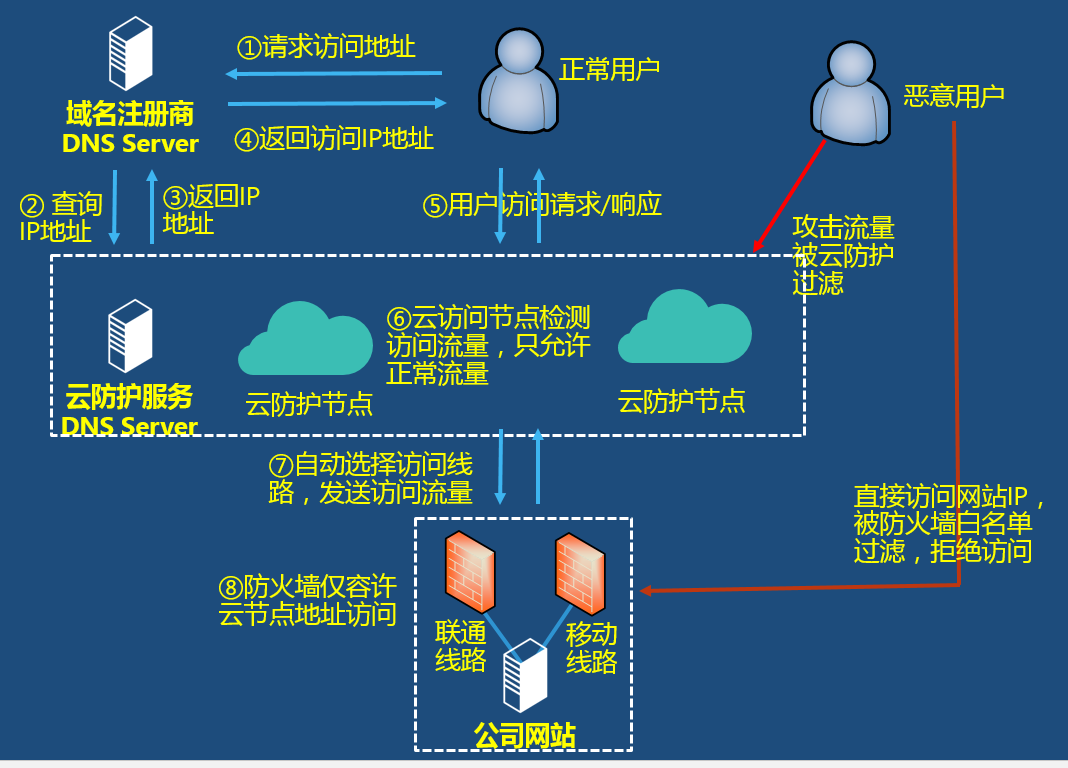


图3 云防护服务工作模式

云防护服务内容主要包括安全防护和CDN加速两大类，其中安全防护主要包括WEB攻击防护、恶意扫描防护、抗拒绝服务攻击、网站防篡改锁定等安全功能；CDN加速是通过CDN节点缓存提高页面访问速度。

四、云防护服务商调研

云防护服务为近两年新兴的服务模式，由于云防护服务商需要在互联网上建立大规模的安全防护集群，中小规模的安全企业很难提供类似服务。目前提供云防护服务的多为互联网安全企业，尤其是有腾讯、百度、阿里、360等互联网企业支持的安全企业。

（一）知道创宇公司的创宇盾

创宇盾是北京知道创宇公司开发的一款基于云与大数据技术的Web系统云防御平台。在全国各重要互联网节点建立了 30个高防高性能机房，共500G骨干网带宽，以公有云或私有云方式提供集中防护。目前创宇盾共为83万网站提供安全防护，其中重点客户包括有公安部、人民银行、工信部、CNCERT。

支持我们全部4个安全需求。支持常见WEB攻击防御，防护策略更新速度较快，在WEB安全方面有优势；支持整站锁功能，可在重保期间缓存所有静态页面，防止被篡改；全国部署有30多个CDN节点；能够防御100G级别的DDOS攻击。

收费模式方面，CDN服务按访问流量包年收费，基础流量每月20TB，远远超过IPO等网站目前访问流量，无需考虑流量超标的情况，即使后续有新网站上线，也无需再额外购买流量包；抗DDOS按攻击流量包年收费，基础流量为峰值5Gbps，也可根据攻击流量按次收费。公司网站目前未遭受过DDOS攻击，5Gbps可满足一般情况下需要。如发生大流量DDOS攻击，可按攻击流量按次计算费用；WEB攻击防御按域名数包年收费；链路负载均衡为默认功能，无需付费。

（二）奇虎360公司的安全CDN

360安全CDN为大中型国有企业、国家部委、电商网站、政府科研机构、金融机构以及中小型网站量身打造的网站安全加速平台。

支持我们全部4个安全需求。支持常见WEB攻击防御，防护策略更新速度较快，自带漏洞扫描功能；全国有40多个CDN节点，计划扩充到160个；450G抗DDOS流量，可根据DDOS攻击流量大小进行调整。

收费模式方面，CDN服务按访问流量包年收费；抗DDOS按攻击流量包年收费；WEB攻击防御按域名数包年收费；链路负载均衡为默认功能，无需付费。重点客户有国家电网、海南航空。

（三）阿里云盾服务

云盾是阿里巴巴集团多年来安全技术研究积累的成果，结合阿里云计算平台强大的数据分析能力，提供DDoS防护，主机入侵防护，以及漏洞检测、木马检测等一整套安全服务。

云盾与阿里云服务结合较为紧密，之前仅支持阿里云线上部署模式，近期可支持非阿里云的用户。

收费模式方面，所有服务按流量包年收费。每月基础流量不超过20Gbps为固定费用，如当月其中一天流量超标，需额外购买流量包。流量包可叠加购买。

（四）星云融创公司安全宝

公司规模相对较小，被百度云全资收购。支持常见WEB攻击防御，部分需要在用户机房部署硬件设备；全国有22个CDN节点；能够防御100G级别的DDOS攻击，提供专家支持服务。收费模式方面，所有服务按包年收费，按服务支持力度分为4种套餐。重点客户有嘀嘀打车。

四、云防护服务费用情况

根据我们了解，云服务服务费用主要分为三部分，一是基础防护费用，实现WEB攻击、系统攻击等功能；二是CDN流量费用，根据不同流量级别收费；三是DDOS攻击流量费用，根据不同规模攻击峰值收费。以下是官方报价，预计真正采购时会有一定程度下降，供参考。

（一）知道创宇公司的创宇盾



（二）奇虎360公司的安全CDN

服务套餐分为3档，

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 基础功能 | CDN流量 | DDOS流量 | 官方报价 |
| 1档 | 有 | 1T/月 | 5G | 25万/年 |
| 2档 | 有 | 5T/月 | 10G | 45万/年 |
| 3档 | 有 | 10T/月 | 50G | 80万/年 |

据360公司介绍，如不需要CDN流量加速，基础功能防护报价可有大幅下降。

（三）阿里云盾

所有服务按使用流量计费。

|  |  |  |  |
| --- | --- | --- | --- |
| 套餐 | 用量 | 费用 | 备注 |
| 基础包 | 20Gbps以内 | 1.68万/月 | 包括DDOS防护、入侵防护、漏洞检测 |
| 流量包 | 100Gbps | 1000元/天 | 超过100Gbps可购买多个流量包叠加 |

（四）星云融创公司安全宝



五、厂商能力对比

各家厂商的主要差别体现在以下几方面：

1、WEB安全防护

知道创宇公司目前为83万网站提供安全防护，包括国家部委和金融领域知名企业。从20XX年开始对外提供服务，运营经验丰富，客户支持力度高。

360公司免费用户有130万，付费用户数有7000多个，从2011年开始对外提供服务，运营时间较长，但360公司重点在个人和桌面安全，对企业客户支持力度不大。云服务不直接面对最终用户，一般委托代理商签署合同。

阿里云盾主要为部署在阿里云上的网站提供安全防护，2015年才开始为外部客户提供云防护服务，对外部用户支持力度较小。

安全宝用户量20多万，主要客户为一些中小企业。

2、DDOS攻击防护

知道创宇和360公司规模最大，云节点数在30个以上，云主机数在1000台以上，防御带宽在300G以上，并且有防御100G以上DDOS攻击的案例。

安全宝在全国有20个云节点，提供最高200G流量的DDOS防护。

3、CDN加速服务

知道创宇和阿里云公司CDN基础流量较高，能够满足目前公司网站访问需要，即使未来网站扩容或增加站点，也无需购买额外的流量包。

360公司CDN服务和安全防护属于两个产品，如果后期服务出现问题，可能在沟通协调上存在障碍。另外360公司的安全防护和CDN没有统一的管理界面，管理和维护不方便。

阿里云公司CDN服务情况和360公司相同。

4、其他方面

知道创宇公司、360和阿里云公司计费模式灵活，都支持每月基础流量加扩展流量的方式，扩展流量部分为后付费模式，每月末单独计费。安全宝为纯包月模式，基础流量较低，但超过流量时费用较高。

六、注意事项

采取云防护有几个注意事项：

一是部署云防护产品，需要更改域名的DNS解析指向。披露网IPO系统使用了证监会的二级域名，经咨询信息中心张立中处长，如修改DNS解析，需公司向信息中心正式发函说明情况。建议先将公司门户网站等系统先切换到云防护平台进行试用，待运行稳定后再切换csrc.gov.cn域名下的系统。

二是对于IPO、公司门户等静态资源为主、与用户交互少的重要网站可同时购买CDN服务和攻击防护服务，公司邮箱等网站CDN加速效果不明显，只需要购买攻击防护服务。

七、调研结论

云防护服务在采购成本、扩展能力、线路带宽、防护技术等方面具备一定优势，更加符合我们的需求。建议选择云防护服务模式，下一步可联系服务厂商安排试用。

综合各方面调研情况，知道创宇公司的创宇盾综合能力较强，建议作为本次云服务首选厂商；360公司的安全CDN和阿里云公司的云盾服务有部分能力较强，综合能力平均，建议作为次选厂商；安全宝公司各方面能力较一般，建议后续关注。