# 企业互联网边界安全解决方案

## 1 概述

随着计算机、宽带技术的迅速发展，网络办公日益流行，互联网已经成为人们工作、生活、学习过程中不可或缺、便捷高效的工具。越来越多的企业的正常运营依托于网络的高效稳定，而互联网的宽松自由的特点，也使其成为了恶意组织、黑客对企业实施攻击的通道。

互联网边界作为“网络大门”的角色，承载着所有访问互联网的进出流量。互联网边界安全需要解决“内忧外患”的问题，对内要规范企业员工合规上网的问题，对外要防御来自外部的攻击行为，保护企业 ERP、OA、CRM、企业邮箱等重要业务系统的正常运行。因此，边界安全是企业安全防护体系的重要阵地，同时互联网边界是企业网络的第一道防线，也是最后一道防线。

## 2 需求分析

### 2.1 防止互联网访问中造成恶意攻击

据 CNCERT《2016 年中国互联网网络安全报告》抽样监测，2016 年约 9.7 万个木马和僵尸网络控制服务器控制了我国境内 1699 万余台主机，共抽样监测到仿冒我国境内网站的钓鱼页面 177988 个，而且高级持续性威胁呈现常态化发展，截止到 2016 年底，针对我国境内目标发动攻击的 APT 组织有 36 个，我国面临的攻击威胁尤为严重，而互联网作为我国最大、使用最广泛的网络往往承受着更多、更高级的攻击威胁。

为了避免从互联网边界成功入侵企业的内网，在企业接入互联网后，一方面要避免内网用户访问钓鱼网站和被植入木马、病毒、勒索软件、访问恶意 URL 等威胁，另一方面要加强对高级持续性威胁的监控与拦截。

### 2.2 防止员工违规访问引发的企业风险

尽管互联网为我们提供了许多有价值的信息资源，但由于互联网本身所固有的开放性、国际性和无组织性，使网络上充斥着不良信息，要做到健康、合法的使用互联网，需要做到下面几点：

- 禁止企业员工访问宣传反动言论、色情、在线赌博、恐怖暴力以及封建迷信的站点；
- 管理员工上网行为，提高员工网上办公的效率禁止员工在上班时间使用 P2P 下载、炒股、网络视频、游戏等软件，提升员工的工作效率和带宽资源的合理使用；
- 防止员工在发帖、网络聊天中包含违规内容网上发布，要避免涉及政治敏感话题、法轮功、分裂主义等不利于社会稳定的违法言论从企业内部发布到互联网，降低企业的法律风险；
- 要及时发现并阻止可能与商业或研发机密有关的信息外泄，减少机密外

泄风险。并且在及时阻止的同时记录日志，实现事后追责。

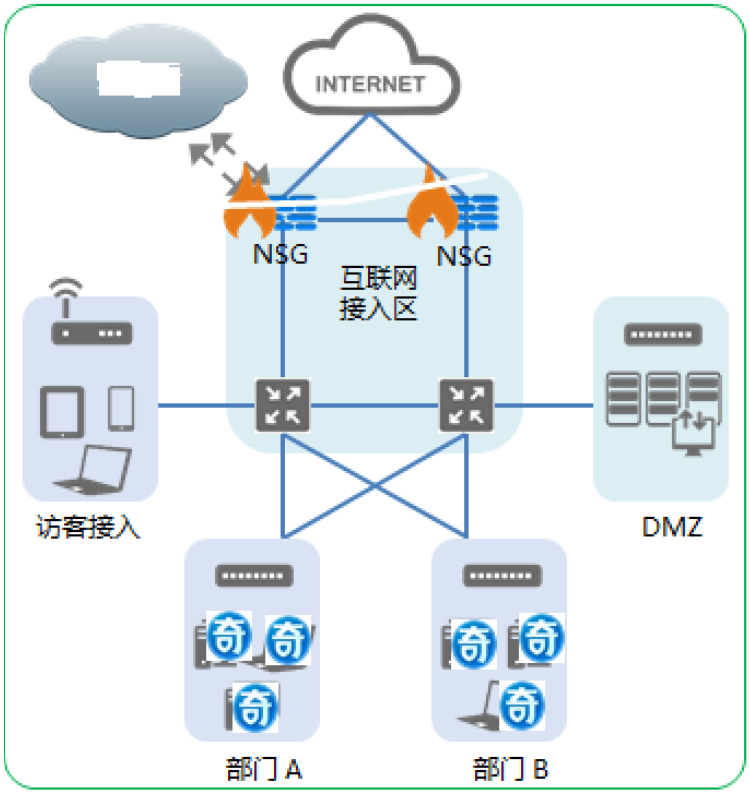
### 2.3 精准定位内部的失陷主机

“失陷主机”是指被攻击者成功侵入，行为特征符合“受到控制”或“发起恶意行为”的主机。当前，失陷主机已相当普遍，权威机构的一项研究表明，在PC数量超过5000的大型企业网络中，有超过90%的企业均存在活跃的失陷主机，而攻陷这些主机的原因多种多样。此外，由于失陷主机受控或发起恶意行为往往难寻规律、隐蔽性强，绝大部分已存在失陷主机的组织根本无法感知。因此，企业互联网边界需要建立检测失陷主机并及时处理的机制，防止因为失陷主机造成的信息外泄或者对外发起恶意攻击，使企业面临经济损失及法律风险。

## 3 解决方案

新一代智慧防火墙（以下简称“智慧防火墙”）是一款兼具复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御等能力，并超越性集成互联网威胁情报、异常行为分析、安全可视化等新一代安全技术的创新型边界安全产品。

如下图，智慧防火墙在互联网边界出口网络部署，基于其自身强大的应用、威胁识别能力和多维数据分析，能做到对通过互联网出口的流量高精度上网管控，通过与云安全服务的协同联动，打破传统防火墙的静态防御、单兵作战的防御模式，全面提升了边界防御能力。

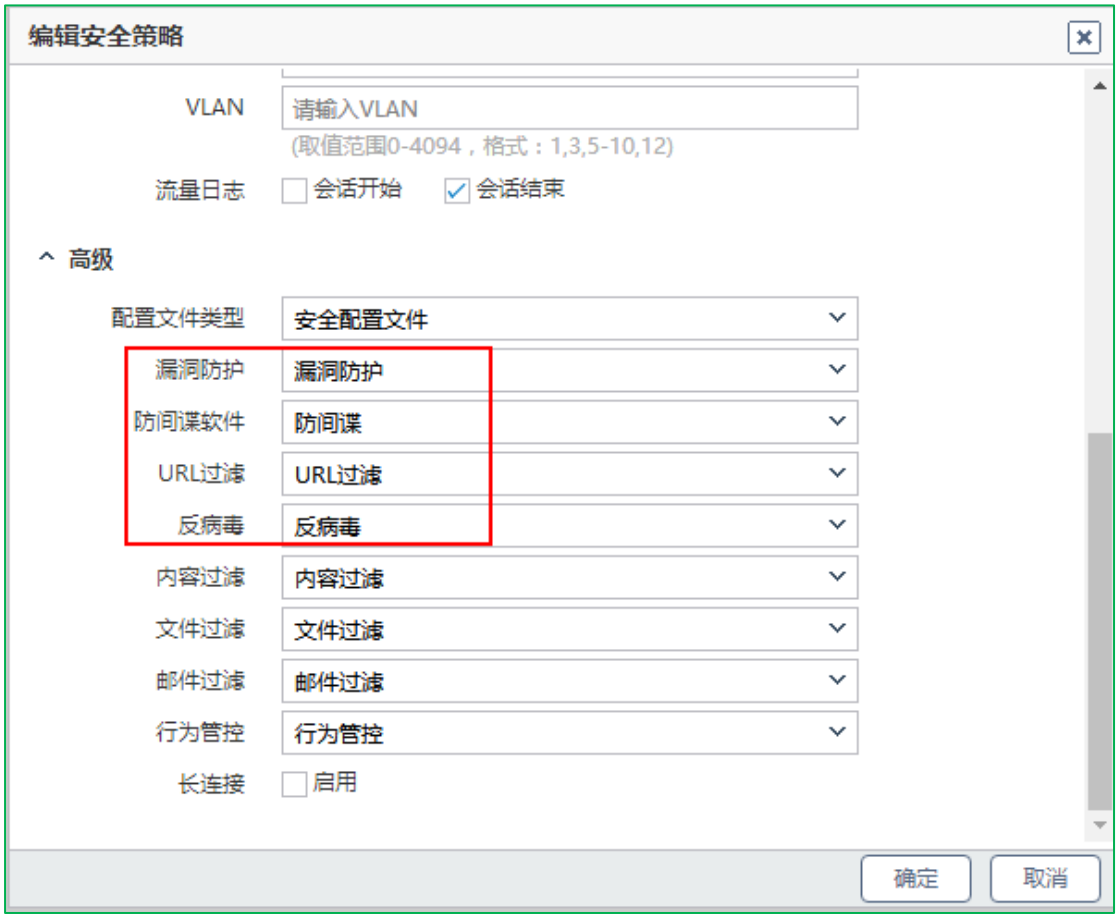



方案拓扑示意图

## 3.1 基于本地引擎和云端协防高效拦截外部威胁

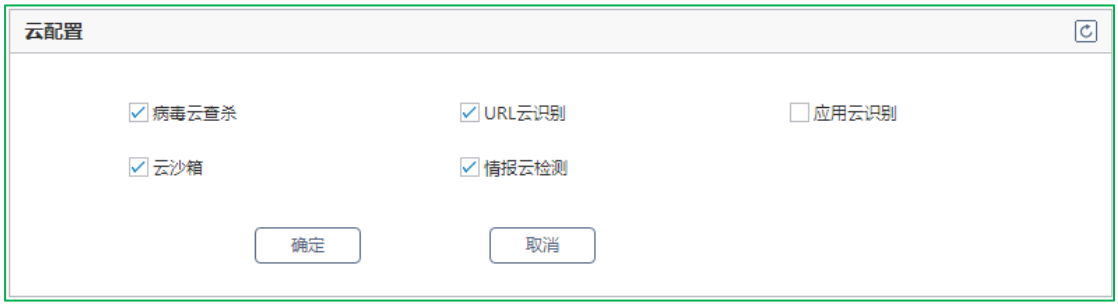
智慧防火墙通过启用一体化安全防护策略，将反病毒、漏洞防护、防间谍软件、恶意 URL 防护等功能集成到一条策略，并基于优越的架构设计保障高性能的安全能力。

通过在互联网边界启用智慧防火墙的漏洞防护、防间谍软件、反病毒、URL 过滤功能，基于本地安全引擎，能高效拦截常见漏洞入侵、间谍软件、病毒、木马、钓鱼网站、恶意 URL 访问等网络威胁。




一体化安全策略

同时，智慧防火墙专属的云安全服务，可为智慧防火墙提供云端的协防能力。在智慧防火墙本地启用病毒云查杀、URL 云识别、云沙箱、情报云检测等配置，即可实现智慧防火墙在检测到异常 URL、可疑文件时，将无法判断的内容上报至云进行进一步分析判定。




**云配置**

云安全服务基于强大的漏洞挖掘能力和情报收集分析能力，可为智慧防火墙提供威胁情报服务，智慧防火墙将互联网出口流量中的可疑行为的特征（可疑文件 MD5，可疑目的 IP，可疑 URL 等）发送到云上进行大数据分析，可有效发现高级威胁。


**来自安全云的威胁情报**

智慧防火墙通过云端协同可以极大提升特征库数量级，补充本地识别库，并提升防火墙对高级威胁的识别能力，提高防火墙拦截的精确度和高效性。

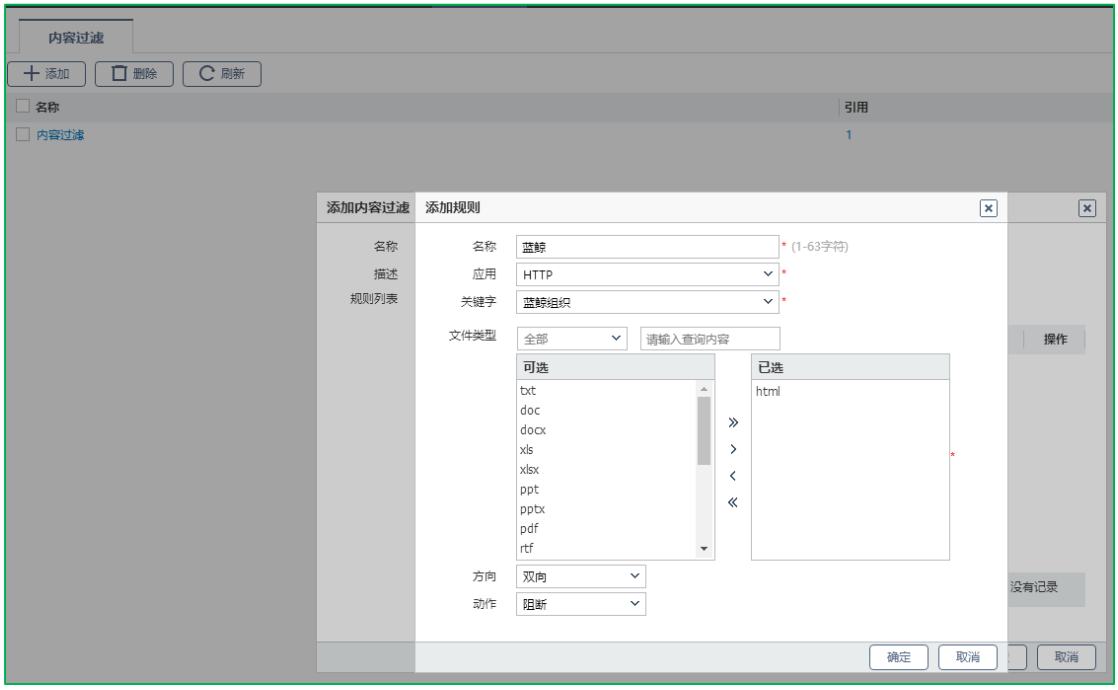
## 3.2 启用精细化、细粒度的上网管控策略

基于智慧防火墙深度内容识别的上网行为管控策略，一方面可有效限制企业内部网络机密信息的传播，从而降低公司机密泄露的风险，保证信息安全；另一方面限制员工终端系统可访问的应用，从而提高工作效率。

智慧防火墙支持通过预定义的 URL 类，及用户自定义的 URL 类，对 URL 进行过滤。实现仅允许用户打开某一些网页，或者禁止用户打开某一些网页。比如可以通过策略实现禁止企业员工访问色情、犯罪、邪教等违规网站。


**URL 分类**

智慧防火墙通过深度内容过滤模块，针对邮件协议、文件传输协议、WEB 应用协议、网页邮箱、云盘进行应用层的内容过滤，可以对含有预定义或自定义违规关键字的内容过滤，防止企业员工对外发布违法言论，规避企业的法律风险。

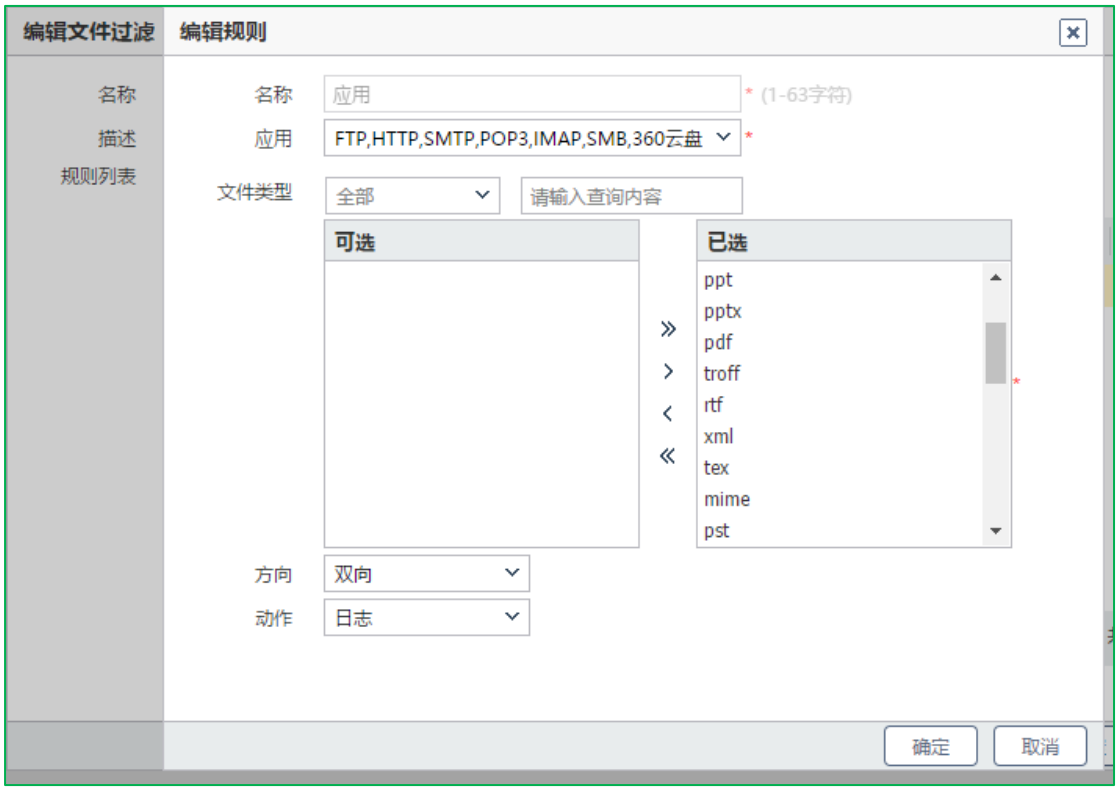



**内容过滤**

智慧防火墙支持精细化应用识别控制，可以做到基于应用的上网行为管控策略，限制网络内部的用户使用某种指定的应用程序或协议，该方法在不限制用户访问互联网的前提下，能够差别化地限制某些影响工作效率或占用大量带宽应用的使用，如 QQ、P2P，并且支持通过 WLAN 上网的手机用户限制使用与工作无关的应用。


**应用分类**

智慧防火墙支持深度文件属性识别技术，对文件类型的识别不依赖后缀名，即使修改文件后缀名也不影响智慧防火墙对该文件过滤识别，对使用 POP3、SMTP、IMAP、FTP、HTTP 协议及网页邮箱、云盘传输文件时，通过识别文件类型，对文件的上传和下载进行过滤可以有效限制企业内部网络机密信息的传播，从而降低公司机密泄露的风险，保证信息安全。




**文件过滤**

智慧防火墙提供精细化的上网行为管控措施，不仅能规避企业员工上非法网站、发布非法言论的问题，还能有效提升员工上班期间工作效率和带宽利用率。

## 3.3 与云协同联动，精准发现内网失陷主机

防火墙的部署位置在企业互联网边界，与云端进行实时协同，检测内网可疑失陷主机，并利用分析中心“智慧调查”相关的关联分析特性及时研判网络风险，进而下发处置策略。

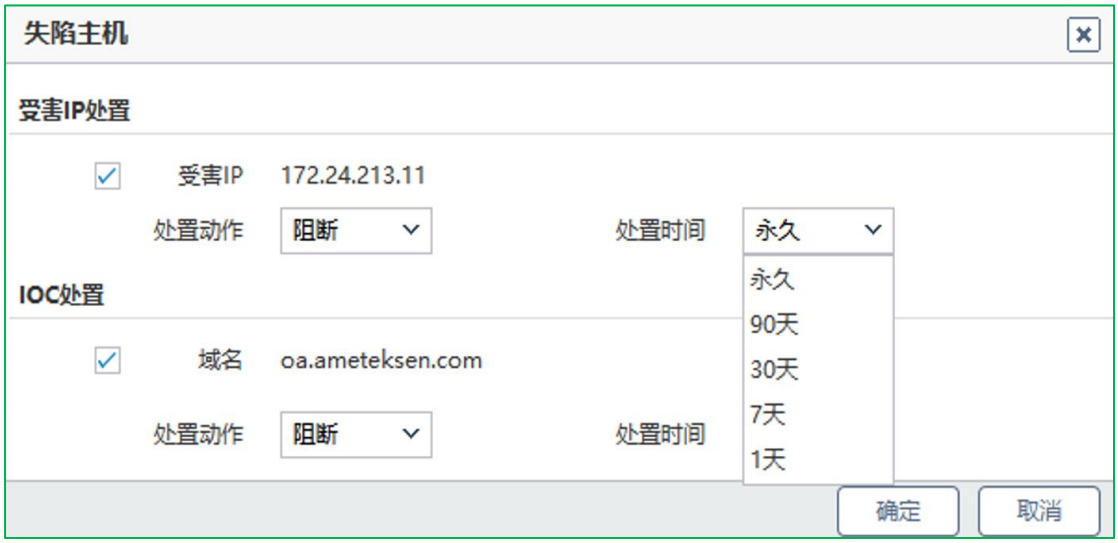
云安全服务将智慧防火墙上报的日志数据汇聚至大数据分析引擎，提取网络内主机的行为数据，一方面可通过大数据技术挖掘偏离正常基线的异常行为，另一方面，由防火墙上报的威胁日志将会和其他多种来源的攻防信息一同汇聚为威胁情报，云安全服务将海量的威胁情报与本地行为数据进行匹配对撞，可“智慧发现”失陷主机或者可能失陷的风险主机。


**“智慧发现”异常主机**

当智慧防火墙提供了可能失陷的风险主机后，可根据受害 IP 或者威胁事件匹配到 IOC 条目进行一键跳转，通过数据中心和分析中心，将流量经过设备各功能模块检测时所产生的的日志信息关联聚合，为呈现了一次攻击发生的全过程。


**“智慧调查”威胁事件**

当经过发现、分析调查工作后，如果确定为失陷主机，智慧防火墙还支持根据自定义时间一键处置失陷主机或者一键处置威胁事件，做到“智慧处置”，使整个处理流程变得简单、高效。




“智慧处置”失陷主机

通过智慧防火墙和云安全服务的协同联动，不但可以预警网内的失陷主机，同时还向用户提供了分析回溯的可见性及一键式的处置策略下发能力，实现对内部风险点和威胁的检测、分析、处置的闭环管理。

# 4 方案的优势亮点

## 4.1 全面、精确的威胁检测能力

基于攻防研究储备和安全大数据能力，智慧防火墙可对几千余种级别的漏洞利用攻击，几百万种级别的恶意文件实现防护。此外，还可与安全私有云、沙箱检测系统等部件展开智能协同，通过病毒云查杀、URL 云过滤、可疑文件深度鉴别等高级功能进一步提升其威胁检出能力，确保互联网边界的安全性。

## 4.2 基于内容、URL、应用行为的精细化管控

智慧防火墙系统提供内容过滤、URL 过滤、网络行为管理功能，从而实现对用户的网络行为进行管控。行为管控策略不仅支持精确到 IP 地址，更可精确到用户。同时，在文件过滤中还实现了对敏感信息泄露的防护，内容过滤中实现了基于关键字的内容发布过滤，提供支持网站应用和手机 APP 管控，使应用控制更加精细化。

## 4.3 云端协同精确定位失陷主机

基于多手段的安全数据采集和深入分析，并得益于情报共享的生态体系，具备全球领先的威胁情报生产能力。基于云端威胁情报技术的失陷主机发现，智慧防火墙可在互联网边界对网络流量进行多维度关联分析、递进式数据钻取，通过人性化 UI 界面直观展现失陷主机的发现、调查、处置一体化流程，及安全事件的溯源取证。

# 5 用户的价值提升

- 通过智慧防火墙精确的威胁检测能力和云端查询能力，为互联网边界提供

安全可靠的全面防护，弥补传统防御的不足，消除“外患”；

- 精细化行为管控为企业客户消除法律风险和机密文件泄露风险，提供高效稳定的网络环境，提升员工工作效率，解除“内忧”；
- 利用前沿理念协同联动和创新的威胁情报技术，构建感知与快速响应能力。