深信服科技

NGAF 下一代防火墙
产品白皮书

深信服科技有限公司

2017 年 6 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改或撤回，恕不另行通知。

深信服科技股份有限公司已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，深信服科技股份有限公司均不对（包括但不限于）最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。

信息反馈

如果您有任何宝贵意见，请反馈：

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋　邮编 518055

电话：0755-86627888

传真：0755-86627999

您也可以访问深信服科技网站 www.sangfor.com.cn 获得更新技术和产品信息

1. 概述

近几年来，随着互联网+、业务数字化转型的深入推进，各行各业都在加速往互联网化、数字化转型。业务越来越多的向公众、合作伙伴，第三方机构等开放，在数字化业务带给我们高效和便捷的同时，信息暴露面的增加，网络边界的模糊化以及黑客攻击的产业化使得网络安全事件相较以往成指数级的增加，面对应对层出不穷的新型安全事件如网站被篡改，被挂黑链，0 day 漏洞利用，数据窃取，僵尸网络，勒索病毒等等，传统安全建设模式已经捉襟见肘，面临着巨大的挑战。

问题一：传统信息安全建设，以事中防御为主。缺乏事前的风险预知，事后的持续检测及响应能力

传统意义上的安全建设无论采用的是多安全产品叠加方案还是采用 UTM/NGFW+WAF 的整合类产品解决方案，关注的重点都在于如何防护资产在被攻击过程中不被黑客入侵成功，但是并不具备对于资产的事前风险预知和事后检测响应的能力，从业务风险的生命周期来看，仅仅具备事中的防护是不完整的，如果能在事前做好预防措施以及在时候提高检测和响应的能力，安全事件发生产生的不良影响会大幅度降低，所以未来，融合安全将是安全建设发展的趋势。

问题二：传统安全建设是拼凑的事中防御，缺乏有效的联动分析和防御机制

传统安全建设方案，搜集到的都是不同产品碎片化的攻击日志信息，只能简单的统计报表展示，并不能结合业务形成有效的资产安全状态分析。另外在防护机制上只能依赖静态的防御策略进行防护，无法及时应对业务发生的变化，不同安全设备之间也无法形成有效的联动封锁机制，不仅投资高，运维方面也难管理。

深信服下一代防火墙安全理念

深信服通过对以上问题的思考进行了下一代防火墙的产品设计，对下一代防火墙赋予了风险预知、深度安全防护、检测响应的能力，最终形成了全程保护、全程可视的融合安全体系。

融合不是单纯的功能叠加，而是依照业务开展过程中会遇到的各类风险，所提供的对应安全技术手段的融合，能够为业务提供全流程的保护，融合安全包括从事前的资产风险发现，策略有效性检测，到事中所应具备的各类安全防御手段以及事后的持续检测和快速响应机

制，并将这一过程中所有的相关信息通过多种方式呈现给给用户。

融合安全，简单有效

2. 深信服下一代防火墙核心价值

2.1. 全程保护

2.1.1. 事前预知：资产/脆弱性/策略有效性

深信服 NGAF 能够在事前对内部的服务器进行自动识别，并且还能自动识别服务器上开放端口和存在的漏洞，弱密码等风险，同时还能判断识别出的资产是否有对应的安全防护策略以及是否生效。

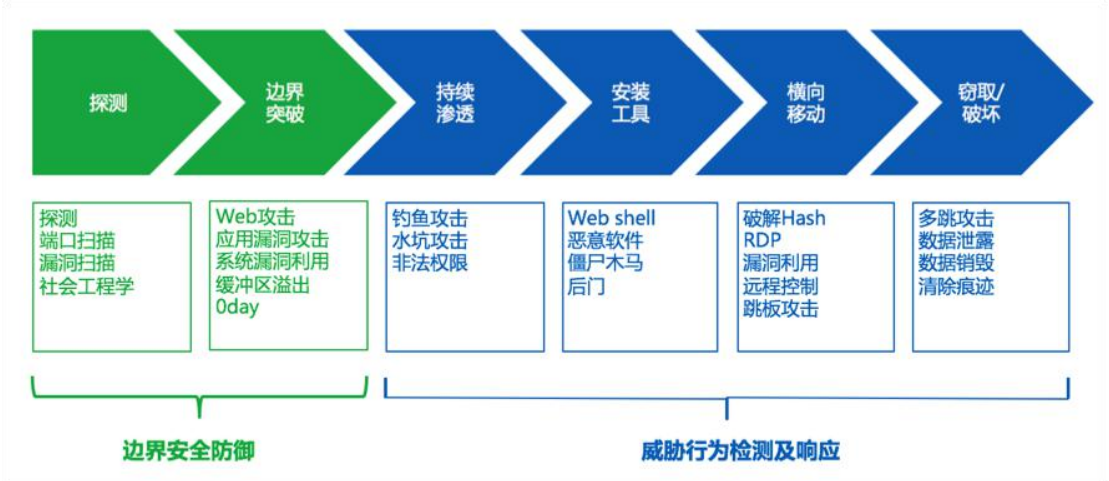
2.1.2. 事中防御：完整的防御体系+安全联动+威胁情报

深信服 NGAF 在事中防御层面融合了多种安全技术，提供了 L2-7 层完整的安全防御体系，确保安全防护不存在短板，同时还能通过安全联动功能加强防御体系的时效性和有效性，包

括模块间的联动封锁，同云端安全联动，策略的智能联动等。此外，深信服 NGAF 还广泛的开展第三方安全机构合作，通过国家漏洞信息库，谷歌 Virustotal 恶意链接库等多来源威胁情报的输入，帮助用户能够在安全事件爆发之前就提前做好防御的准备。

2.1.3. 事后检测&响应：威胁行为的持续检测&快速响应

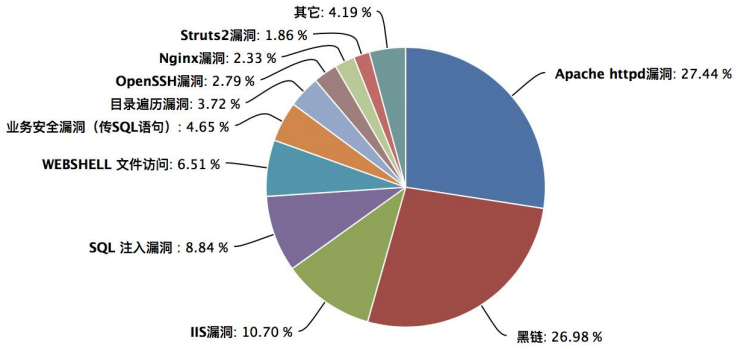
传统安全建设主要集中在边界安全防御，缺乏对绕过安全防御措施后的检测及响应能力，如果能做好事后的检测及响应措施，可以极大程度降低安全事件产生的影响。深信服 NGAF 融合了事后检测及快速响应技术，即使在黑客入侵之后，也能够帮助用户及时发现入侵后的恶意行为，如检测僵尸主机发起的恶意行为，网页篡改，网站黑链植入及网站 Webshell 后门检测等，并快速推送告警事件，协助用户进行响应处置。



2.2. 全程可视

2.2.1. 事前对安全风险的认知

➢ 清晰了解资产脆弱性



➢ 快速发现策略有效性

2.2.2. 事中对保护过程的认知

➢ 攻击事件匹配不同攻击阶段

2.2.3. 事后对保护结果的认知

➢ 基于信息资产维度的安全现状展示

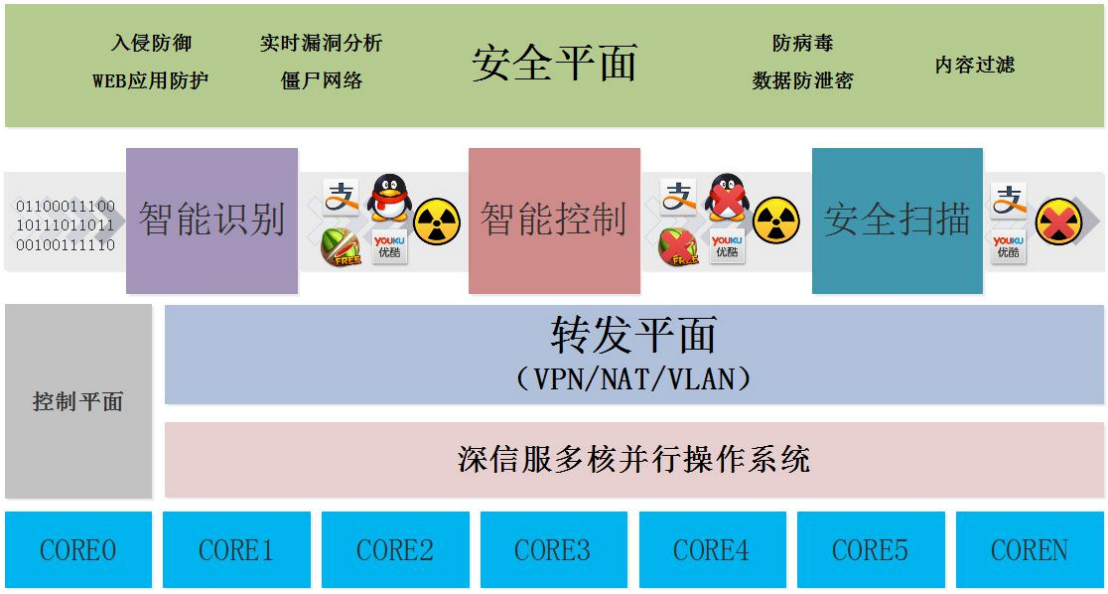
➢ 综合风险报表

风险	测试系统(" ")、财务系统 、研发代码服务器 等共68个服务器已被入侵 等共4个主机已被感染	**建议：** 请参考对应业务、用户风险详情中的安全加固建议进行处理，避免造成严重的业务损失
黑链	新闻发布主站(www.test.com) 已被挂1个黑链 BBS(bbs.test.com)已被挂1个黑链	**建议：** 1. 清除对应页面黑链内容 2. 下载主机安全检测工具，对网站进行全面扫描
攻击	共遭受攻击者攻击12274次	**结论：** 虽然当前网络整体情况较差，但大部分攻击已被防火墙防护
漏洞	共发现漏洞数204个，其中高危漏洞158个 共发现被利用的漏洞12个	**结论：** 当前业务系统整体脆弱性较高，请参考防火墙，运行状态>实时漏洞风险>查看完整报表，找到对应的漏洞解决方案，进行修复

3. 主要功能介绍

3.1. 系统架构设计

深信服下一代防火墙构筑在 64 位多核并发，高速硬件平台之上，采用自主研发的并行操作系统（Sangfor OS），将转发平面、安全平面并行运行在多核平台上。多平面并发处理，紧密协作，极大的提升了网络数据包的安全处理性能。



- **控制平面**

负责整个系统各平面、各模块间的监控和协调工作，此平面包括配置存储、配置下发、控制台 UI、数据中心等功能。

- **转发平面**

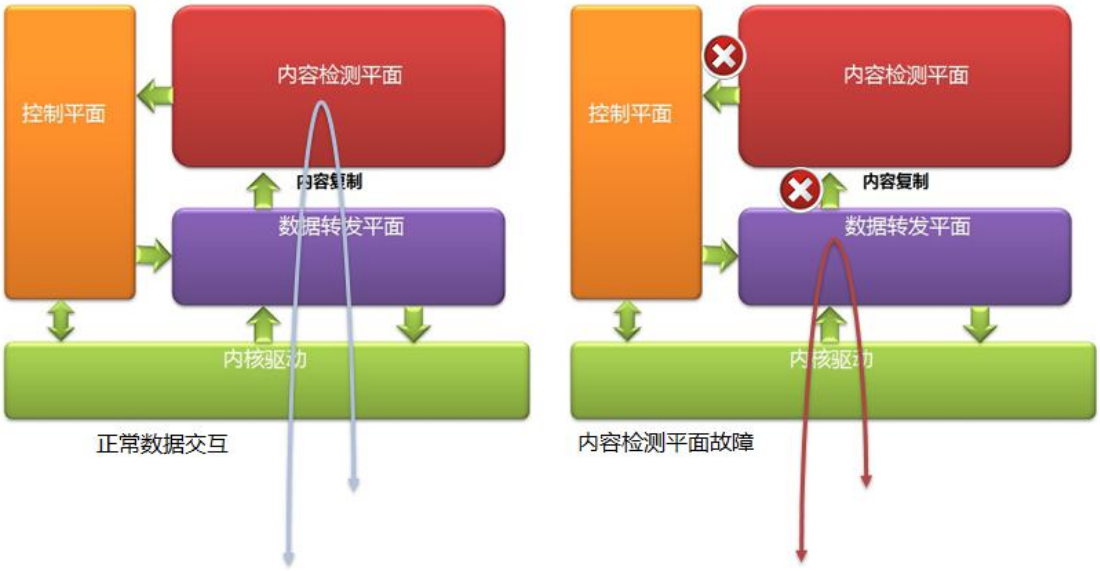
负责网络数据包的高速转发，此平面包括路由子系统、网桥子系统、邻居系统、VPN、NAT、拨号等功能。

- **安全平面**

负责安全功能的协调运行，采用一次解析引擎，一次扫描便可识别出各种威胁和攻击，此平面包括入侵防御、WEB 应用防护、实时漏洞分析、僵尸网络、数据防泄密、内容过滤、防病毒等功能。

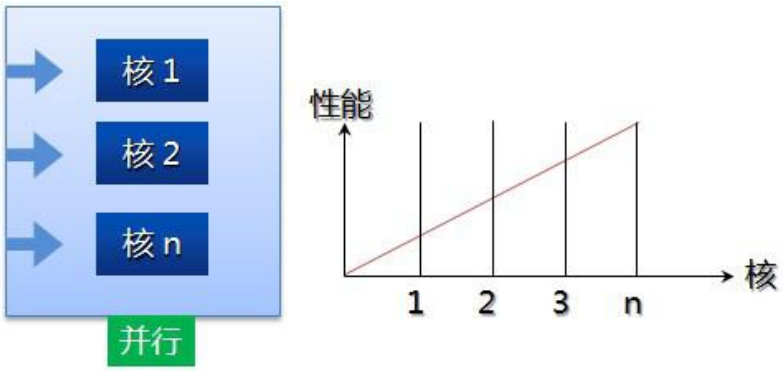
3.1.1. 分离平面设计

深信服下一代防火墙通过软件设计将网络层和应用层的数据处理进行分离，在底层以应用识别模块为基础，对所有网卡接收到的数据进行识别，再通过抓包驱动把需要处理的应用数据报文抓取到应用层。若应用层发生数据处理失败的情况，也不会影响到网络层数据的转发，从而实现高效、可靠的数据报文处理。



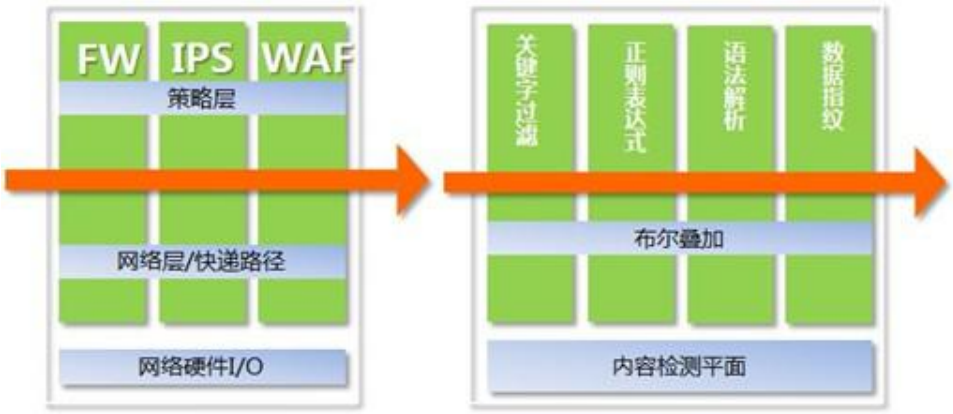
3.1.2. 多核并行处理

深信服下一代防火墙的设计不仅采用了多核的硬件架构，在计算指令设计上还采用了先进的无锁并行处理技术，能够实现多流水线同时处理，成倍提升系统吞吐量，在多核系统下性能表现十分优异，是真正的多核并行处理架构。



3.1.3. 单次解析架构

深信服下一代防火墙采用单次解析架构实现报文的一次解析一次匹配，有效提升了应用层效率。实现单次解析技术的一个关键要素就是软件架构设计实现网络层、应用层的平面分离，将数据通过“0”拷贝技术提取到应用平面上实现威胁特征的统一解析和统一检测，减少冗余的数据包封装，实现高性能的数据处理。



3.1.4. 跳跃式扫描技术

深信服下一代防火墙利用多年积累的应用识别技术，在内核驱动层面通过私有协议将所有经过下一代防火墙的数据包都打上应用的标签。当数据包被提取到内容检测平面进行检测时，设备会找到对应的应用威胁特征，通过使用跳跃式扫描技术跳过无关的应用威胁检测特征，减少无效扫描，提升扫描效率。比如：流量被识别为 HTTP 流量，那么 FTP server 的相关漏洞攻击特征便不会对系统造成威胁，便可以暂时跳过检测进行转发，提升转发的效率。

3.1.5. Sangfor Regex 正则引擎

正则表达式是一种识别特定模式数据的方法，它可以准确识别网络中的攻击。经深信服安全专家研究发现，业界已有的正则表达式匹配方法的速度一般比较慢，制约了下一代防火墙的整机速度的提高。为此，深信服设计并实现了全新的 Sangfor Regex 正则引擎，将正则表达式的匹配速度提高到数十 Gbps，比 PCRE 和 Google 的 RE2 等知名引擎快数十倍，达到业内较高水平。

深信服下一代防火墙的 Sangfor Regex 大幅降低了 CPU 占用率，有效提高了 NGAF 的整机吞吐，从而能够更高速地处理客户的业务数据，该项技术尤其适用于对每秒吞吐量要求特别高的场景，如运营商、电商等。

3.2. 基础防火墙特性

深信服 NGAF 兼容传统防火墙的所有功能特性，包括交换/路由、访问控制，A-A/A-S 双机热备、软硬件 Bypass、系统管理、日志报表、会话管理、抗 DDoS 攻击、应用代理、DHCP/DNS 等等。

3.2.1. PPPoE

通过 ADSL 接入 Internet 已经成为越来越多中小企业的选择，而 ADSL 需要拨号以后才能获得 IP 地址。深信服 NGAF 支持 PPPoE 协议，作为 PPPoE Client 端完成与 PPPoE Server 建立连接和地址获取，通过设置用户名和口令即可支持 ADSL 接入，获得动态 IP 地址、网关及 DNS 地址，自动完成拨号过程，接入 Internet 网络。解决中小企业上网问题。

3.2.2. NAT 地址转换

支持静态网络地址转换（Static NAT）和动态网络地址转换（Dynamic NAT），实现内网地址转换成公网地址后进行网络通信。支持目的 NAT，将对外网地址的访问映射为对内网地址访问，支持将对一个公网地址的访问映射为内网多个地址，实现内网服务器的负载均衡访问，同时支持目的端口转换。

3.2.3. IPv6/IPv4 双协议栈

支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、等条件进行安全访问规则的设置；支持 IPv6 静态路由；支持双栈、6to4 及 6in4 隧道实现 IPv6 网络与 IPv4 网络访问等。深信服 NGAF 产品已获 IPv6-Ready 认证。

3.2.4. VPN

深信服 NGAF 根据企业 VPN 常见使用场景，支持多种 VPN 隧道业务，包括 IPSec、GRE、SSL、L2TP VPN 等。用户可通过 GRE、IPSec 或 SSL VPN 隧道实现分公司与总部之间的数据安全传输，通过 SSL 或 L2TP VPN 隧道实现 PC 以及移动客户端与总部之间的数据安全传输；支持多种隧道模式，即可以让用户通过七层 Web 链接进行内网资源的快速访问，又可以让用户通过三层隧道实现任意内网应用资源的便捷使用。

3.2.5. 链路聚合

链路聚合（Link Aggregation），是指将多个物理接口捆绑在一起，成为一个逻辑接口，以实现出/入流量在各成员接口中的负荷分担。

SANGFOR NGAF 根据用户配置的端口负荷分担策略(主备、负载均衡-hash、负载均衡-RR)决定报文从哪一个成员接口发送到下一跳地址。当交换机检测到其中一个成员接口链路发生故障时，就停止在此接口上发送报文，并根据负荷分担策略在剩下接口链路中重新计算报文发送的接口。故障接口恢复后会再次重新计算报文发送接口。

链路聚合在增加链路带宽（如果一个接口 1G 带宽，另外一个接口也是 1G 带宽，如果把这两个接口聚合成一个逻辑接口，理论上这个逻辑接口的带宽就是 2G。）实现链路传输弹性和冗余等方面是一项很重要的技术。

3.2.6. 路由功能

深信服 NGAF 可以实现静态路由、默认路由、浮动静态路由等基础功能，同时能够实现如 BGP、RIP、OSPF 等动态路由协议，并更好地支持策略路由、多播路由等功能。

3.3. 事前风险预知

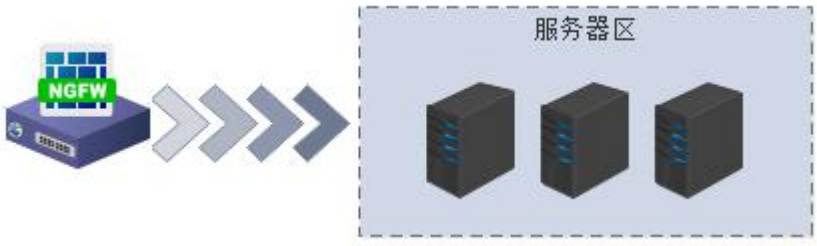
3.3.1. 资产自动发现

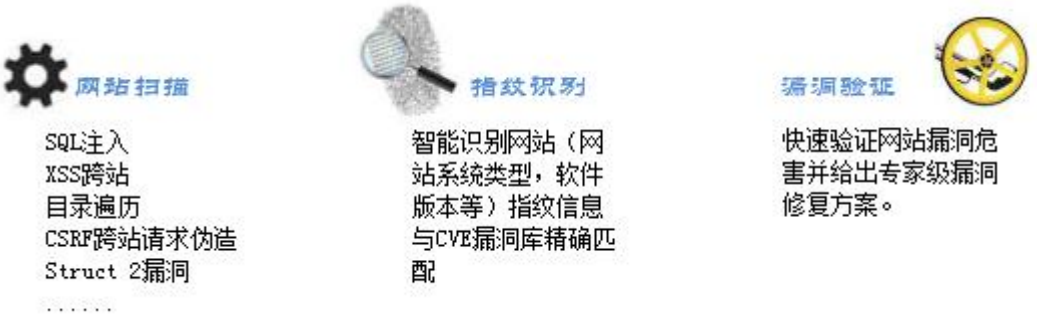
深信服 NGAF 为帮助保护用户快速管理资产，避免安全防护策略的遗漏实现了基于流量检测的资产自动发现功能，可以通过流经流量的 IP 地址检测及端口检测快速发现自身资产，帮助用户进行策略的有效配置。

对于网络中的流量，我们可以通过是否与知名 DNS 服务器连接、是否访问知名网站、是否有被搜索引擎进行检测等算法来判定哪些是内网主机。在通过端口的链接情况，记录开放的端口情况，帮助用户了解自身网路情况。

3.3.2. Web 扫描

深信服 NGAF 的 WEB 扫描器是深信服结合多年来在 web 应用安全上的研究成果，基于大量信息安全事件应急响应的丰富经验下开发出的一款安全扫描器，该扫描器旨在帮助广大用户对 web 服务器网站进行深度的安全扫描，指纹识别，漏洞验证，全面预知 web 应用系统的安全现状，并提供专业的安全加固建议。





3.3.2.1. 丰富的扫描插件

支持 SQL 注入，XSS 跨站脚本攻击，目录遍历，CSRF 跨站请求伪造，远程文件包含，命令注入，敏感信息泄露，Struct 2 漏洞等众多扫描插件，覆盖所有 OWASP TOP10 高危漏洞，保证全面深入的 WEB 网站扫描效果。

3.3.2.2. 智能网站指纹识别

支持对 web 网站服务器操作系统类型：Apache，IIS，Tomcat，Nginx，Weblogic 等服务器/中间件类型；php/jsp/asp/c#/.net/python 等网站语言类型进行自动识别，并和 CVE/CNNVD 漏洞库智能关联分析。

3.3.2.3. 专家级漏洞分析和修复建议

为帮助广大 web 管理人员轻易读懂和掌握专业性较强的安全报告内容，告别晦涩难懂的漏洞扫描报告，深信服 WEB 扫描器检测报告对漏洞进行了非常详细和介绍和漏洞危害说明，并将安全检查过程中发送的 payload 测试报文进行高亮显示，web 管理人员通过高亮显示部分的信息，即能轻易初步掌握漏洞原因。

3.3.3. 风险分析

提供主动扫描功能，通过检查防火墙配置，帮助管理员分析服务器开放的端口和存在的风险，并对扫描结果提供对应防护操作，如漏洞防护，端口屏蔽等来方便用户进行安全防护。

端口扫描

对用户指定的服务器 IP，端口进行扫描，告知用户该服务器开放了那些端口和服务

漏洞分析

针对端口扫描结果对开放的端口和服务进行风险分析，告知用户服务器存在的漏洞，并

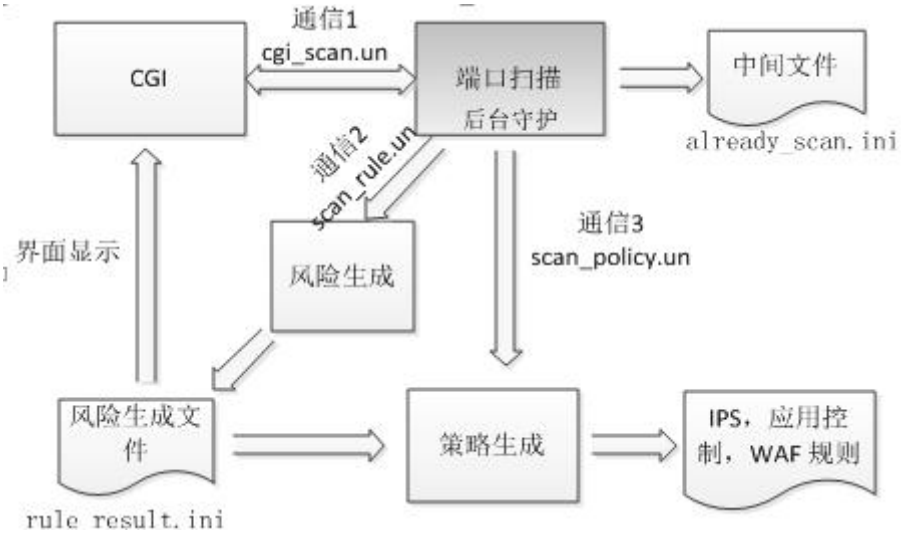
根据防火墙配置告知用户现存风险的防护状态。

弱密码探测

提供内置和自定义弱密码库，对用户指定的服务器进行弱密码探测，分析服务器是否存在弱密码风险。

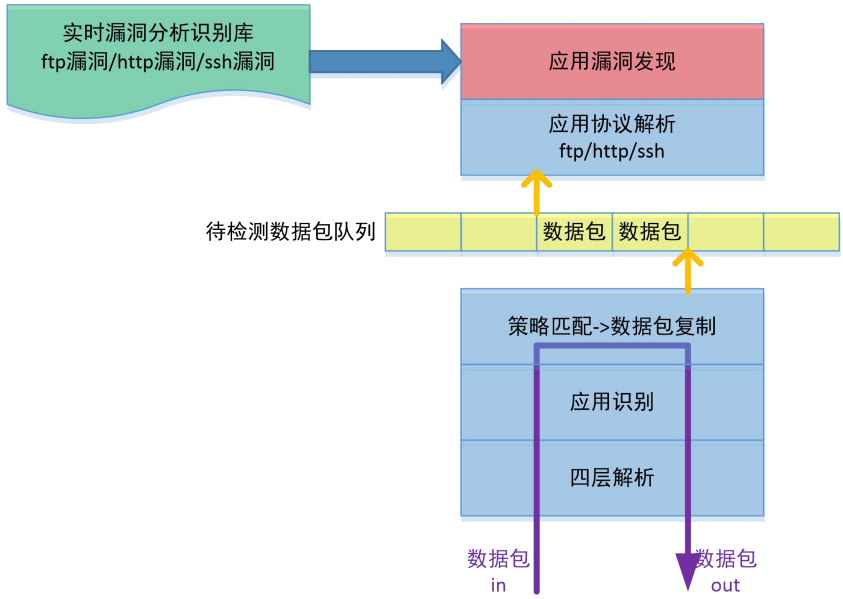
策略防护

提供防护操作按钮，通过新增防火墙配置，对服务器存在的风险进行防护。



3.3.4. 实时漏洞分析

深信服 NGAF 实时漏洞分析系统实时旁路地检测经过设备的应用流量，对流量进行对应的应用解析，对解析后的应用数据匹配实时漏洞分析识别库，发现服务器存在漏洞。



3.3.4.1. 旁路检测

实时漏洞分析采用的是旁路检测技术，即将待检测的数据包镜像一份到待检测队列，检测进程对检测的数据包进行扫描检测，对原有数据包的转发不会造成任何性能影响。

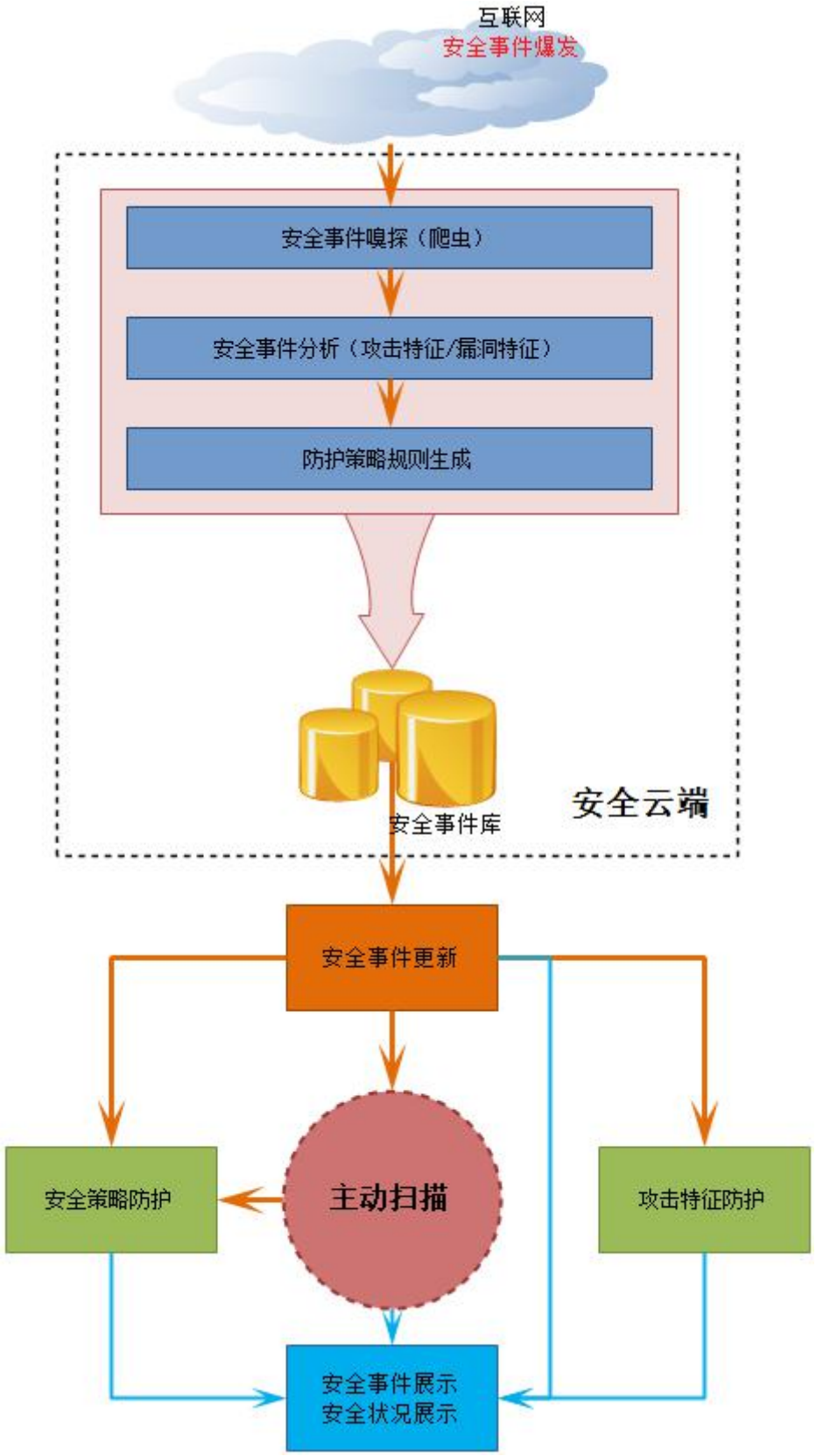
3.3.4.2. 强大的漏洞特征库

实时漏洞分析所使用的漏洞特征库由深信服北京研究中心安全专家针对目前流行的软件、系统等漏洞提取特征，形成库并快速的更新到 NGAF 设备，保证识别出网络中出现的较新漏洞。

3.3.5. 威胁情报预警与处置

在云端通过安全事件响应分析模块自动对安全事件进行及时的响应和分析，产出安全事件的危害描述、漏洞特征、攻击特征和防护策略，网关设备通过更新机制把安全事件更新包更新到本地，并通过控制台弹窗的方式告知用户当前的安全事件和危害，本地扫描器针对漏洞特征对当前防护的业务系统进行全面扫描分析定位是否存在此安全事件漏洞。如果本地存在安全漏洞，则通过安全引擎对此漏洞的安全攻击特征进行防护，并且通过自动化生成安全防护策略的方式帮助用户达到全面有效防护此安全事件的目的。在对此安全事件完成安全防护后，本地扫描器还会再次扫描评估是否全面有效的防护了此安全事件。

原理流程如下：



3.3.6. 策略有效性识别

深信服 NGAF 通过三个维度实现了策略有效性检测：

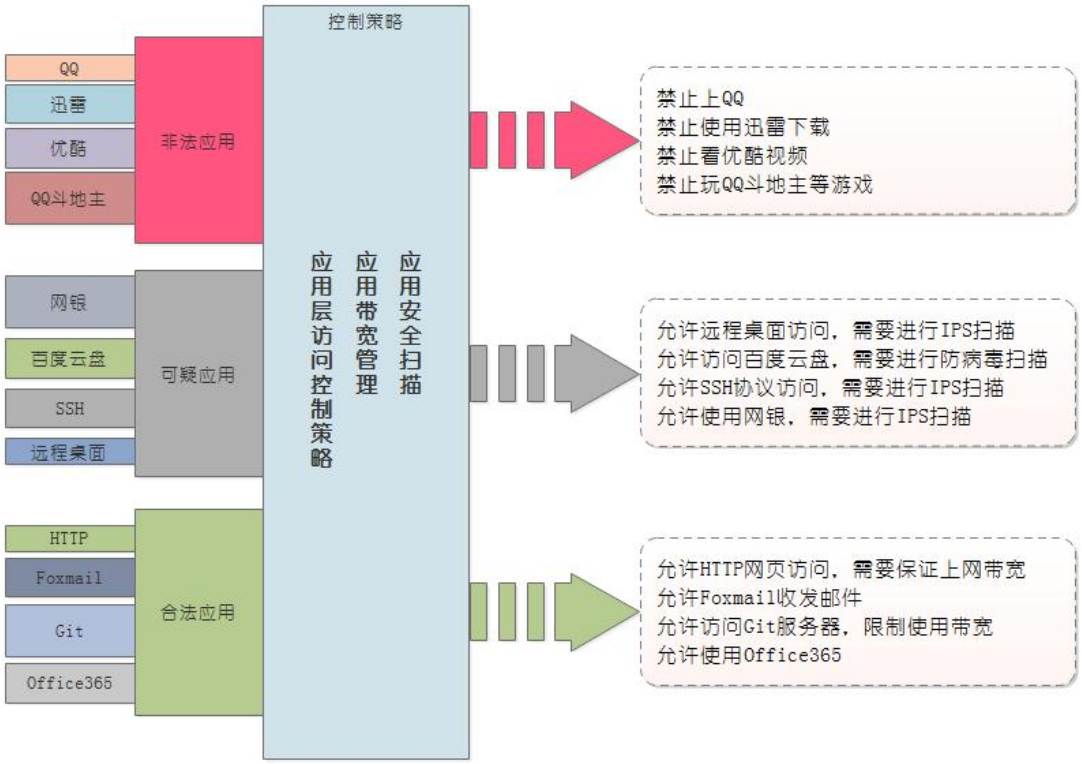
- 通过监测流量进行发现，判定是否对设备与业务系统之间进行了策略配置实现检测、防御、响应；
- 通过策略的对比检查，发现是否存在无效策略、策略冲突、策略配置不当等问题；
- 通过规则库的版本检测，高危 0day 预警是否开启等方式判定设备是否具备新威胁的防御能力。

3.4. 事中安全防护

3.4.1. 智能控制

深信服 NGAF 除了能实现等同于传统防火墙的访问控制功能之外还能实现基于应用及地域的访问控制，帮助用户更好的进行精准控制。

3.4.1.1. 应用控制



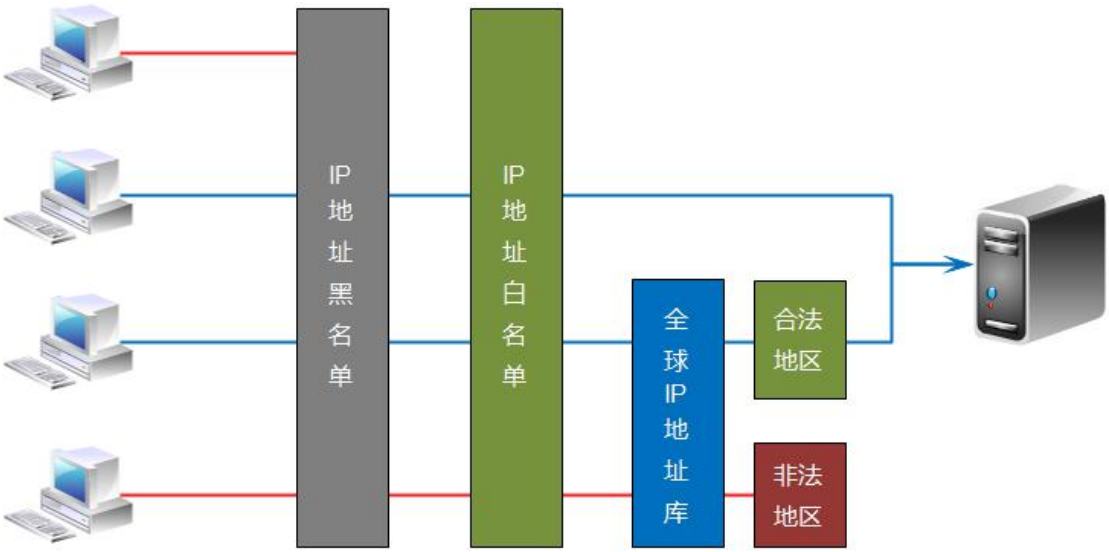
传统防火墙的访问控制或者流量管理粒度粗放，只能基于 IP/端口号对数据流量进行一刀切式的禁止或允许。深信服下一代防火墙基于更好的应用和用户识别能力，对数据流量和访问来源进行精细化辨识和分类，使得用户可以轻易从同一个端口协议的数据流量中辨识出任意多种不同的应用，或从无意无序的 IP 地址中辨识出有意义的用户身份信息，从而针对

识别出的应用和用户施加细粒度、有区别的访问控制策略、流量管理策略和安全扫描策略，保障了用户更直接、准确、精细的管理愿望和控制诉求。

例如：允许 HTTP 网页访问顺利进行，并且保证高访问带宽，但是不允许同样基于 HTTP 协议的视频流量通过；允许通过 QQ 进行即时通讯，但是不允许通过 QQ 传输文件；允许邮件传输，但需要进行防病毒或明个信息过滤，如发现有病毒入侵或泄密事件马上阻断；等等。

3.4.1.2. 地域访问控制

地域访问控制主要是通过对访问者的 IP 地址进行归属地判断，判断所属国家或地区是否能够对业务进行访问。SANGFOR NGAF 内置了一个全球的 IP 地址库，并定期更新。地址库由三部分组成：黑名单、白名单和全球地址库，用户可以在 WEBUI 上对此地址库配置黑白名单和 IP 归属地纠错。具体访问控制流程如下：



一、访问者的 IP 首先会根据 IP 黑名单进行匹配，如果此 IP 是黑名单的 IP 则直接拒绝访问；

二、根据 IP 白名单进行匹配，如果此 IP 是白名单的 IP 则直接允许访问；

三、如果不在黑白名单中，则通过 IP 地址库进行匹配，得出此 IP 的归属地（那个国家或地区），然后根据用户配置的此国家或是地区的访问策略进行拒绝或允许访问。

3.4.2. 基于漏洞的安全防护

深信服 NGAF 的威胁分析引擎具备 4000+条漏洞特征库、3000+Web 应用威胁特征库，可以全面识别各种应用层和内容级别的单一安全威胁；另外，深信服凭借在应用层领域 10 年

以上的技术积累，组建了专业的安全攻防团队，可以为用户定期提供较新的威胁特征库更新，以确保防御的及时性。

3.4.2.1. 安全团队定期更新

深信服安全团队对于网络中不断发现的攻击形式进行解析，通过后端的专家团队对攻击的不断解析发现其中的攻击特征，并将攻击特征整理归纳填充到现有的特征库中为用户定期进行更新，当遇到重大安全威胁时深信服的安全团队会同时发布威胁预警并进行实时更新，帮助用户抵御较新的安全威胁。

3.4.2.2. 在线设备全网联动

深信服 NGAF 为满足对新威胁防御的需求，让用户以最快的速度具备防御新威胁的能力，实现了安全云与在线设备的联动。通过云端收集上万台在线设备的未知威胁进行分析，并将分析结果发送给所有的深信服 NGAF，使得用户具备防御最新威胁的能力。

3.4.2.3. 多家机构共享特征

以目前网络攻击的更新速度来看，单一厂商很难实现对最新威胁的实时更新。为了更好的服务客户，深信服通过与 CNCERT、Google virus total 等十余家权威机构的合作来实现共享威胁情报，帮助用户接收到多方位的信息，实现对新威胁的有效防御。

3.4.2.4. 在线沙盒未知检测

在对已知威胁具备了防御能力之后，为了弥补固定特征库防御方面会有遗漏的问题，深信服提供了云端在线的沙盒检测功能。通过沙盒环境下未知流量的运行来监测系统环境的变化，提取相关参数变化形成分析结果，确定威胁类型并将结果下发的设备端。

同时深信服内部每周也会通过云端在线沙盒收集流量来进行分析，用以填充设备特征库。

3.4.2.5. 精准分类的防护策略

考虑到针对主机和终端的不同操作系统或者软件攻击时所要利用漏洞的不同，深信服 NGAF 对此问题将防护策略分为了针对客户端和服务器端两种类型，使得使用可以根据自己的使用场景进行快速选择，让防护更局针对性。

3.4.3. web 层防护

深信服 NGAF 能够有效防护 OWASP 组织提出的 10 大 web 安全威胁的主要攻击，并于 2013 年 1 月获得了 OWASP 组织颁发的产品安全功能测试 4 星评级证书（最高评级为 5 星，深信服 NGAF 为国内同类产品评分最高）主要功能如：

3.4.3.1. 防 SQL 注入攻击

SQL 注入攻击产生的原因是由于在开发 web 应用时，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。NGAF 可以通过高效的 URL 过滤技术，过滤 SQL 注入的关键信息，从而有效的避免网站服务器受到 SQL 注入攻击。

3.4.3.2. 防 XSS 跨站脚本攻击

跨站攻击产生的原理是攻击者通过向 Web 页面里插入恶意 html 代码，从而达到特殊目的。NGAF 通过先进的数据包正则表达式匹配原理，可以准确地过滤数据包中含有的跨站攻击的恶意代码，从而保护用户的 WEB 服务器安全。

3.4.3.3. 防 CSRF 攻击

CSRF 即跨站请求伪造，从成因上与 XSS 漏洞完全相同，不同之处在于利用的层次上，CSRF 是对 XSS 漏洞更高级的利用，利用的核心在于通过 XSS 漏洞在用户浏览器上执行功能相对复杂的 JavaScript 脚本代码劫持用户浏览器访问存在 XSS 漏洞网站的会话，攻击者可以与运行于用户浏览器中的脚本代码交互，使攻击者以受攻击浏览器用户的权限执行恶意操作。NGAF 通过先进的数据包正则表达式匹配原理，可以确地过滤数据包中含有的 CSRF 的攻击代码，防止 WEB 系统遭受跨站请求伪造攻击。

3.4.3.4. 主动防御技术

主动防御可以针对受保护主机接受的 URL 请求中带的参数变量类型，以及变量长度按照设定的阈值进行自动学习，学习完成后可以抵御各种变形攻击。另外还可以通过自定义参数规则来更准确的匹配合法 URL 参数，提高攻击识别能力。

3.4.3.5. 应用信息隐藏

NGAF 对主要的服务器（WEB 服务器、FTP 服务器、邮件服务器等）反馈信息进行了有效的隐藏。防止黑客利用服务器返回信息进行有针对性的攻击。如：

HTTP 出错页面隐藏：用于屏蔽 Web 服务器出错的页面，防止 web 服务器版本信息泄露、数据库版本信息泄露、网站绝对路径暴露，应使用自定义页面返回。

HTTP(S)响应报文头隐藏：用于屏蔽 HTTP(S)响应报文头中特定的字段信息。

FTP 信息隐藏：用于隐藏通过正常 FTP 命令反馈出的 FTP 服务器信息，防止黑客利用 FTP 软件版本信息采取有针对性的漏洞攻击。

3.4.3.6. URL 防护

Web 应用系统中通常会包含有系统管理员管理界面以便于管理员远程维护 web 应用系统，但是这种便利很可能会被黑客利用从而入侵应用系统。通过 NGAF 提供的受限 URL 防护功能，帮助用户选择特定 URL 的开放对象，防止由于过多的信息暴露于公网产生的威胁。

3.4.3.7. 弱口令防护

弱口令被视为众多认证类 web 应用程序的普遍风险问题，NGAF 通过对弱口令的检查，制定弱口令检查规则控制弱口令广泛存在于 web 应用程序中。同时通过时间锁定的设置防止黑客对 web 系统口令的暴力破解。

3.4.3.8. HTTP 异常检测

通过对 HTTP 协议内容的单次解析，分析其内容字段中的异常，用户可以根据自身的 Web 业务系统来量身定造允许的 HTTP 头部请求方法，有效过滤其他非法请求信息。

3.4.3.9. 文件上传过滤

由于 web 应用系统在开发时并没有完善的安全控制，对上传至 web 服务器的信息进行检查，从而导致 web 服务器被植入病毒、木马成为黑客利用的工具。NGAF 通过严格控制上传文件类型，检查文件头的特征码防止有安全隐患的文件上传至服务器。同时还能够结合病毒防护、插件过滤等功能检查上传文件的安全性，以达到保护 web 服务器安全的目的。

3.4.3.10. 用户登录权限防护

针对某些特定的敏感页面或者应用系统，如管理员登陆页面等，为了防止黑客访问并不断的进行登录密码尝试，NGAF 可以提供访问 URL 登录进行短信认证的方式，提高访问的安全性。

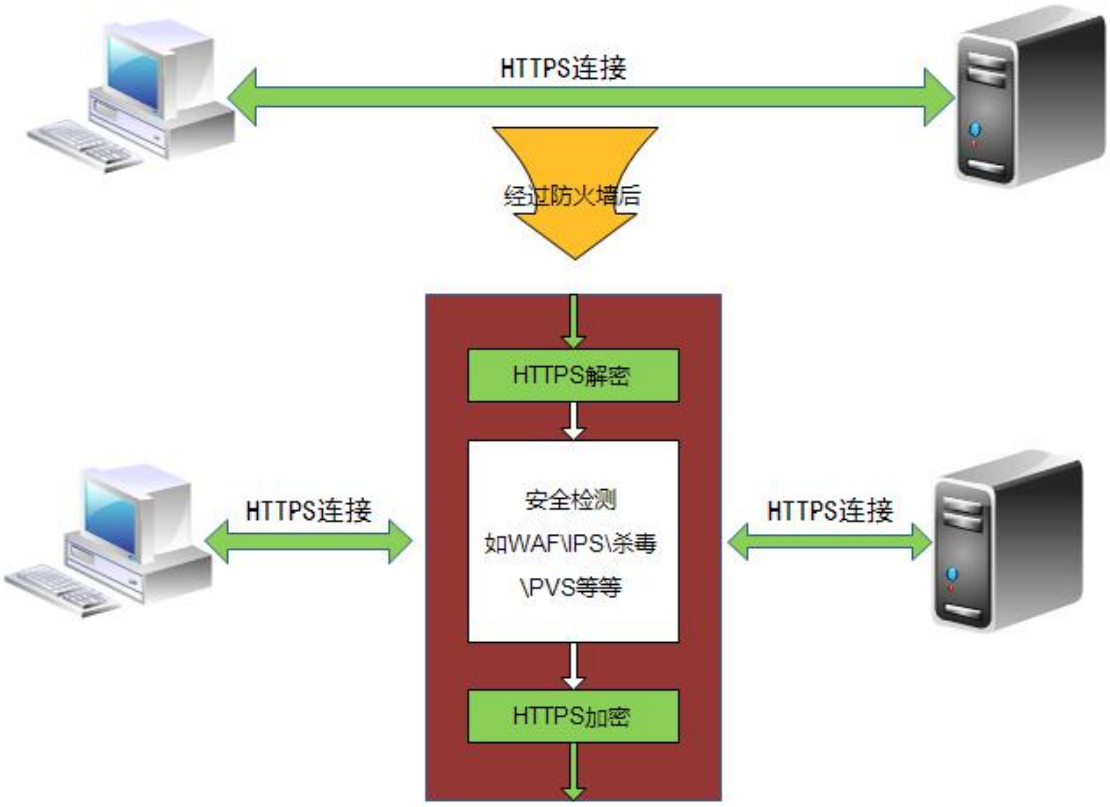
3.4.3.11. 缓冲区溢出检测

缓冲区溢出攻击是利用缓冲区溢出漏洞所进行的攻击行动。可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。NGAF 通过对 URL 长度，POST 实体长度和 HTTP 头部内容长度检测来防御此类型的攻击。

3.4.3.12. HTTPS 解密

由于 HTTPS 的数据是经过 SSL 加密处理的，如果不进行 HTTPS 解密，SANGFOR NGAF 无法分析加密数据包里面的内容，从而也无法达到各种攻击检测和防护的作用，而只能进行数据转发。

HTTPS 解密主要是在 SANGFOR NGAF 内部实现了 HTTPS 的代理功能。当 NGAF 识别到用户在与 HTTPS 服务器建立连接时，根据用户配置的策略，把这条连接的所有数据包抓到应用层，并用用户配置的 SSL 证书进行 SSL 解密，然后把解密后的数据包进行各种安全检测处理，如数据包无异常，则再使用用户配置的 SSL 证书进行加密发送出去。



3.4.4. 未知威胁检测

深信服 NGAF 在发现未知流量时，将会主动（配置允许的条件下）将未知流量上传到云端沙盒进行未知威胁的检测工作。深信服云端沙盒可以通过监测沙盒环境下的文件执行情况、异常网络行为、注册表改动等行为来进行未知威胁的判定工作，再通过特征库更新的方式下发到所有在线的 NGAF 上。

深信服目前已经有上网台 NGAF 与云端联动，每天运行大量的未知流量发现新威胁特征，用以充实特征库，帮助用户抵御较新的攻击行为。

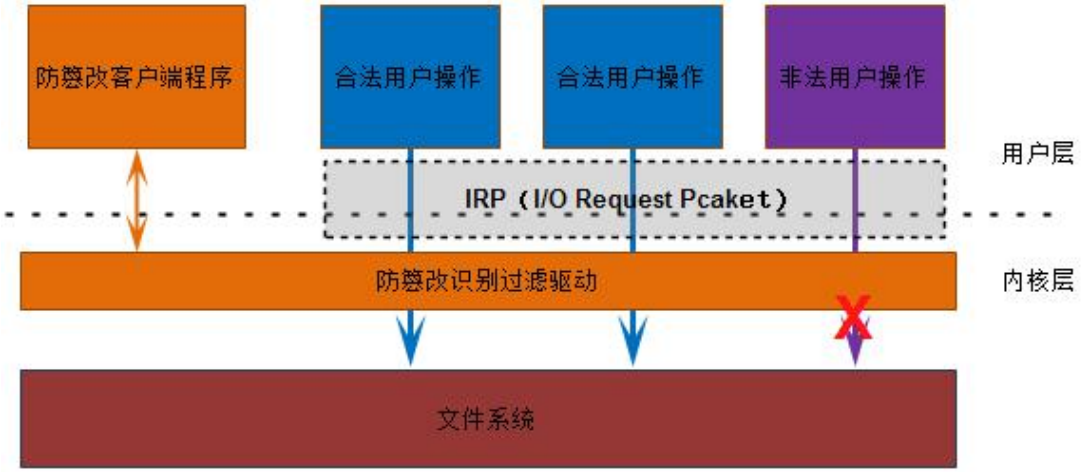
3.4.5. 防篡改

深信服 NGAF 防篡改系统由两部分组成：深信服 NGAF 和深信服防篡改客户端。客户端和下一代防火墙紧密结合，功能联动，保证网站内容不被篡改。

3.4.5.1. 先进的 IRP 流拦截技术

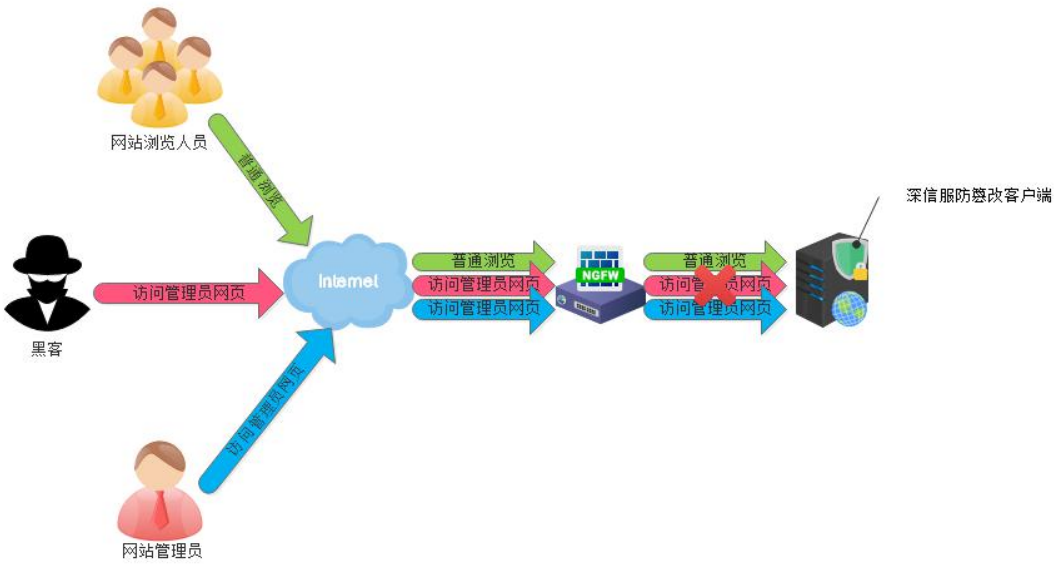
深信服防篡改客户端采用系统底层文件过滤技术，在文件系统上加载防篡改客户端驱动程序，拦截分析 IRP（I/O Request Pcaket）流，识别用户对文件系统的所有操作，并根据防篡改策略对非法的操作进行拦截，以确保受保护的网站目录文件不被篡改。

1. 客户端软件采用目前最流行的 IRF 文件驱动流，通过在客户端软件配置需要保护的文件目录和允许修改该目录的应用程序，识别修改被保护网站目录的应用程序是否合法；
2. 文件驱动检测并识别到非法应用程序修改目录时，拒绝该应用程序的修改动作，并记录行为日志，上报到 NGAF；
3. 客户端软件只有连接了 NGAF 才能激活使用，不能独立使用；使用客户端软件连接 NGAF 时，NGAF 上面须配置一条策略使被保护服务器 IP 与客户端软件能够进行匹配；

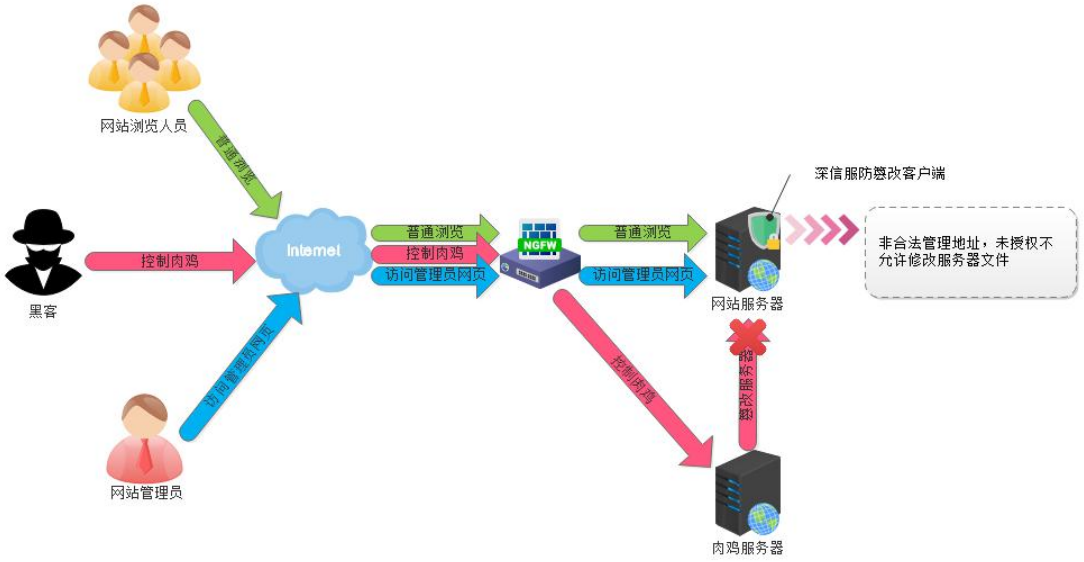


3.4.5.2. 网站管理强认证

深信服 NGAF 对网站管理进行二次认证，防止网站管理员因密码泄露而被篡改，并且对用户网站服务器进行 web 防护，防止网站因 webshell、sql 注入等攻击被篡改。



管理员后台管理账号密码泄露，黑客即使知道了管理员账号密码，因为无法通过 NGAF 的二次验证，因而无法篡改网站服务器的目的。



黑客入侵到内网，控制了一台肉鸡，想通过肉鸡篡改网站服务器，深信服防篡改客户端发现管理员的源 IP 地址不合法，并且没有通过授权，因而也无法达到篡改网站服务器的目的。

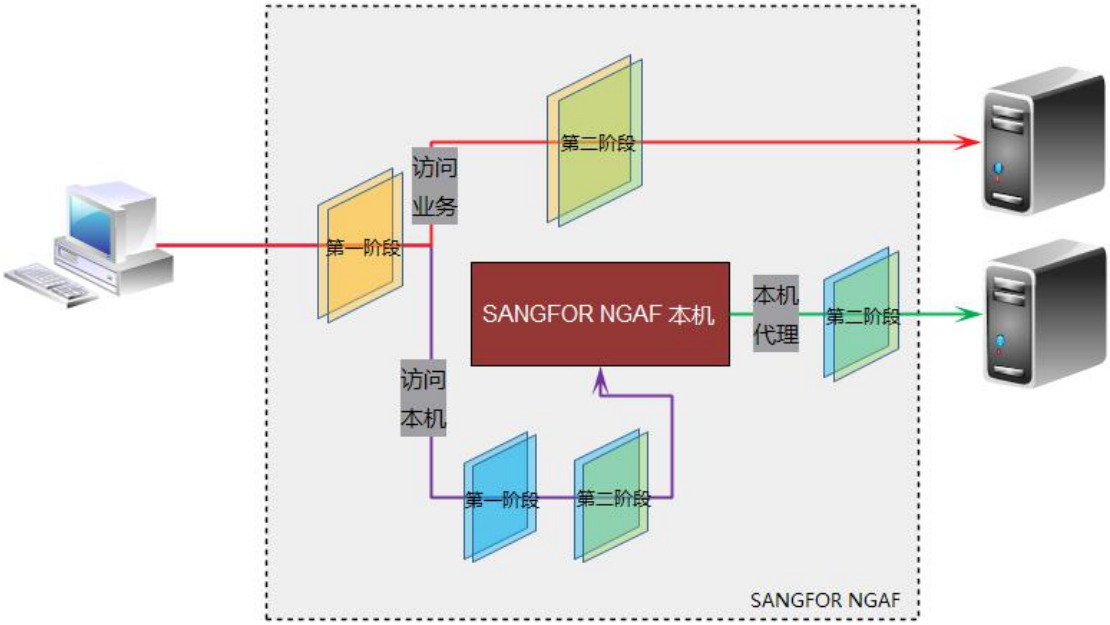
3.4.5.3. 支持多种网站维护方式

深信服 NGAF 防篡改系统支持 FTP，CMS 等多种网站后台管理方式，在对客户网站服务器起到保护作用的同时，不会给管理员带来额外的管理负担，做到的真正的简单实用。

3.4.6. DDOS 防护

深信服 NGAF 采用自主研发的 DOS 攻击算法，可防护基于数据包的 DOS 攻击、IP 协议报文的 DOS 攻击、TCP 协议报文的 DOS 攻击、基于 HTTP 协议的 DOS 攻击等，实现对网络层、应用层的各类资源耗尽的拒绝服务攻击的防护，实现 L2-L7 层的异常流量清洗。

SANGFOR NGAF 通过两个检测阶段进行 DDoS 的检测和防护：

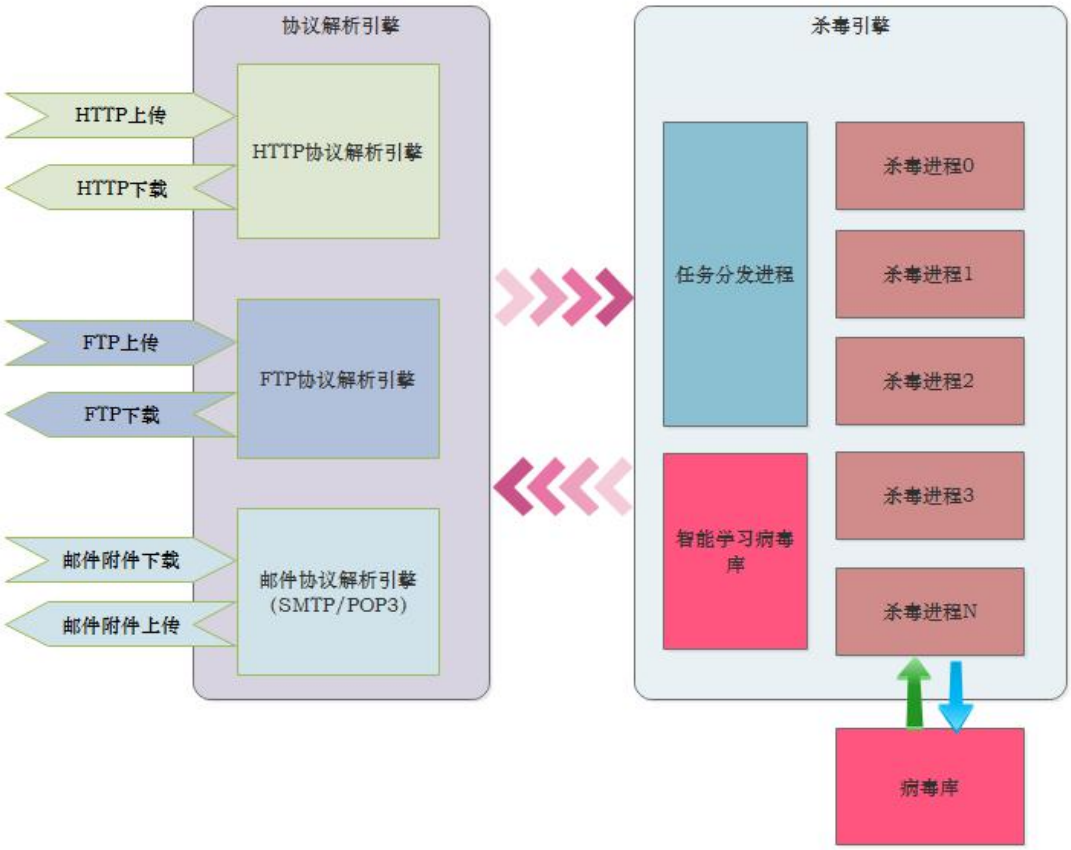


对于业务数据第一阶段进行 TCP 异常包、IP 选项攻击、未知 IP 协议攻击、IP 分片攻击、LAND 攻击、WINNUKE 攻击、SMURF 攻击、TCP 选项攻击、各种 FLOOD 攻击（包括 SYN FLOOD, ICMP FLOOD, UDP FLOOD, DNS QUERY FLOOD）等 DDoS 检测。当第一阶段中检测到 SYN 包频率过高时，将在第二阶段对 TCP 连接做 SYN COOKIE 代理，第二阶段还进行 ICMP 大包攻击(即 ping of death)等检测。

对于本机（访问 SANGFOR NGAF 自身）数据，DDoS 检测模块会在第一阶段做端口扫描的检测（SYN 扫描和 CONNECT 扫描），包括所有的 nmap 扫描：FIN 扫描，NULL 扫描，xmas tree 扫描，UDP 扫描，ACK 扫描，MAIMON 扫描，WINDOWS 扫描，TCP Idle 扫描。而第二阶段根据第一阶段的检测结果决定是否做本机的 syn 代理。

3.4.7. 病毒防护

深信服 NGAF 采用流模式和启发式文件扫描技术，可对 HTTP、SMTP、POP3、FTP 等多种协议类型的近百万种病毒进行查杀，包括木马、蠕虫、宏病毒、脚本病毒等，同时可对多线程并发、深层次压缩文件等进行有效控制和查杀。



3.4.7.1. 多协议并行解析

为了充分利用深信服 NGAF 的多核硬件的架构优势，NGAF 中的协议解析引擎采用了并行解析架构，可以对包括 HTTP、SMTP、POP3、FTP 等不同的协议并发进行解析，极大的提高解析效率。

3.4.7.2. 内存共享杀毒

协议解析引擎和杀毒引擎之间直接通过共享内存传递病毒样本和杀毒结果，进程之间数据交互零拷贝，不会因为不同引擎间的数据拷贝导致杀毒效率降低。

3.4.7.3. 多进程并行查杀

杀毒引擎采用深信服 NGAF 自研发的多进程任务分发架构，利用多核硬件架构，可以极大的提高杀毒引擎同时查杀的病毒样本数目。

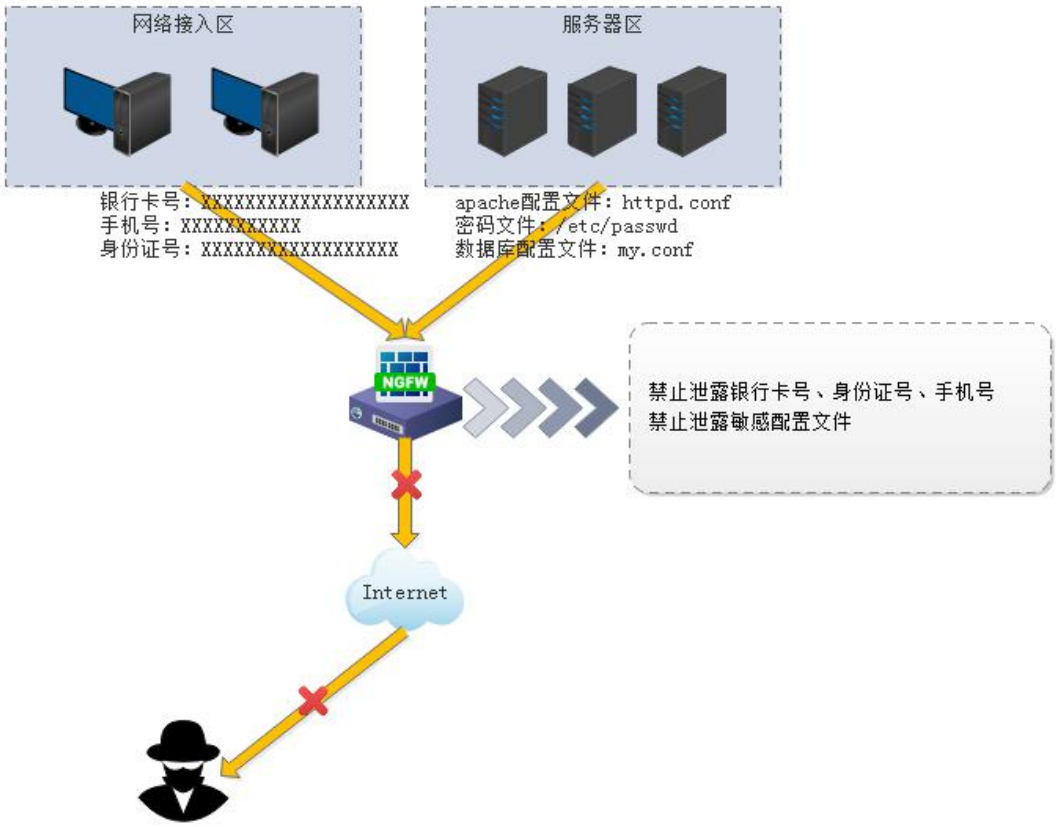
3.4.7.4. 智能学习病毒

杀毒引擎对于已经查杀过病毒样本，将智能的提取样本特征写入缓存，当协议解析引擎

再次发起相同的病毒样本查杀任务时，可以快速的返回查杀结果，从而极大的提高病毒查杀效率。

3.4.8. 数据防泄密

深信服 NGAF 提供可定义的敏感信息防泄漏功能，根据储存的数据内容可根据其特征清晰定义，通过短信、邮件报警及连接请求阻断的方式防止大量的敏感信息被窃取。深信服敏感信息防泄漏解决方案可以自定义多种敏感信息内容进行有效识别、报警并阻断，防止大量敏感信息被非法泄露。（如：用户信息/邮箱账户信息/MD5 加密密码/银行卡号/身份证号码/社保账号/信用卡号/手机号码……）



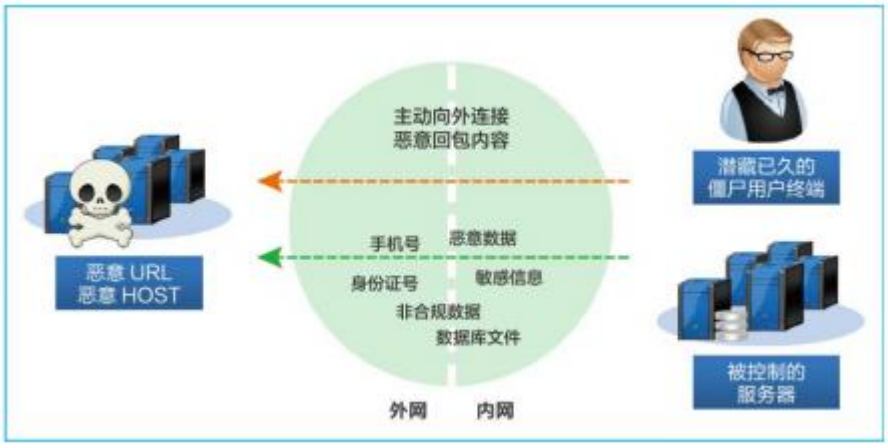
深信服 NGAF 数据防泄密特征库由深信服北京研究中心的安全专家实时跟踪业界的安全动态，收集软件的敏感信息特征，提取成特征库并实时更新到 NGAF。保证 NGAF 能够及时的阻断黑客对敏感信息的访问，保护客户的隐私信息。

3.5. 事后检测及响应

3.5.1. 持续检测

3.5.1.1. 失陷主机

深信服 NGAF 独有的失陷主机检测功能，能够实时对外发流量进行检测，协助用户定位内网被黑客控制的服务器或终端。该功能融合了僵尸网络识别库，全球在线的僵尸网络荣誉库，业界领先的失陷主机行为识别技术对黑客的攻击行为进行有效识别，针对以反弹式木马为代表的恶意软件进行深度防护。



同时结合多种失陷主机的行为特征为主机失陷的概率进行评分，帮助用户对问题进行精确定位，减少误判带来的运维浪费。


受感染主机等级规则说明（该规则是通过对主机下所有僵尸网络相关风险日志进行综合关联分析得出的）

主机严重性	等级	定义
已被感染 主机展现出了感染恶意软件的明确行为	10	具有与已知恶意软件关联的URL、域名、IP地址等进行通信，同时存在数据泄漏或已危害数据库的主机
	9	具有与已知恶意软件关联的URL、域名、IP地址等进行通信，并且主机正在尝试向其他主机传播恶意文件
	8	具有与已知恶意软件关联的URL、域名、IP地址等进行通信或者使用可能被恶意软件用作通讯协议的已知协议(HFS协议)的主机
感染可能性：高 主机展现出了感染恶意软件的高可能性行为	7	具有对外发起DDOS攻击行为的主机，或者具有访问疑似飞客蠕虫类域名行为的主机
	6	被检测出存在已知恶意软件关联的通信数据包特征的主机，或者被检测出存在传播恶意shellcode行为的主机
	5	具有访问疑似DGA自动生成域名行为的主机，或者具有疑似进行反弹连接行为的主机
感染可能性：中 主机受到已知恶意软件入侵，但尚未展示出被感染的行为	4	具有下载恶意可执行文件、恶意PDF或挂马网页等行为的主机，但是无用户感染的迹象
	3	具有下载疑似恶意文件行为的主机，如文件后缀和文件名不符，但是无用户感染的迹象
感染可能性：低 主机展现出了感染恶意软件的低可能性行为	2	主机正在使用可能被恶意软件用作通信协议的已知或未知协议，如IRC协议，主机访问疑似恶意软件通信使用的域名、IP
	1	检测出了中低威胁异常流量的主机，或者具有访问钓鱼、盗号等恶意网站或邮件行为的主机，如SSL协议跑在非标准的443端口

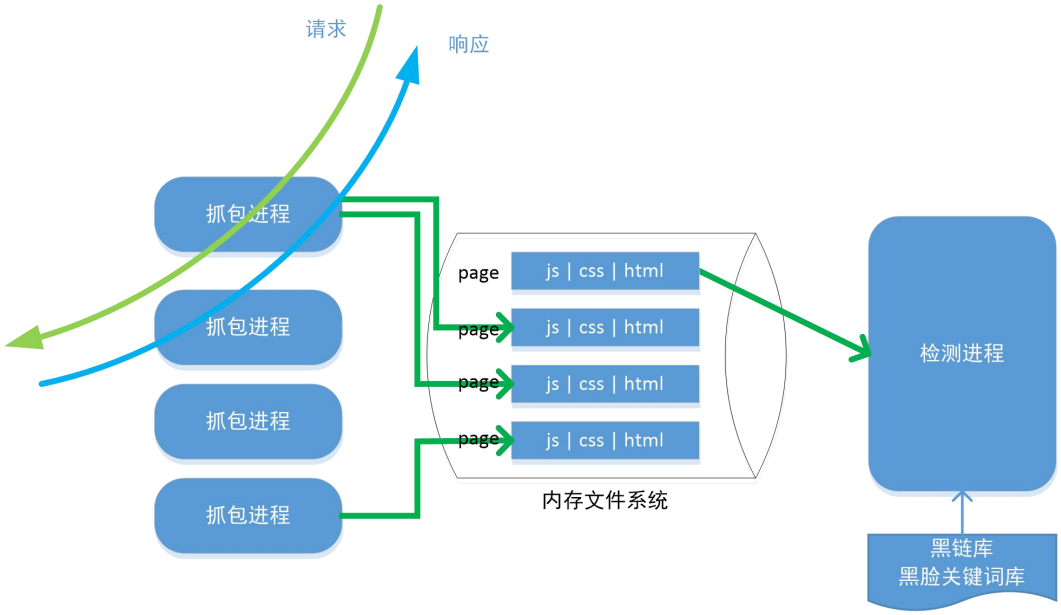
3.5.1.2. 黑链检测

黑客通过非法手段在 web 服务器中的的页面插入非法链接，或者在 web 服务器中放置存在非法链接的页面。这些非法链就是黑链。

黑链对客户造成许多的不良影响：损害网站形象、降低搜索排名、同时也说明客户网站存在严重安全隐患。

黑链检测功能实现识别客户的 web 服务器是否被植入黑链。其技术实现原理为：先通过对经过放火墙的流量进行 http 抓包，还原 html 页面、js 文档、以及 css 文档；然后从黑链特征、黑链 url、以及黑链关键词、js 跳转等几个方面对黑链进行检测。

黑链检测通过在线更新机制，维护黑链 url 库和黑链关键词库，保证检测的有效性和正确性。



黑链特征检测

检测页面中存在<a>标签的块属性标签或者<iframe>等标签是否存在隐藏自我的样式。

黑链 url 检测

检测外链<a>标签的跳转目标是否为已知的非法站点。

黑链关键词检测

检测外链<a>标签和关键词敏感的标签的内容中是否存在常用的黑链关键词。

js 跳转检测

检测 js 语法，发现异常的站点跳转。

3.5.2. 安全响应

为了帮助客户在发现问题后进行快速响应，避免因延时处理带来更大的危害，深信服 NGAF 通过三个层面帮助客户解决网络安全问题。

3.5.2.1. 策略自动生成

日常运维中大多数用户每天都会看到上千条的安全日志，在对于这些安全问题的处理上如果依靠人工分析那么往往无法快速有效的策略配置。在对设备的配置方面还需要原厂工程师协助处理，这个日常工作带来了很大的延误。

深信服 NGAF 通过基于问题的发现，可自动生成响应的防护策略，帮助客户快速简单的实现策略更新，更快地实现安全防护。

3.5.2.2. 工具提供

对于失陷主机的发现往往可以快速帮助客户定位问题根源，但问题发现后往往带来的便是如何清除的问题。深信服 NGAF 自带僵尸主机清除工具，帮助客户简易处理失陷主机，快速清除隐患。

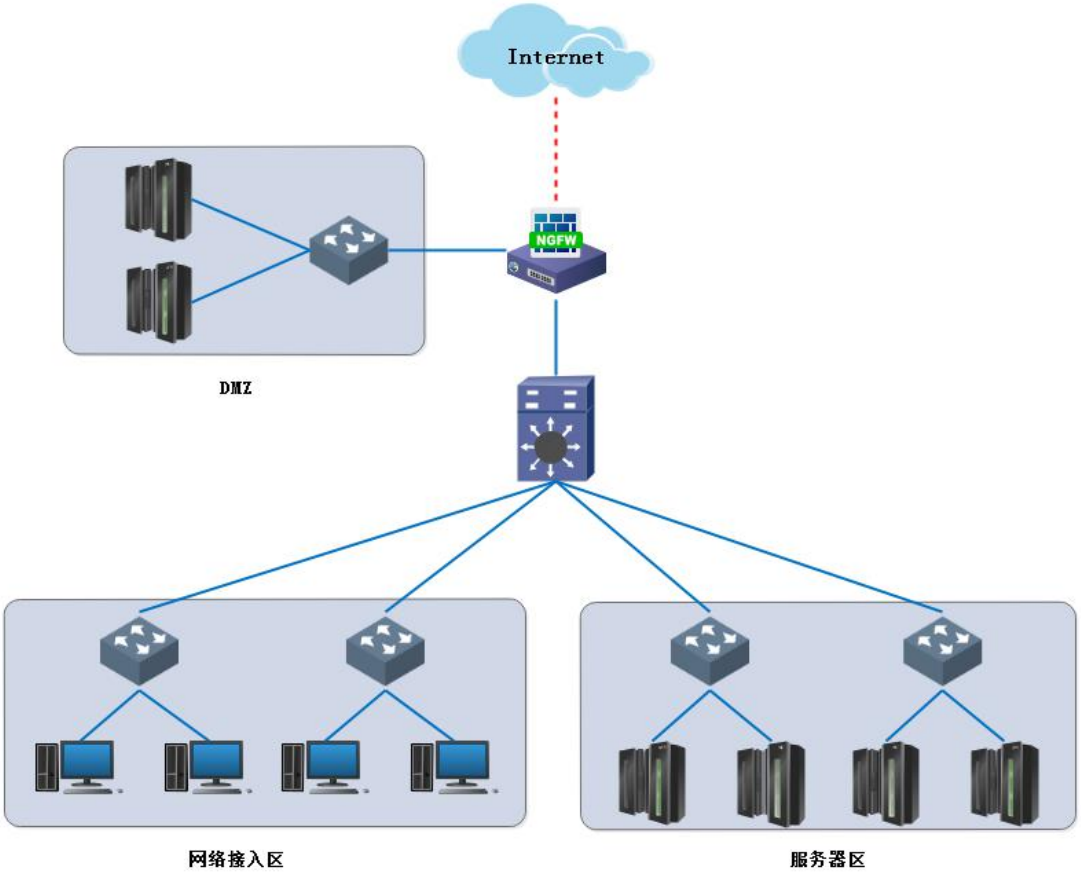
3.5.2.3. 云端支持

深信服 NGAF 通过云端在线的安全专家，可以 7*24 小时的快速协助用户处理安全问题，针对发现的安全风险进行安全加固，对于未知的问题进行威胁鉴定，通过人工服务弥补机器的智能缺陷。

4. 部署模式

4.1. 网关模式

网关模式是指设备工作在三层交换模式，NGAF 以网关模式部署在网络中，所有流量都经过 NGAF 处理，实现对用户或者服务器的流量管理、行为控制、安全防护等功能。作为的出口网关，NGAF 的安全功能可保障网络安全，支持多线路技术扩展出口带宽，NAT 功能代理内网用户上网、服务器发布，实现路由功能等。



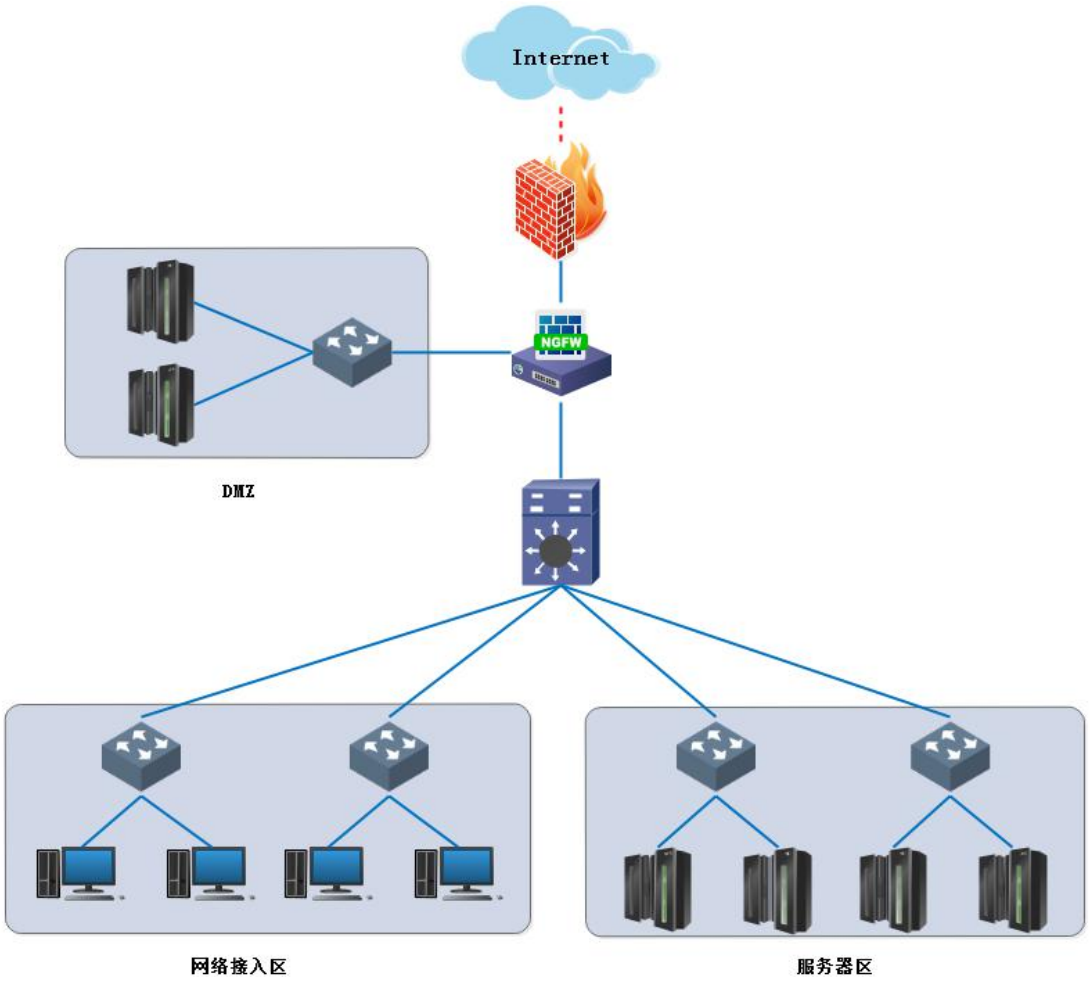
部署方式：

- NGAF 的 WAN 口与广域网接入线路相连，支持光纤、ADSL 线路或者是路由器；
- NGAF 的 LAN 口（DMZ 口）同局域网的交换机相连；
- 内网 PC 将网关指向 NGAF 的局域网接口，通过 NGAF 代理上网。

4.2. 网桥模式

4.2.1. 单网桥模式

网桥模式是指设备工作在二层交换模式，NGAF 以网桥模式部署在网络中，如同连接在出口网关和内网交换机之间的“智能网线”，实现对用户或者服务器的流量管理、行为控制、安全防护等功能。网桥模式适用于不希望更改网络结构、路由配置、IP 配置的环境。

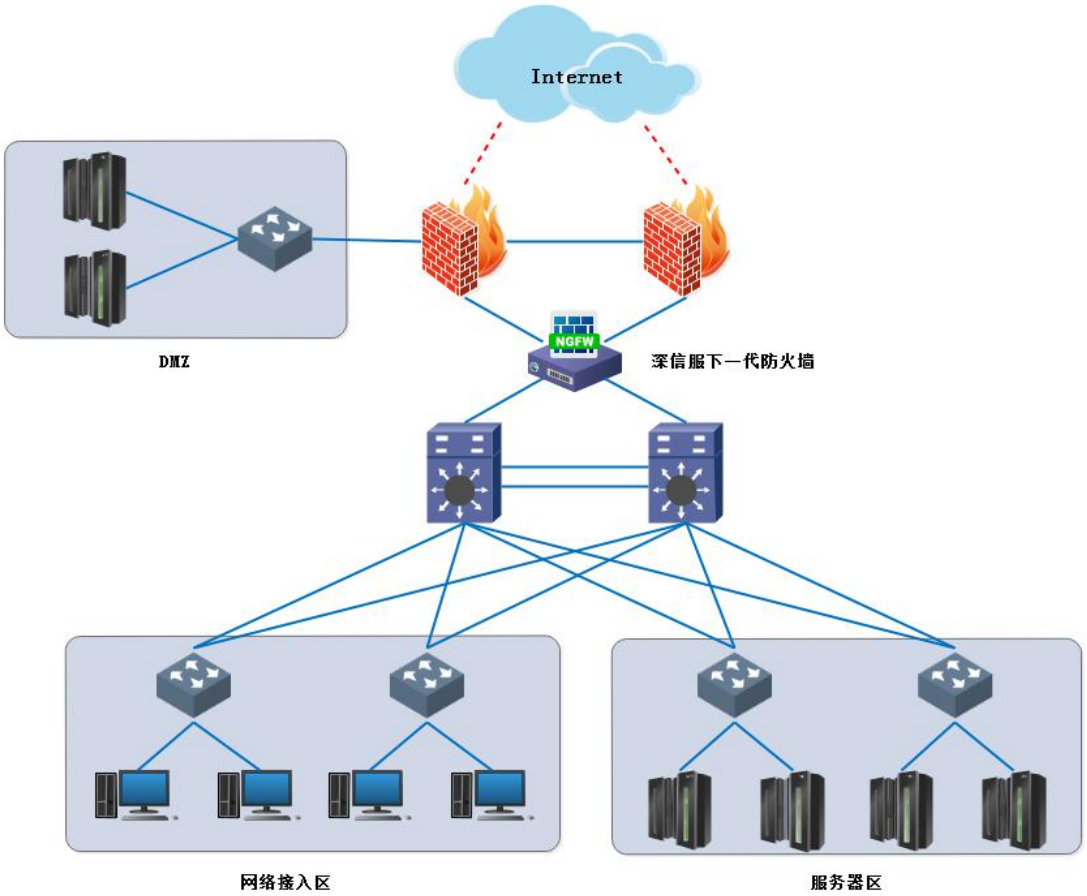


部署方式：

- NGAF 的 WAN 口同出口网关 LAN 口相连，为 NGAF 分配一个网桥 IP，该 IP 和出口网关 LAN 口在同一网段；
- LAN 口（DMZ 口）同核心交换机连接；
- 局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

4.2.2. 多网桥模式

考虑到网络的稳定性、可靠性，往往采用双机、双线路构建基础网络。NGAF 支持多路桥接模式，适应多机网络环境要求。在不影响原有双机、双线路前提下，对流经 NGAF 的所有数据流进行控制、拦截、流量管理、安全检测等操作。

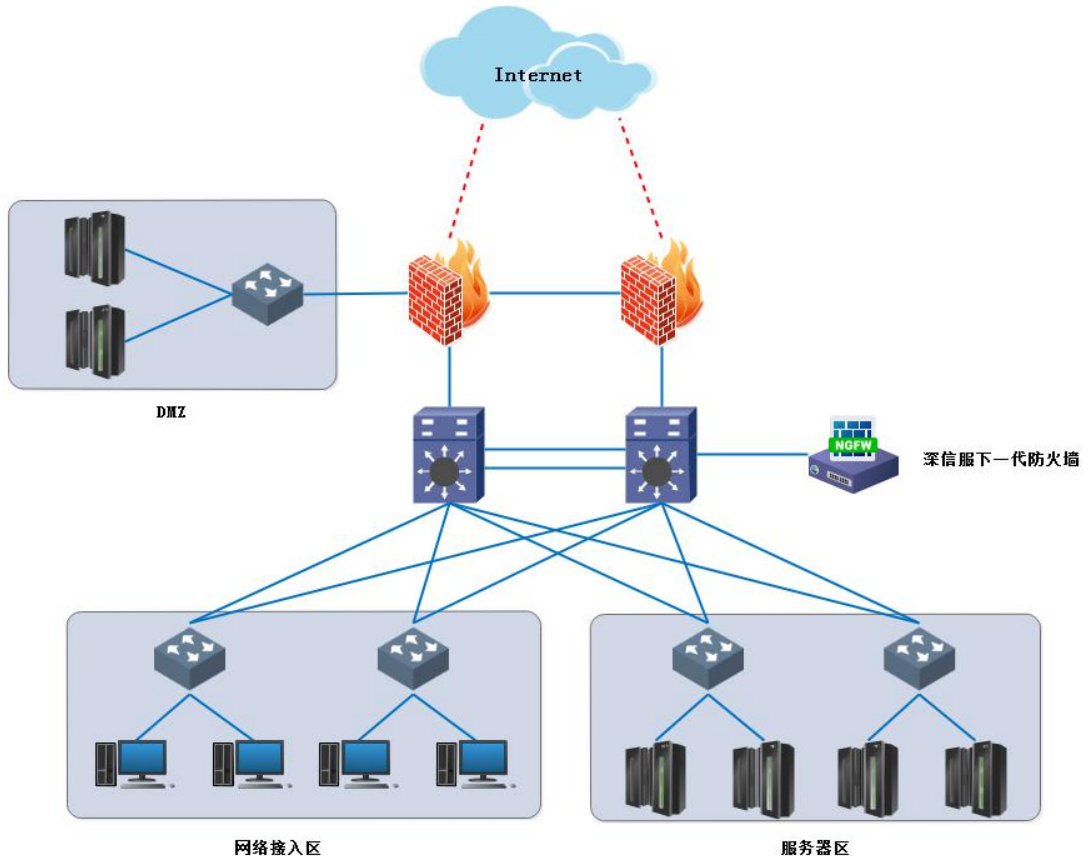


部署方式：

- 通过 NGAF 配置界面，定义两对桥接口（WAN1-LAN1，WAN2-LAN2）；
- 为每对网桥分配 IP 地址。

4.3. 旁路模式

NGAF 以旁路模式部署在网络中，与交换机镜像端口相连，实施简单，完全不影响原有的网络结构，降低了网络单点故障的发生率。此时 NGAF 获得的是链路中数据的“拷贝”，主要用于监听、检测局域网中的数据流及用户或服务器的网络行为，以及实现对用户或服务器的 TCP 行为的管控。



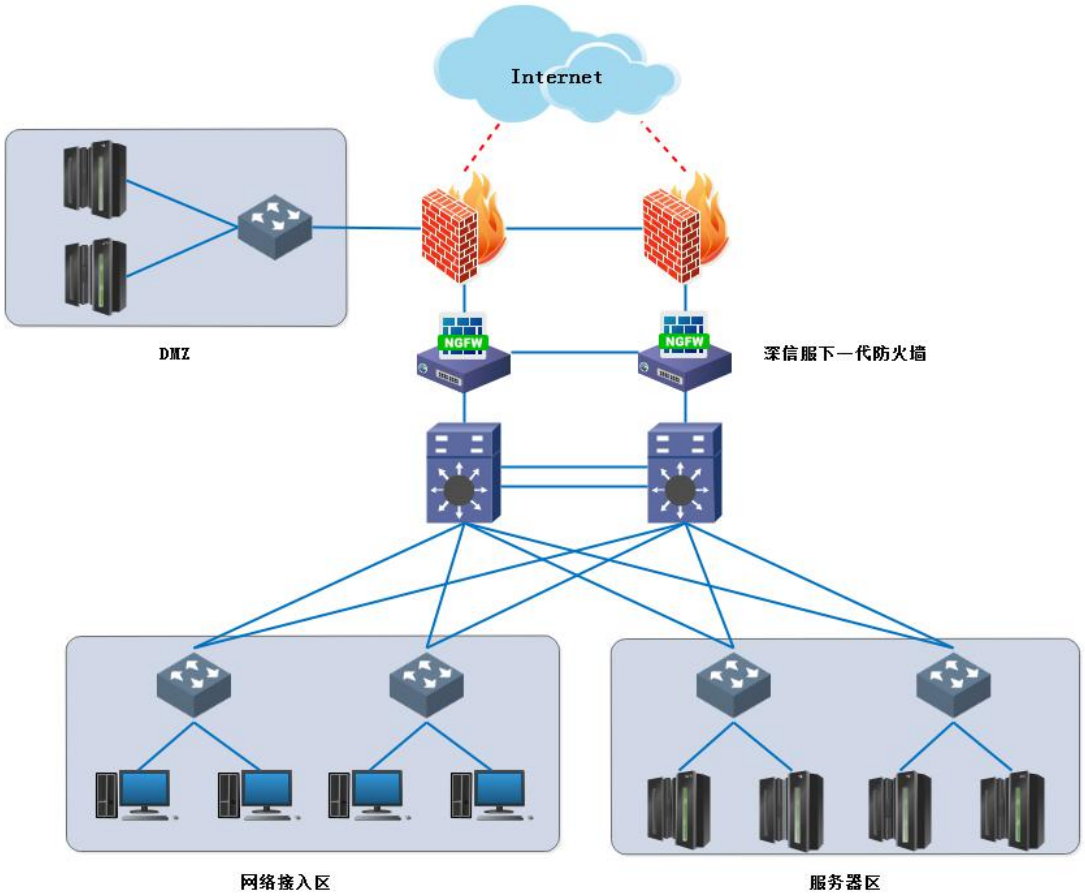
部署方式：

- 配置出口交换机的镜像端口，与 AC 的广域网口相连，实现对内网数据包的监听。

4.4. 双机模式

4.4.1. 主主模式

为了同时部署两台设备，NGAF 支持两台以上设备同时以主机模式运行，起到设备冗余与负载均衡的作用。在这种环境中，NGAF 以单网桥模式、多网桥模式或者网关模式部署在网络中。

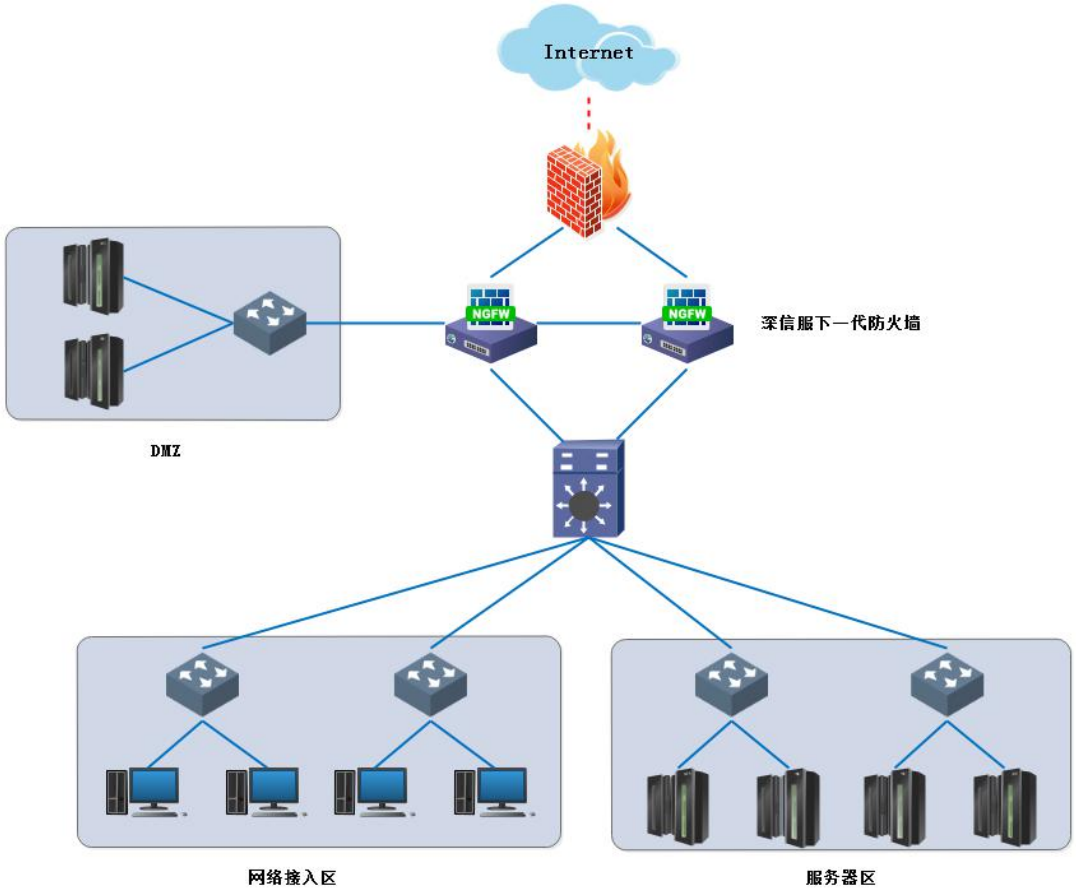


部署方式：

- NGAF 以网桥模式或者路由模式部署在网络中，为每台 NGAF 配置网桥 IP；
- 每台设备上指定的通信网口在同一个局域网内，NGAF 之间即可实现同步。

4.4.2. 主备模式

为了网络稳定可靠，同时部署两台设备，NGAF 支持两台设备以双机模式运行。两台设备通过心跳口相连，一主一备，当主设备发生故障时自动切换到备用设备，提高网络的稳定可靠性。在这种环境中，NGAF 以单网桥模式、多网桥模式或者网关模式部署在网络中。



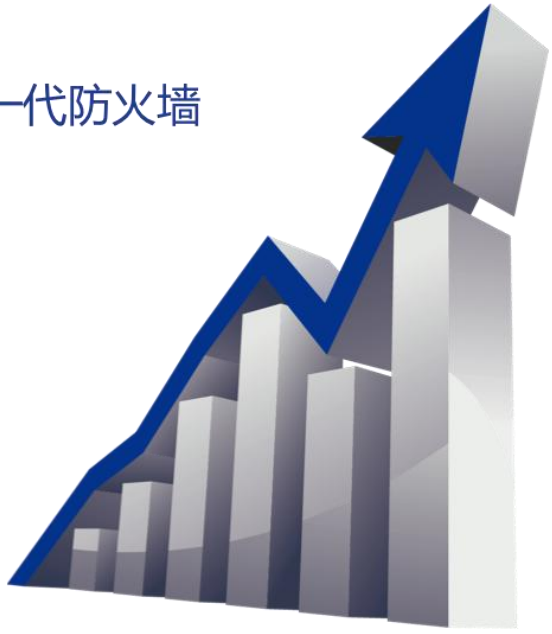
5. 市场表现

5.1. 高速增长，年复合增长超 70%

2011年发布**国内首台**下一代防火墙

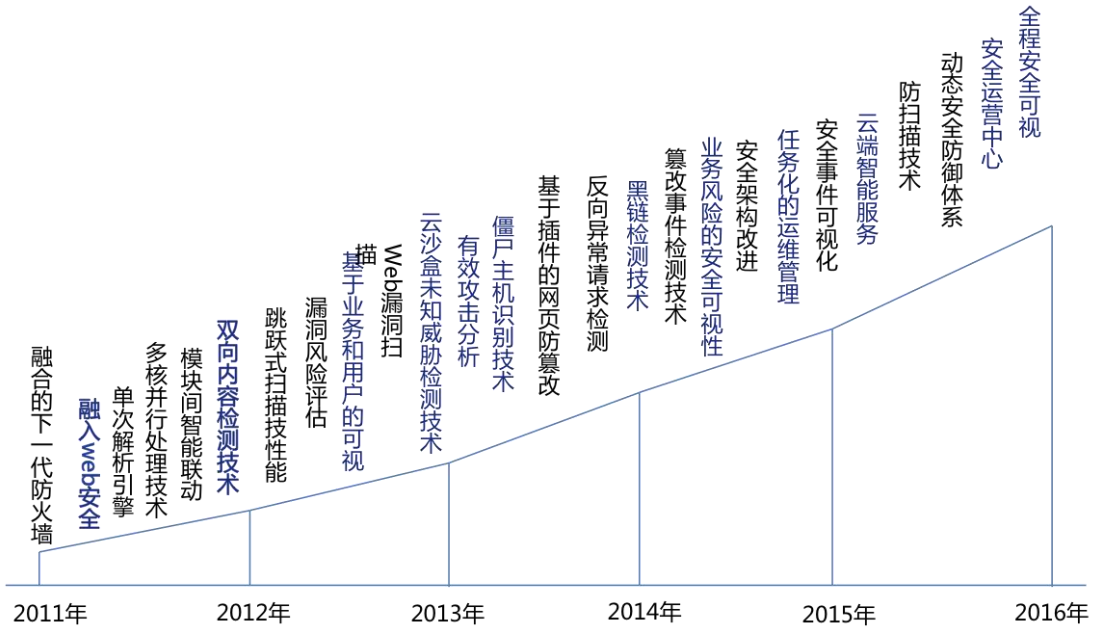
4万家用户一致好评

5.4万台在线稳定运行



5.2. 众多权威机构一致认可

5.3. 为客户需求而持续创新



6. 关于深信服

深圳市深信服科技股份有限公司成立于 2000 年，是专注于网络安全与云计算领域，致力于为用户提供更简单、更安全、更有价值的创新 IT 解决方案服务商。

目前，深信服在全球共设有 55 个直属分支机构，其中包括香港、新加坡、马来西亚、印尼、泰国、英国和美国等七个国际直属办事处和分公司，员工规模将近 3000 名。

随着企业规模的扩大发展，深信服也获得了多方认可。先后获得了“CMMI5 国际认证”、“第一批国家高新技术企业”、“国家规划布局内重点软件企业”“亚太地区德勤高科技高

成长 500 强”等殊荣。同时，深信服还是 IPSec VPN 和 SSL VPN 两项国家标准的主要承建单位、并受邀参与制定《第二代防火墙标准》。在行业合作上，深信服是互联网应急中心应急服务支撑单位、国家信息安全漏洞共享平台 CNVD 成员单位、中国国家信息安全漏洞库 CNNVD 技术支撑单位和公共漏洞和暴露组织 CVE 认证合作单位。

目前，全球有近 40,000 家用户正在使用深信服的产品。其中，在中国入选世界 500 强的企业有 80%的企业都是深信服的用户。同时，凭借优秀的产品表现，深信服多款产品入围了包括国家税务总局、国家电网、建设银行、工商银行、中国移动和中国电信在内的各行业集采，各款产品均得到了广泛应用。

时刻走在行业前沿，深信服始终保持着创新能力

多年来，深信服持续将年收入的 20%投入到研发，并在深圳、北京、长沙和硅谷设立了研发中心，研发人员比例达到 40%。在对创新发展的持续投入下，深信服一直保持着每 1-2 年推出一款新产品、每季度更新 1 个新版本的研发速度。截至 2016 年 6 月，深信服共申请超过 400 项国内发明专利以及 20 项美国专利。此外，深信服是推出了全球第一台 IPSec VPN 和 SSL VPN 二合一 VPN，是国内率先推出上网行为管理和下一代防火墙的厂商。

将产品和服务做到更好，深信服快速响应市场需求

深信服研发人员每月都会进行例行的客户拜访以收集产品需求，每年都能收到超过 1000 条有效需求，并在研发工作中将其迅速转化为产品新版本。同时，深信服在深圳、长沙、吉隆坡三地设有超过 100 坐席的 CTI 中心，提供 7*24 小时的电话咨询和远程调试服务。在全国范围内，深信服在 49 个城市设立了备品备件库，配有原厂工程师更快地提供技术支持。

进入的每一个细分市场，深信服都会努力成为佼佼者

深信服的硬件 VPN、SSL VPN、上网行为管理、广域网优化等多款产品保持在市场占有率第一位；下一代防火墙市场排名第二，应用交付产品市场排名第二、也是排名第一的国产品牌。目前，深信服 SSL VPN、上网行为管理、下一代防火墙、广域网优化、应用交付、服务器虚拟化基础架构 6 款产品均入围了 Gartner 魔力象限，获得国际认可。