# 不妥协的安全

目录



华为企业ICT解决方案 悉您所需 为您所用

HUAWEI


# 华为2013年度安全研究报告

DDoS攻击次数较去年同期增长了 29.81%

HTTP应用性攻击占 87.74%

超过 72.91% 的攻击流量大于1Gbps

最长攻击持续了 349小时36分钟42秒

详细报告:
http://enterprise.huawei.com/topic/AntiDDoS_2013/index.html


## 华为USG6000下一代防火墙 悉您所需 为您所用

**以精准感知能力全面保障您的网络安全**

迈入云时代，网络边界日渐模糊，网络环境愈加复杂，企业需要更加可靠的安全屏障。华为USG6000下一代防火墙，基于ACTUAL全局环境感知，具备业内领先6000+应用识别能力和500万威胁识别能力、8种用户认证手段和全业务虚拟化技术，提供精细高效的业务隔离和安全防护，全面保障网络安全。

- 基于ACTUAL（应用，内容，时间，用户，攻击、位置）的环境感知体系实现业务环境的全局感知，提供真正面向业务的安全管控
- 6000+应用识别，500万威胁防护，30+文件内容感知提供了精准的访问控制能力
- 全新的硬件平台和引擎设计，实现了应用层性能的大幅提升，提供万兆级的全威胁防护能力，满足大型企业网络防护

更多详情，敬请访问：**enterprise.huawei.com**

*华为USG6000下一代防火墙*

扫描二维码 查阅解决方案详情

扫描二维码 查阅官方微博

使用微信 扫一扫 二维码添加 官方微信

HUAWEI

华为，不仅仅是世界500强

# ICT技术发展下的新安全

左文树
华为安全产品领域总经理

## Q：未来3-5年，企业网络安全面临的主要安全风险是什么？

A：ICT快速发展的今天，信息化已经融入各行各业，渗透到企业的各个环节，如办公、生产、服务、配送等，信息化已经成为现代企业的生存之本。信息化正高速发展，未来3-5年，云、移动化、社交化以及大数据将会完全与企业网络相融合，不断改变企业的网络环境，变革企业信息的存储、共享和使用的方式，一个更加开放的网络模型正在形成。下面我们从“端-管-云”的角度看这个ICT变革带来的安全挑战：

### 终端侧

伴随智能终端的普及，BYOD的盛行，众多安全隐患出现：一、在同一台智能终端上同时处理私人数据和企业数据，给企业数据的信息安全带来隐患；二、大量私人终端的使用，从而形成终端多样化，管理复杂化的特点；三、移动化让传统以IP地址定义网络边界日益模糊，边界安全逐渐失守。而越来越多的入侵行为以移动终端作为突破点，向企业内部发起入侵，随着4G网络的成熟，智能终端被当成黑客入侵企业内网的绝佳跳板。非法接入，身份盗用、匿名访问、越权使用、数据泄漏以及移动操作系统与应用的漏洞和隐藏木马都将成为未来企业在终端层面面临的主要安全风险。

### 管道侧

随着社交化的发展，移动应用海量增长，各种社交软件、办公软件、网络应用类软件广泛接入企业网络，让攻击和数据泄露的途径丰富多样。传统基于IP地址和端口的策略和防护手段在各式基于web的应用面前收效甚微。未来不久，移动应用又将成为黑客攻击和数据窃取的主要途径，传输途径多样化既带来企业运营效率提升，同时也增加了威胁入侵的渠道。在信息化的发展变革中，这个矛盾将长期存在，将成为企业面临的又一主要安全风险。


# 云端侧

云计算以其卓越的创新性和前瞻性，给IT行业、互联网行业和通信行业在技术和商业模式方面带来了深刻影响，被广泛视为信息产业的下一次革命。云战略已越来越成为企业信息化发展的必然选择，同时作为企业新业务的战略发展方向。当企业数据中心改造、迁移到云中之后，数据大量集中，越来越多的核心信息资产存储在云端，这在带来信息访问便捷化的同时，也让企业的核心机密更加集中、更加暴露的处于开放环境。这必然引起黑色利益集团的垂涎，针对核心数据的破坏、篡改以及窃取事件将越来越多，且规模庞大，手段多样化，APT攻击方式将盛行，这将是企业网络在云端面临的主要安全风险。

## Q: 在应对这些安全挑战的过程中，企业应该重点关注的问题是什么？

A: 企业CIO的关注重点将会聚焦于大数据、移动化、云服务和社交化，并不断调整企业架构，以适配环境的不断改变。面对新的企业架构，安全是需要重点考虑的问题。面对未来3-5年的安全风险，整体安全防御架构、安全管控的全面性以及安全运营成本应该是CIO重点关注的问题。 面对快速发展变化的网络环境，企业应该具备一种动态弹性的安全架构，可根据网络环境和威胁变化动态调度威胁防御，实现全网层面的统一防护，避免出现短板而使防御体系坍塌。其次，需要从“端-管-云”的角度思考安全建设，实现终端管控、管道监管、云端数据保护，提供全面纵深的防御能力；当威胁向应用层迁移，管控能力也需要同步迁移到应用层，这就需要重点关注面向应用层的管控能力，安全设备的应用识别能力尤为重要，可识别的应用种类要多，更要细，要能够对应用的不同功能进行区分。



## Q: 华为下一代防火墙（NGFW）是如何践行华为安全战略的？

A: 根据“下一代网络安全”的总体战略，华为USG6000系列下一代防火墙将整体的安全管控构建于感知能力基础之上，通过“ACTUAL”全局环境感知架构，在应用、内容、时间、用户、攻击和位置六个维度提供精确的感知能力，构建出一个多维的立体感知模型，通过感知模型，将网络环境映射为业务环境，并将业务可视化，这样更有利于提供真正面向业务的安全管理。

在下一代网络环境，我们不应该再仅仅从孤立的产品视角去看待防火墙，他应该是整个网络环境的一个控制单元，不仅可以通过自身计算提供全面的安全防御，而且需要具备响应整网防护需求的调度，满足全网安全协防的调度需求，从单点防护步入全网防护年代。在敏捷网络中，所有设备都变成安全事件的监听者，通过将可疑流量引入虚拟的安全资源中心，实现全网安全资源的按需使用，实现全网的整体防护。

敏捷网络的安全资源中心通过对全网设备安全事件的汇总，让下一代防火墙也具备基于大数据的可疑行为分析，增强对未知威胁的响应能力。与此同时，华为云安全能力中心的多项技术创新成果在华为下一代防火墙上首次被商用。在云端，通过最全面的安全沙箱和信誉体系配合，华为下一代防火墙具备对各类APT攻击的快速响应能力，有能力保障下一代网络环境的全网安全。

Demand Generation 是通过规划并执行系列营销活动，引导客户购买意愿，从而为公司的产品、服务或解决方案生成销售线索的市场营销举措。■

对于安全防御体系和安全产品功能复杂度的提升，在不过多增加资金预算的情况下，满足对新型环境的安全运营管理成为企业CIO关注的另一热点问题。如何能够根据网络环境、业务流量以及威胁态势，基于大数据分析和流量分析自动生成管理策略、自动下发并形成良性循环，同时保障安全管控的准确度，这是企业CIO在不断关注和寻找的安全管理方向。

## Q: 华为“下一代网络安全”的安全战略是怎样的?

A: 华为下一代网络可以理解为基于SDN架构的新型敏捷网络，而华为下一代安全强调的是敏捷网络下的可控、可用、可信。安全设备能够更细致的感知企业ICT环境，通过上下文信息对风险和威胁得出全面的分析和判断。在华为敏捷网络中，安全不再是一个个孤立的网络节点，而是通过多层次的虚拟化技术构成了一个安全资源池，动态管理，按需调度，实现全网安全协防。同时，结合华为在全球部署的云安全信誉体系，提升对网络攻击和风险的快速响应与防护能力，抵御未知威胁。

华为致力于网络已经超过20年时间，服务安全领域也超过10年时间，为全球超过数万企业和电信运营商提供安全防护，在网络与安全领域积累了丰富的经验。为了落实下一代网络安全战略，华为打破传统思路，从新的角度出发重新思考，实现安全的三个转变：

- 第一个转变是从被动到主动。华为在遵守各个国家/地区法律法规、不涉及侵犯隐私的前提下在全球部署云安全系统，采集安全事件与样本，为IP、URL和文件构建信誉，企业部署华为安全产品之后即可享受到华为全球信誉云的服务和评估。
- 第二个转变是从技术为本到客户为本。华为下一代安全把以前只放在专业安全厂商实验室里的技术使其产品化，部署到客户网络中和云端，直接为客户提供服务，把未知恶意软件的防御响应时间缩短到“分钟”级甚至“秒”级。其中最具代表性的就是沙箱技术。
- 第三个转变是首次把大数据用于安全防御。华为通过自身遍布全球五大洲的企业专网和IT系统上的成功实践，把大数据应用于企业信息安全防御。通过对网络设备、安全设备、终端系统和业务系统的事件采集，在大数据平台上进行关联分析，从而能够发现非法的攻击行为。

在华为的SDN方案设计之初，我们就坚定的认为下一代安全必须与下一代网络是一个整体，只有这样才能解决传统网络安全的不解之祸。

# 下一代防火墙面临的新挑战

**下一代防火墙，即NGFW（Next-Generation Firewall），2009年由全球著名分析机构Gartner定义，至此在硬件安全网关市场引起了一场“工业革命”。全球主流安全网关厂商纷纷向NGFW定义看齐，争先恐后将自有产品升级到NGFW或推出全新的NGFW系列产品，NGFW已成为硬件安全市场最为闪耀的一颗新星。**

**至今，NGFW的概念已产生五年，按照ICT的发展速度，五年基本是一代产品的更换周期。在这五年里，并没有第三方分析机构对NGFW进行重新定义，于是各个安全厂商纷纷拉起了一场重新定义NGFW风潮，希望对它赋予更高的能力要求，满足ICT技术与网络威胁的快速发展。本文将追溯到重新定义NGFW的源头，悉数NGFW面临的诸多挑战来看NGFW的发展方向。>>**

## 环境的改变从未停止

移动化、社交化、云和大数据是ICT发展的四大趋势。根据Facebook 2013年Q3财报，Facebook月活跃用户达11.9亿人，其中移动端占据8.74亿，比去年同期增长了45%，全球1/6人口在使用社交应用。 根据Dimensional Research的调查结果显示，55%以上的受访企业认为移动安全是当前的TOP安全问题，其中71%的受访企业认为移动设备增加了安全事件，47%的受访企业有大量客户数据存储在移动设备上。

NGFW作为网络边界安全防护产品，必须能够适配网络环境的不断变化，才能提供精确的网络安全防护。但BYOD让网络边界日渐模糊，企业环境更加开放，社交应用为信息的传递提供了更便捷的途径，云和虚拟化正在改变企业的信息化使用方式。这一系列的变化仅仅依靠NGFW定义中的“应用+用户”识别越来越难以支撑。

对感知能力诉求的不断增强将是NGFW在新环境下的最大挑战，防护的精准程度将直接取决于感知能力。如何感知环境的变化？如何进行移动终端的访问控制？如何感知用户漂移？如何管控移动应用的每一个动作？如何适配虚拟环境的迁移？这些都是NGFW在ICT环境不断变迁情况下需要重点考虑的问题。

## 网络威胁愈演愈烈

经济利益、商业对抗等正驱动网络攻击由单兵作战转向集团进攻。APT(Advanced Persistent Threat)攻击是一种来自于不同区域，有组织、有特定目标、隐蔽性强、破坏力大、持续时间长的新型攻击，是当前最有代表性的一类攻击形式。APT的最显著特点是：攻击特征难于提取；单点隐藏能力强；攻击渠道多样化；攻击持续时间长。APT攻击的如上特点，使传统以特征匹配、实时检测与阻断的防御方式基本失效。

对于此类攻击的防护要求，NGFW定义本身提及甚少，如果NGFW仅仅使用特征匹配的单一防护方式，终将导致边界防护的彻底失效。那么究竟该如何对抗APT？NGFW需要不断调整思路，采取多样化检测与控制手段，才能应对挑战。

然而APT只是新型攻击方式的一种，随着经济利益的诱惑，攻防能力的博弈，各种新型攻击随时有可能产生，是否能拿出一套具备实时响应能力的动态防御体系，应对各种新型攻击模式，形成有效的防御机制，这是NGFW在当前威胁环境下面临的主要挑战。

## “管理体验”的需求不断提升

传统防火墙工作于网络层，基于端口进行管控。被管控的端口比较固定，数量通常少于100个，因此，传统防火墙的对“简单管理”的诉求并不突出。但NGFW的概念让防火墙的管理从网络层上升到了应用层，将面向数以千计的应用和数以万计的用户，管理复杂度增长最少2个数量级。另一方面，在NGFW上，安全防御复杂度提升，除了传统防火墙功能外，入侵防御、防病毒、URL过滤、数据防泄露等一系列功能的融合让管理维度增加，复杂度提升。而客户的需求始终是在产品的升级换代过程中，能同时保持客户体验的提升。

高级锁定目标攻击(Advanced Targeted Attacks，ATA)正不断渗透标准的安全管控，让安全管控一成不变的企业蒙受巨大的商业损失。面对日益复杂的网络环境，企业必须遵循最小授权原则，不断调整安全策略才能保证安全，如何有效地做到这一点，是NGFW在管理能力方面的一个新的挑战。

从过去十年FW的应用来看，防火墙规则总是到处泛滥，但是入侵防御和应用控制使问题更加复杂。现在正是使用下一代防火墙降低复杂性的时机，但是如果实施不当，则可能会适得其反。

NGFW只有在管理体验上不断超越，才能发挥时代赋予它的防护职责。

## 性能需要不断超越

作为“网络出口，直连部署”的特殊场景需求，FW对性能的追求从未停止过，业内T比特防火墙都已产生。但当多项安全功能叠加后，防火墙在性能上是否还能表现优异？UTM（Unified Threat Management）的产生在带来成本降低、部署简单的同时，性能骤降70%~90%让企业（尤其是大型企业）望而却步。自2004年UTM被定义至今，已近十个年头，UTM依然无法逾越性能低的鸿沟。

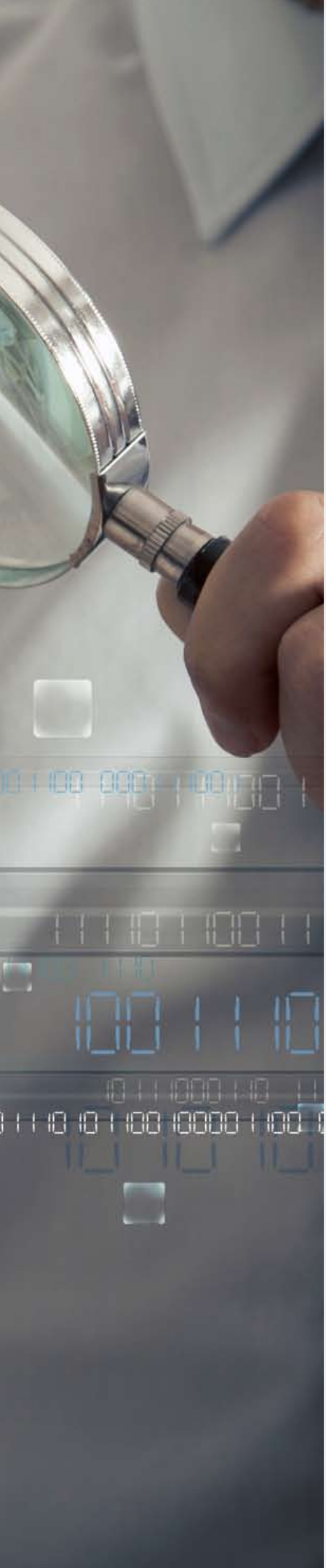
NGFW作为UTM的一种替代形式，必须从根本上解决性能问题。在NGFW的定义中，明确指出 NGFW必须能够满足大型企业的边界防护需求。那么大企业的边界防护需求如何定义呢？业内有些NGFW产品在开启应用识别能力后，性能下降超过50%，开启全威胁防护后，性能下降甚至达到70%。如果没有一个刚性的定义，那NGFW与UTM在性能方面就没有了质的区别，NGFW依然难以摆脱低性能的阴影。

NGFW要满足大型企业出口防护，性能必须有一个刚性的量化指标，当开启全威胁防护后，性能下降不应超过50%，同时应该提供万兆的双向全威胁防护性能。■

综上所述，对于NGFW而言，虽然Gartner对它赋予了全新的能力要求，但随着ICT环境和网络威胁的发展变化，满足定义要求的NGFW同样面临诸多挑战。一款好的NGFW，不但应该满足最基本的定义要求，同样需要面向变化趋势和客户诉求，满足一系列由于业务驱动的更加完善的能力要求。值得欣慰的是，各大安全厂商已经纷纷发起了对NGFW的重新定义，对自身NGFW产品提出了更加严格的要求，市场已有不少优秀的NGFW出现，满足下一代网络环境的边界安全防护。

# 打造不一样的下一代防火墙

下一代防火墙（Next-Generation Firewall，NGFW）在访问控制的精细度、威胁防护范围、易用性、性能四个方面对传统防火墙进行了革命性的改变，业界普遍认可对NGFW的这个定义。但满足NGFW的定义要求就足以应对风云变幻的ICT环境吗？业内厂商对于这一问题，纷纷交出了自己的答卷。华为对于自己的NGFW，提出了更高的要求，以满足下一代网络环境下的边界防护需求。>>



## 传统安全网关之困

随着互联网的发展以及IT/CT技术的深度融合，企业的运营模式发生了巨大改变，无论是生产还是营销都更多的依赖于互联网。利用新技术带来效率提升的同时，企业面临的安全形式也更加严峻。一方面，攻击数量快速增加，基于Web的攻击每年以600%的数量增长；另一方面，攻击的手段更加隐蔽，方法越来越多。除了传统的入侵、病毒、木马、蠕虫外，还出现了APT（Advanced Persistent Threat）攻击这种新的攻击形式。人们突然发现，传统的安全设备已经无法保障企业网络安全。

- 不足的管控：与过去不同，企业当前使用的大部分应用与端口不再有一一对应关系，而是基于Web开发的。传统安全网关在进行流量检查时看到的是千人一面，无法准确的识别和区分不同业务，更不要说进一步的差别控制了。移动办公的趋势使员工经常在不同的区域接入网络，原有基于固定IP安全管控的模式也不再有效。

- 复杂的管理：为防御各种攻击，安全设备提供了更加强大的功能，这对使用者的技能提出了极高的要求。企业很难在安全市场上招聘到具备足够技能的安全专家，只能做简单的安全管理，难以充分发挥安全设备的全部作用。

- 孤立的防护：黑客行为从原来的文化变成一个产业，网络攻击更加频繁，手段也越来越复杂。传统的安全设备要么只能防范单一类型的攻击；要么多种设备各自为政，缺乏有效的协同，被攻击轻易绕过。

- 安全与性能无法兼顾：UTM（Unified Threat Management）将多种安全功能叠加在一起，看起来解决了综合防御的问题。但由于架构中各安全模块能是串行设计的，当同时使用防火墙之外的其他功能时性能会急剧下降。常见的，UTM开启IPS后，性能会衰减到原有的10~20%。UTM用户只能在安全和性能之间二选一。

尽管业界不断推出新的安全产品，但很多是新瓶装旧酒，只是对传统设备某部分的优化，未从根本上解决问题。安全设备必须对ICT变化提出的新需求做出响应，重新设计。

## 业界NGFW之惑

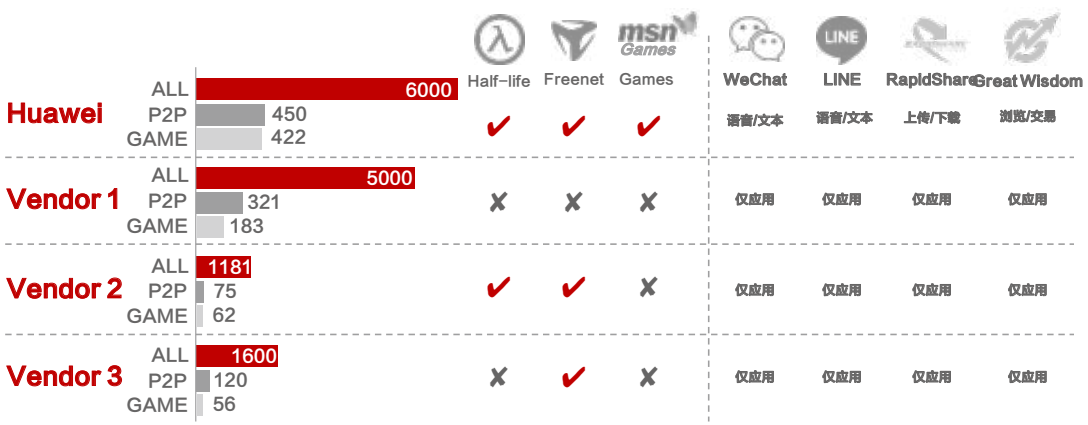
2009年Gartner提出了下一代防火墙（NGFW, Next Generation Firewall）的概念，就是为了适应ICT的新趋势、新变化，解决传统网关设备无法解决的问题。总结对NGFW的定义，可以概括为下面的几个特征：

- 包括传统防火墙的功能，具备应用感知的能力，并使用基于应用的安全策略。NGFW是在新ICT环境下传统防火墙的替代品，对传统FW的应用场景必须前向兼容。需要将防火墙最基本的访问控制功能扩展到应用，尤其是对大量基于Web开发的应用的管控。应用感知是NGFW引入的最重要的能力之一。
- 防火墙与IPS的深度集成。两个功能要相互协作而不仅仅是的简单叠加，提供的安全大于使用两个独立设备的总和。
- 额外的防火墙智能。提供更多的信息，帮助使用者更好地制定出合理的安全策略。
- 满足大企业使用的性能要求。不同于UTM，当IPS开启后整体性能不会下降过多，依然满足在大企业使用的要求。

## 精细的访问控制

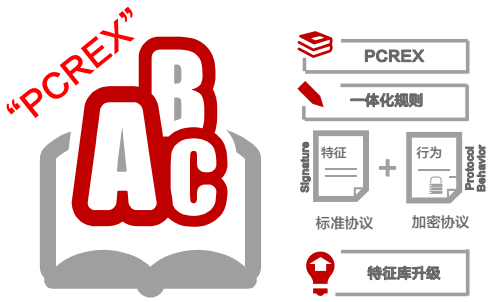
访问控制是NGFW的基础能力，访问控制应该更加精准。受益于超过10年的业务感知（Service Awareness）技术积累，和不断增加的研发投入，华为提供了业界最精细的访问控制能力。

华为NGFW能够基于应用、用户、时间、内容、威胁、位置6个维度进行对网络流量进行管控。在应用管控方面，能够准确识别超过6000种网络应用，数量业界最多。与其他厂商不同，华为NGFW不仅能识别出应用，更能对应用的不同功能进行区分。例如：对于Line应用，可以区分文字聊天和语音；对网盘类应用RapidShare，能够区分出上传和下载。



当前的应用为了避免被网关设备识别并控制，采用了很多躲避技术，例如：端口伪装、乱序、随机填充、加密等，如果仅仅依靠报文的特征码很难准确的识别。华为拓展了正则语法（PCRE, Perl Compatible Regular Expressions），开发出PCREX语言作为应用特征的描述语言，让应用特征变成可以运行在华为智能感知引擎(IAE, Intelligence Awareness Engin)上的一段代码。通过报文分片重组、协议去干扰、统计识别、行为识别等综合手段，准确的识别各类复杂应用。使用PCREX描述应用特征还带来另一优势，更新应用识别能力无需升级防火墙软件，不会中断企业的业务。这个特点使华为NGFW的识别能力更新速度远超其他厂家。


**多种分析技术**
**让加密应用无所遁形**



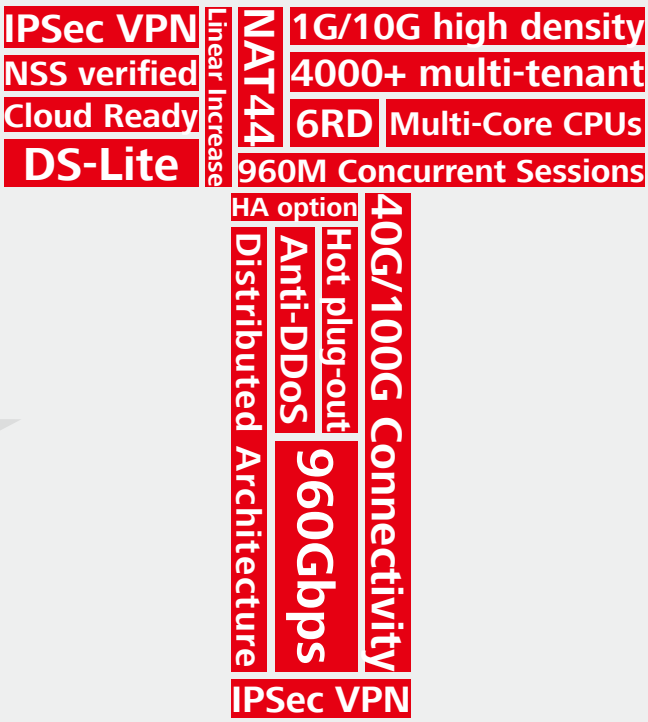

**独家数据驱动语言**
**引擎免升级识别不中断**

华为的NGFW利用“多”、“细”、“准”、“快”的应用识别提供了最精细的访问控制能力。

## T比特级别的云数据中心保护

USG9500

华为云数据中心防火墙USG9500为大企业网络、数据中心和ISP提供了卓越的性能，多维度的威胁防护和高可靠性。
Learn more at http://enterprise.huawei.com/cn/products/network/network-security/firewall-utm/hw-143117.htm

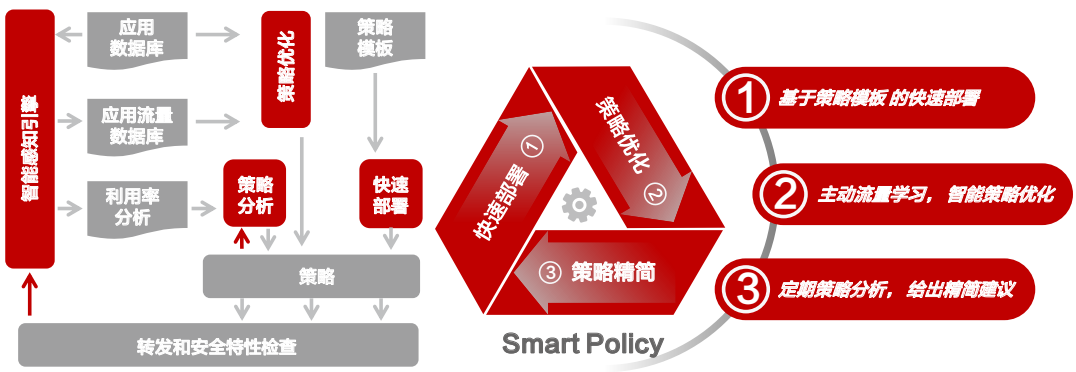



## 简单的管理

攻击无孔不入，企业需要遵循“最小授权原则”，不断调整安全策略确保合法的访问通道不会被攻击所利用。遗憾的是，在企业对NGFW的实际使用中很难做到这一点。通过客户调研和第三方分析，华为发现CIO在管理上对防火墙最大的三个关注点。

- 安全策略如何实施
- 基于应用的访问策略是否正确
- 如何优化防火墙策略级

企业的传统网关上遗留了大量的基于端口的防护策略，需要将这些策略优化为基于应用的防护策略。市场上的一些NGFW产品，仅提供了有限的报表作为策略优化的参考，优化工作还是依赖于安全专家的经验和投入。尽管优化和策略的有效性验证耗费了巨大的时间和人力，策略的准确性还是难以保证。因此，很多企业即使采购了NGFW产品，依然部署着原有基于端口的策略，这无疑隐藏着巨大的风险。




华为NGFW的Smart Policy技术，采用人工智能的手段帮助安全人员维护安全策略。基于使用场景提供基础模板，实现策略快速部署；能根据网络流量环境给出建议的安全策略，帮助安全人员准确、快速地完成策略优化；识别出冗余和失效的策略，帮助安全人员精减无效策略，简化管理。通过华为的Smart Policy技术，安全管理员无需过多的技能和时间就能做好管理，降低安全设备的TCO。

## 全面的威胁防护

华为不仅实现了防火墙和IPS的深度集成，将病毒防护（AV，Anti-Virus）和内容过滤功能也深度集成到了NGFW中。应用特征、IPS特征、AV特征采用同样的PCREX语言进行描述，实现了三位一体的防护。此外，华为利用业界最全的沙箱——PE沙箱、Web沙箱、手机沙箱，建立安全信誉体系。网关受益于安全信誉，能够及时发现利用零日漏洞发起的攻击。


最全面的沙箱种类
有效抵御APT

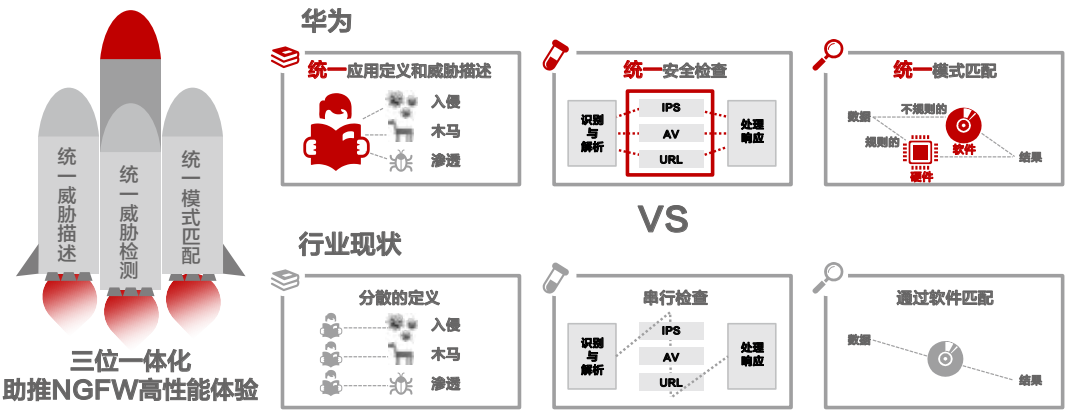
| Sandbox | Windows | WEB | Mobile |
|---|---|---|---|
| Huawei | ✓ | ✓ | ✓ |
| Vendor 1 | ✓ | ✗ | ✗ |
| Vendor 2 | ✓ | ✗ | ✗ |
| Vendor 3 | ✓ | ✗ | ✗ |
| Vendor 4 | ✓ | ✓ | ✗ |

**独家支持手机沙箱，快速识别手机恶意威胁**

## 高威胁防护性能

华为在开启所有安全功能时，性能下降不超过50%，满足大企业场景的使用需要。保持高性能得益于三个核心技术：

- 第一，所有的特征采用统一的描述语言，对网络流量的解析只做一次，解析的结果在后续的检测中可以共用。避免了重复解析的资源消耗。
- 第二，不同于UTM中各个安全模块的串行处理，华为NGFW在应用识别后，多项安全功能的处理是并行的，缩短了整体时延。
- 第三，华为NGFW针对大流量、大运算能力的配备了专门的协处理器，避免对防火墙访问控制性能的影响，也大幅提高了IPS等内容安全的性能。




三位一体化
助推NGFW高性能体验

华为的NGFW产品解决了ICT新形势下企业网络安全对访问控制、防护范围、易用性、性能上的新诉求。建立了一个安全、友好、可靠的威胁防御体系，成为企业网络新时代的安全守护神。■

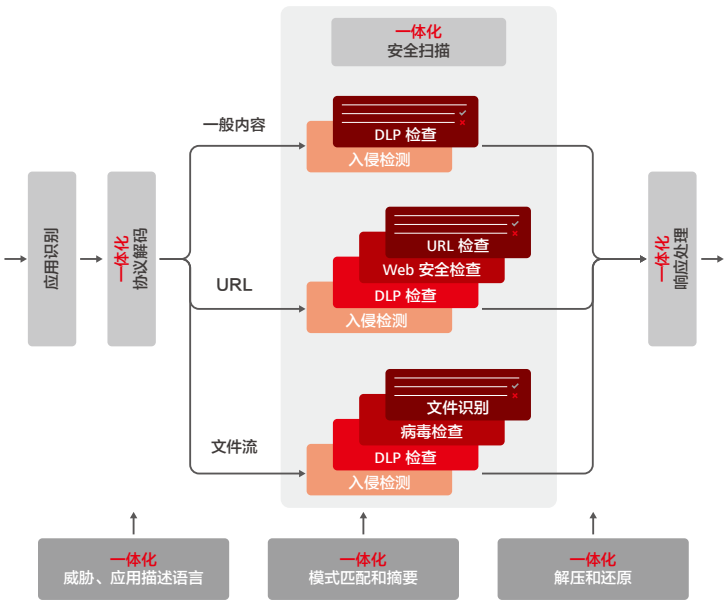
# 高性能下一代防火墙是如何炼成的

“安全有余、性能不足”，这或许是UTM（Unified Threat Management）产品的一个最大遗憾。当NGFW（Next-Generation Firewall）产品被定义，“满足大型企业应用”成为NGFW对性能要求的最低门槛。华为2013年发布的USG6000系列下一代防火墙产品，，实现了安全和性能的完美融合，在打开所有威胁防护下，能够实现万兆级的应用层全威胁防御。华为USG6000采用智能感知引擎（IAE，Intelligent Awareness Engine）技术和NG-Security新一代硬件平台，提供了NGFW产品高性能支撑，产品全面覆盖1G-40G应用层防护场景。

华为下一代防火墙采用全新一体化架构的智能感知引擎（IAE, Intelligence Awareness Engine），通过该项技术，能够实现下一代防火墙的核心安全功能，同时能够带来全功能和高性能的全新用户体验。>>

IAE是三位一体的安全业务处理框架和一系列安全特性或组件的集合，配合各种安全知识库，以及和安全智能中心实时联动，是方便各种产品在其上进行内容安全业务的定制、扩展、集成和快速发布的安全服务程序。其中，何谓三位一体的安全处理架构？即统一威胁定义、并行威胁检测和模式匹配加速三个方面的一体化加速处理。区别于传统安全设备，各种威胁采用不同的定义方式，IAE采用了统一的PCREX语言定义多种威胁，为核心模块的统一处理奠定基础，加快了威胁识别的效率。在检测过程中，基于多核CPU架构，IAE采用了一次解析，多业务并行处理的架构。其核心的应用解析和特征匹配处理由硬件加速模块高速处理，各个安全业务并行的跟踪处理结果并更新状态，当威胁特征的条件都符合时，立即根据安全策略触发响应动作，而当条件不符合时，IAE会自动调整跟踪状态，确保检测安全的流量高速转发。这种架构确保了多种安全业务开启情况下，对整体性能影响最小。

另外，华为下一代防火墙采用了全新一代高性能系列NG-Security硬件平台。NG-Security硬件平台采用“多核MIPS”+“硬件协处理加速”+“高速SwitchFabric”的架构，通过高速总线实现多核CPU与业务处理模块、接口扩展模块之间的通信。NG-Security硬件平台同时进行了冗余设计，提高硬件可靠性。增强了性能和功能的扩展，进一步实现了存储的扩展，满足网络安全设备对本地日志存储的需要。




全新的一体化架构

华为NG-Security硬件平台采用64位高性能新一代多核MIPS平台，MIPS架构基于一种固定长度的定期编码指令集，其精简的指令集、指令与高速数据缓存分层的设计、并发的多级流水线、以及专门为网络报文吞吐所设计的高速接口及DMA能力，结合华为公司电信级的嵌入式实时操作系统，保证了华为下一代墙平台处理的高性能。同时，在NG-Security硬件平台的高端机型，还可多扩展一块CPU处理板，即相当于实现1+1的CPU扩展能力，每颗CPU均为多核MIPS处理器，这样的弹性扩展能力可实现硬件处理能力的翻倍。

华为NG-Security硬件平台集成了IPSec、SSL加解密运算、压缩解压缩、模式匹配、以及硬盘RAID的硬件协处理器。使得本来应该由CPU软件来计算处理的特定、重复的耗费CPU性能的业务，如加解密、压缩解压缩、模式匹配等，由协处理器来完成，其处理能力将有质的飞跃。同时CPU就不需要参与此类复杂计算，对CPU的消耗大大降低，使CPU集中实现擅长的网络报文的处理。

华为NG-Security 硬件平台选用容量达480Gbps的交换芯片作为多核CPU、业务处理模块、扩展接口模块之间的互联总线，高容量的交换总线为模块之间的提供的足够的带宽，保证了各模块之间的业务交换。同时选用大容量高速的SAS硬盘，为用户提供实时记录日志和报表，减少CPU与外围网管采集软件的交互流量和性能消耗，进一步提高CPU的利用率，并且为用户提供实时大容量的日志和报表记录。■

华为下一代防火墙软硬兼施，内外兼修，通过其软硬件的创新，在相同防火墙性能的条件下启用应用威胁防护特性后，性能下降在50%以内，实现真正意义上的万兆全防御性能，达到业界顶尖水平，为客户提供全网络最佳的性能体验。安全和性能两者兼得。

# 下一代防火墙引发的管理变革

社交网络、云、BYOD的兴起，致使应用爆炸式增长，各种利用应用风险形成的威胁泛滥，传统的以协议和端口为威胁防护基础的安全网关无法再满足日益严峻的安全形势需要，下一代防火墙（NGFW）应运而生，成为近年来安全业界的热点。>>

## 下一代防火墙需要额外的智能

NGFW全新的安全视角，把应用作为安全策略的基础元素，不仅实现应用可视，更专注于精细化管控，使得企业在遵循最小授权原则下，部署和执行严格的安全策略成为可能。NGFW具有深度融合IPS、防恶意软件等安全功能,比传统防火墙更具威胁防护能力，使得企业对不同应用部署合适的深度防护成为可能。


**所有这些，NGFW看上去对安全的理解相当完美，那么，是不是拥有NGFW就意味着从容面对各种威胁，高枕无忧?**

NGFW在带来精细化管控和深度安全防护的同时，也给防火墙管理员带来了巨大挑战。

首先，基于应用的安全策略带来了策略部署的复杂度。传统网关基于端口进行管控和防护，被管理的端口数量少且变化不多。NGFW基于应用进行管控和防护，被管理的应用数量数以千计。管理员一般都非常熟悉端口，也很明白基于端口去制定策略。如果让防火墙管理员先去了解和熟悉数以千计的应用，以及每个应用带来的安全风险，再来制定基于应用的安全策略，管理复杂度可见一斑，这显然对防火墙管理员的技能提出了更高的要求，管理员将很难制定出符合最小授权原则的策略。

其次，对于从传统防火墙迁移到NGFW的企业，遗留大量的传统防火墙基于端口的安全策略急需迁移到NGFW基于应用的安全策略，发挥NGFW精细化管控的能力。但两者并没有一一对应关系，凭借防火墙管理员的自身理解，逐条进行迁移是不切实际的。

再次，防火墙策略往往跟随企业的业务发展而不断增多，长期的手工维护，导致不少冗余和低效策略，致使防火墙管理变得低效和容易出错，带来安全性问题。

因此，即使拥有了NGFW，但是管理不好NGFW，也无法给网络带来实质的安全，NGFW需要额外的智能。

## 华为安全策略智能管理解决方案

华为NGFW以安全以“设备”为本为理念，推出安全策略智能管理解决方案。通过策略快速部署组件、流量智能学习引擎、智能策略优化器、智能策略分析器等重要组件，发挥NGFW应用可视和威胁感知的最大效应，实现把安全风险与策略制定有机结合起来，把防火墙管理员从学习应用、分析应用风险、定义安全策略等工作中解放出来，让NGFW设备成为风险发现者和策略推荐者，让防火墙管理员成为策略决策者，有效提升管理员的工作效率，提高策略制定和实施的正确性，保障企业业务的安全。

面对中小企业新部署防火墙的场景，华为NGFW策略快速部署组件提供基于应用小类的多种预定义策略模板，如针对社交网络的安全深度防护策略模板，针对即时通信的上网行为管理策略模板、针对P2P类应用的限流策略模板等。这些预定义的策略模板，已经帮助管理员把应用进行分类，并根据应用的不同风险，预定义了安全动作，管理员可根据自身的业务情况，直接引用策略模板创建策略，并加以简单的配置修改即可直接部署，大大降低了基于应用的安全策略部署难度，提升了网络运维效率。

对于那些从传统防火墙过渡到NGFW的企业，华为NGFW通过智能流量学习引擎和智能策略优化器两大组件，对已有的传统防火墙安全策略进行调优。首先，流量智能学习引擎对周期性的的业务模型进行学习，凭借华为业界领先的应用感知技术，覆盖超过6000种应用种类，保障对企业业务的细粒度识别。其次，智能策略优化器通过分析应用的各种风险，如承载恶意软件、数据泄露风险、可被利用攻击等，对整体业务情况进行安全评分，有效展示网络中的应用组成和应用风险。再次，智能策略优化器基于应用组成和应用风险情况，给出NGFW基于应用的安全策略策略建议，如配置IPS/AV/内容过滤/文件过滤等深度安全防护。从而把防火墙管理员从大量繁杂的学习应用、分析应用风险、定义安全策略等工作中解放出来，只需关注NGFW优化后的推荐策略是否符合企业要求，决策是否接受建议或者在推荐策略的基础上简单进行修改配置，快速进行策略调优。

对于那些拥有数以千计甚至更多防火墙安全策略的企业来说，华为NGFW通过智能策略分析器的独特算法，对安全策略相互间的冗余情况、策略本身的命中率情况、策略对象的命中率情况进行分析和呈现，指导管理员快速识别冗余和低效元素，按需进行策略精简，企业无需再购买昂贵的第三方策略分析软件，降低投资和运维成本。■

# 华为助多特蒙德体育场开展体育经营新模式

华为下一代防火墙为多特蒙德体育场在宽带时代下的体育场经营提供了全面、高效、可靠的安全防护，并利用有限的租用带宽为球迷提供了满意的宽带服务质量 >>

## 背景

德国多特蒙德足球俱乐部（BVB）是历史悠久的德甲豪门，曾获得8次国内顶级联赛冠军、3次德国杯冠军、5次德国超级杯冠军，以及1次欧洲冠军杯和1次欧洲优胜者杯。在2012~2013赛季的欧洲冠军联赛，多特蒙德杀入决赛。其主场西格纳伊度纳公园（Signal Iduna Park）体育场最大容量80645人，曾作为1974年和2006年世界杯的比赛场地，是德国最大、全球第九大体育场。在2012~2013赛季，场均观众人数数全球第一，达到80534人。为了提高球迷粘性，并拓展新商机，多特蒙德体育场决定部署无线接入服务，并开展在线博彩、facebook、twitter，视频回放点播等业务，给球迷提供更好的服务和更丰富的网络体验。

多特蒙德体育场要利用有限的接入带宽，为大量访问者提供宽带接入服务。既要确保自身提供服务的安全、可用、稳定；又要保障服务质量，为不同类型的用户提供差异化的服务质量；同时，对用户的上网行为进行管理，避免为体育场带来法律风险。

## 高性能、高可靠的全面安全防护

球场内开展的在线博彩、视频回放点播、facebook、twitter等业务，需要进行全面的安全防护。保证安全的同时也要保障服务的体验和可靠性。充分利用有限的Internet出口带宽，为八万名球迷提供差异化的服务质量。多特蒙德体育场面临的关键挑战包括：

- 对提供服务的数据中心进行Anti-DDoS保护；检测入侵并以一定方式进行防护；准确识别出入数据中心的文件是否包含病毒，按预定义的措施进行处理。保证八万余观众能够流畅、不间断地享受体育场提供的服务；
- 利用租用的有效带宽，优先保障视频点播、在线博彩、网页浏览等网络服务的质量；优先为季票观众、VIP球迷、提供更好的宽带服务；
- 能够查看并审计球迷的网络访问行为，禁止球迷访问非法网站，给体育场带来法律风险；

## 华为体育场经营安全防护和流量优化解决方案

为应对多特蒙德体育馆万兆高性能安全防护和流量优化的需求，华为提供了基于下一代防火墙的安全防护方案，在体育场的Internet出口和数据中心各部署两台USG6680。方案的优势和特点如下：

### 1. 全面安全防护，高性能、高可靠

在部署在数据中心的防火墙上开启IPS、AV、Anti-DDoS功能，保护体育场的网络服务的持续可用。在部署在Internet出口的防火墙上开启URL过滤、应用识别与控制、审计等功能，对球迷的网络访问行为进行管理，并进行流量控制优化服务质量。USG6680采用专用协处理器加速流量内容解析和处理，在全部防护功能全部开启后，防火墙吞吐率仍能达到20Gbps，确保防火墙不会成为网络瓶颈。Internet出口和数据中心部署的USG6680均配置双机热备，以负载分担方式工作，保证服务的可靠性。

### 2. 准确的应用识别，灵活的带宽管理，保障关键业务质量，提供差异化服务

USG6680能准确识别6000种以上的网络应用，并基于应用进行带宽管理，提高关键业务的服务质量。例如：禁止P2P应用，避免低价值流量占用带宽资源；识别视频、网页浏览类应用后，修改其DSCP标签提高转发优先级，在后续的路由设备上优先转发。

USG6680支持8种用户认证方式，与体育场的用户认证系统同步认证信息，基于用户控制带宽，制定每个用户的最小带宽和最大带宽。对于不同类型的用户，例如：季票观众、VIP球迷、普通球迷、临时观众，提供不同的最小带宽保障，提高对核心用户的粘性。

### 3. 通过URL过滤和安全审计，识别恶意用户，避免法律风险

USG6680的URL分类功能能够准确的对超过8500万网站进行分类，并支持自定义URL分类。通过URL过滤功能，体育场可以控制球迷对非法网站的访问，避免法律风险。同时开启审计功能，记录球迷访问的URL，识别出反复尝试访问非法网站的用户和账号，对其进行控制。



## 从容应对宽带接入时代的体育经营

华为基于万兆下一代防火墙帮助多特蒙德体育场构建了安全、高效、高性价比的万兆宽带访问和数据中心防护体系，利用有效的带宽满足了超过8万名球迷对宽带服务的高质量使用需求，助力多特蒙德体育场在宽带接入时代从容开展体育经营新模式。

# 华为助力深圳广电构筑下一代广播电视网信息安全基础架构

在所有的备选产品中，华为USG6000系列下一代防火墙在性能和安全能力方面表现优异，同时有效保障了可靠性、扩展性和易管理要求，成为深圳广电办公网、业务网边界防护的首选。>>

## 背景

2010年1月，温家宝主持召开国务院常委会议，决定加速进行“三网融合”建设，在广电行业加速推进下一代广播电视网（NGB, Next Generation Broadcasting Network），2010年7月，国务院发布了第一批三网融合12个试点城市名单，深圳位列其中。

深圳广电地处中国改革开放的前沿窗口，引领了电视传媒的生产与管理，打造“国家三网融合示范城市”。2011年，深圳广电率先完成网络融合改造，在“三网融合”总体推进过程中起到了排头兵的作用。2011年5月，原国家广播电影电视总局科技司下发了《GD/J038—2011 广播电视相关信息系统安全等级保护基本要求》，深圳广电全网融合下的信息安全架构建设就是按此要求展开的。

## 关键挑战

广播电视网是我国重要的信息基础设施之一，在业务内容、舆论公信度等方面具有不可替代的优势，电视节目不仅仅是信息传播工具，而且是党和政府最重要的舆论阵地。NGB发展遵循的总体原则为保障国家信息与文化安全，建立符合全业务运营要求的可管、可控、具备安全保障能力的技术管理系统和业务支撑系统。具体分为三个阶段，第一阶段（2010-2012年），研究三网融合战略下安全与管理体系；第二阶段(2013-2015年)，研究支持超高速、超大容量、高效率、可重构的网络技术，适合于三网融合的安全设备；第三阶段(2016-2019年)，根据NGB的整体目标，面向发展过程中的新问题，结合技术、业务和安全管理的最新发展，持续推动NGB自主创新。具体安全建设依据等级保护要求。

深圳广电前期已完成了对办公网、业务网及数据中心的定级与备案工作，随着业务的不断发展与融合，信息安全问题越发显得重要。

2013年NGB安全建设已进入第二阶段，正是安全设备选型和采购的关键时期，那么什么样的安全设备才能满足NGB的总体技术要求和广电行业等级保护的安全性要求呢

## 高安全性：

深圳广电希望分别在互联网边界，生产网边界和数据中心边界提供全面的防护能力，保障业务24小时不间断运行。设备必须满足等级保护要求，满足不同级别的防护要求。不但包括细粒度的访问控制能力，还需要深度融合入侵防御、防病毒，Anti-DDoS和应用识别等各项安全特性。

## 高性能：

适应广电业务的流量特点，确保能够在高峰流量期对业务进行全面的安全检查，同时也要考虑未来业务发展的总体要求，这就需要最少10G以上的全业务防护性能。

## 高可靠性:

鉴于广电业务的特殊性，深圳广电希望所有的安全防护采用双机冗余部署，并实现主要硬件器件冗余能力，最大限度的保障业务可持续性。

## 可扩展性:

作为运营网络，必须能够支撑业务的快速发展和网络需求的变化，具备灵活的，多样化的组网能力。同时，支持IPV6网络环境，不但提供网络协议转发，更可基于IPV6网络提供全面的安全防护。

## 简单易用:

广电网络“三网融合”的转换过程也是由专网向公共网络转换的过程。对于数据网络的诸多安全问题，深圳广电网络安全人员期望更简单高效的管理，因此希望安全设备在满足安全防护的同时，管理越简单越好，最好是“傻瓜式”的。

## 解决方案

为了保障产品符合业务诉求，深圳广电对国内外各厂商产品进行了严格的测试，华为USG6000系列下一代防火墙在性能和安全能力方面表现优异，同时有效保障了可靠性、扩展性和易管理要求，成为深圳广电办公网、业务网边界防护的首选品牌。

华为根据深圳广电不同业务场景的性能要求，通过USG6650+USG6680相结合的解决方案，在互联网边界和办公网边界采用USG6650提供20G防护，在业务网边界用USG6680提供40G防护，为每一个业务系统和办公系统提供边界隔离与防护。同时全网设备通过管理中心统一调度管理和报表展现，整网方案为深圳广电构建了一套简洁高效的安全防护体系。

USG6000系列是华为2013年发布的下一代防火墙新品，在满足Gartner对NGFW定义要求的基础上，提供6000+应用识别和6维安全管控，是业界管控能力最精细的下一代防火墙。USG6000系列在能力上紧随ICT发展趋势和威胁趋势变化，提供基于特征的入侵防护和基于行为的未知威胁防护，为深圳广电提供了全面的网络安全防护。

## 客户价值

**防护能力最全面，保障深圳广电业务顺畅。**USG6000系列在提供基于特征匹配的入侵防护和病毒防护能力的基础上，更基于云端沙箱技术，提供对未知威胁的行为特征分析，可有效防范针对广电业务系统的各类未知威胁及APT攻击。在网络双向提供精细的访问控制和用户身份认证，提供基于用户和应用权限管理，即保障了深圳广电业务的稳定开展，也可满足广电行业不同级别的安全等级保护要求。

**全威胁高性能防护，支撑大业务流量。**USG6000系列通过全新的软硬件设计，可以做到在全威胁防护开启情况下，性能下降小于50%，在所有参与的安全厂商中，性能下降幅度最小。大于10G的全威胁防护性能有能力同时为每一个业务系统提供全方位的安全防护。全特性的虚拟化能力还可为每一个等级的业务系统提供独立的安全计算环境，保障“国家级”等保防护要求。

**硬件可靠性设计，保障业务延续。**华为为深圳广电提供的解决方案在电源、风扇、硬盘上均采用冗余设计，同时在每个节点采用双机热备冗余部署，有效降低了每一个环节可能带来的业务风险。

**面向网络发展趋势，兼顾未来业务防护。**USG6000系列采用了高密度接口设计，最大可提供64个千兆接口和16个万兆接口的扩展能力，保障深圳广电在业务进一步发展的情况下充分的接口扩容能力。同时，USG6000系列提供全面的IPV6支持，在未来深圳广电与IPV6网络对接时，即可保障顺利对接，也可实现IPV6环境下的安全防护。

**高效的管理手段，降低TCO。**华为USG6000系列在设计开发过程中引入了全新的管理理念，即基于流量学习的自动化策略配置和优化。在设备上线时通过预置模板提供快速部署；上线后通过流量学习与分析，自动生成安全策略建议，不断的细化安全策略管理。在稳定运行后，通过策略学习自动精简冗余策略，提高策略匹配效率。USG6000系列的自动化管理手段让深圳广电轻松开启了全威胁安全防护，TCO降低30%以上。

华为下一代防火墙深圳广电解决方案解决了用户的相关建设诉求，在保障业务安全性和延续性的同时，严格按照广电行业等保要求进行产品推荐和方案设计，助力深圳广电构筑全网融合安全信息基础架构信息安全等级保护工程。华为方案的优异表现获得了深圳广电领导的一致好评。

# 只要点击，不要攻击。

## 华为Anti-DDoS方案助力阿里巴巴在11.11抵御庞大攻击，创造350亿元交易记录

Alibaba.com

11.11购物节当天，黑客也在疯狂“血拼”。然而华为Anti-DDoS方案却能轻松化解攻击，助力阿里巴巴单日交易量达到1.88亿笔，交易额突破350亿元。它采用全流量采集、大数据分析的思想，从50多种纬度建模和关联分析，可实现全面攻击防护和秒级响应速度，是业界唯一单机可提供T级DDoS防御能力的产品，每年帮助阿里巴巴抵御40,000多次攻击，树立电子商务的安全新标杆。

请登陆**www.huawei.com**了解更多。

HUAWEI

如需更多信息，
请扫描二维码

**商标声明**

 、HUAWEI、**华为**、  是华为技术有限公司的商标或者注册商标。
在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

**免责声明**

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

**华为技术有限公司**
**深圳市龙岗区坂田华为基地**
**电话**: (0755) 28780808
**邮编**: 518129
**版本号**: M3-032102-20140221-C-1.0

www.huawei.com