2013年1月22日星期二

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

信息安全解决方案关键信息一指禅

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

【1】防泄密 Key Message

KM1：领先的精细化管控手段确保企业信息资产不泄露

方案特色1	多达16种管控手段保护企业终端各种场景下的安全 **给客户带来的价值**：各种场景下确保企业终端不泄露机密信息 **差异化**：多达16种手段保证终端数据不泄密，包括外设接口管理控制、终端非法外联控制、屏幕拷屏控制、磁盘/USB存储设备加密、移动终端数据加密及远程擦除等, 业界最全。
方案特色2	精细化过滤，保证企业外发信息安全 **给客户带来的价值**：避免企业员工通过邮件外发、web外发、IM外发等方式泄露企业机密信息 **差异化**： 1.支持外发文件类型及大小检查，依照预定策略实施放行或阻断，防止涉及知识产权、企业机密等文档泄漏 2.通过关键字匹配，识别WEB/邮件等外发数据中的敏感信息，并可根据策略实时阻断 3.支持外发操作的记录与审计，及时发现违规外发企业机密信息风险，追溯责任主体。
关键技术	✓web内容控制技术可以对HTTP协议传输的Web页面内容和附件进行控制，按关键字过滤内网用户通过web页面提交的文本内容和大小；通过文件大小和类型控制HTTP、FTP方式外传文件。 ✓邮件外发控制可以对SMTP邮件和Webmail实现邮件发件人、收件人、邮件标题和内容以及邮件附件的控制。

【2】防攻击 Key Message (1/4)

KM1：业界最高威胁防护能力：100+DDoS攻击防御、秒级响应

方案特色1	**提供业界最强防护性能，最大1T攻击防护性能，是业界同类产品的50-100倍** **客户价值：**能够抵御超大规模的DDoS攻击，应对越来越猛烈的攻击态势，保证业务持续 **差异化：**近些年针对大型IDC关键资源的DDOS攻击流量经常超过10G，业界同类产品的Syn-flood（主流攻击）防护能力只有10Gbps，超过此流量的攻击根本无法防御，最终会导致服务瘫痪，华为方案可以提供领先业界100倍的防御能力，保证1-3年内的持续防护效果。
方案特色2	**防护包括CC攻击在内的全部流量型和应用型DoS攻击，并率先支持IPv6环境下的攻击防护，提供业界最全面的攻击防护能力** **客户价值：**全面的攻击防护种类，可以有效保护客户网络，不会因为应用型、流量型攻击而导致网络故障 **差异化：**现网攻击种类复杂多样，往往一种攻击即可攻瘫用户网络，丰富的攻击防御种类可确保用户免除各种攻击威胁。业界同类非独立DDOS产品，仅能支持Flood类等几十种场景攻击，不具备应用型攻击防御能力
关键技术	✓ 独立专业插板，高性能多核CPU，单板160G DDoS防护能力，整机6倍扩展，接口板分流技术保证线性业务扩展 ✓ 七层过滤、行为分析、会话监控，信誉分析技术以及全流量检测机制和全球2万G的流量样本采集能力，保证攻击识别更全面。

【2】防攻击 Key Message (2/4)

KM2:高质量安全：99%病毒检出率，0 IPS误报，为客户网络提供最强防御能力

方案特色3	**威胁检测准：99%病毒检出率、0 IPS误报，威胁更新<4小时，提供业界最强防御能力** **客户价值：**不放过任何蠕虫、木马、病毒、应用层攻击等网络威胁、不阻挡任何正常的企业应用，具有检测、防御最新威胁的能力，保障客户网络的持续运行； **差异化：**业内同类产品病毒检测率在80%左右，IPS误报在30%；华为采用赛门铁克先进的反病毒、入侵检测技术，AV检出率高达99%，0 IPS 误报
方案特色4	**一键式配置：IPS/AV即开即用，及时保护网络** **客户价值：**全面的攻击防护种类，可以有效保护客户网络，不会因为应用型、流量型攻击而导致网络故障 **差异化：**现网攻击种类复杂多样，往往一种攻击即可攻瘫用户网络，丰富的攻击防御种类可确保用户免除各种攻击威胁。业界同类非独立DDOS产品，仅能支持Flood类等几十种场景攻击，不具备应用型攻击防御能力
关键技术	✓ 基于漏洞的IPS检测技术，无论攻击行为如何变化，均可精确检测和阻断，同时减少了签名库的数量，提升了检出率、提高性能； ✓ 采用文件级内容扫描的AV引擎，结合全球领先的静态启发式检测技术，提供高达99%的精准检出率 ✓ 10多年企业网服务经验，多种行业的策略模板，即开即用

【2】防攻击 Key Message (3/4)

KM3:完备的移动办公整体安全防护：多达10种认证方式，安全防护更完备

方案特色5	**支持本地口令、AD/LDAP、Radius、证书、令牌、USB Key、短信、终端标识码、图形码、移动Ukey认证方式和认证组合，用户可以自由选择使用，确保了身份认证更加安全** **客户价值**：多种认证方式适应用户各种差异环境，用户可自由选择使用，确保了身份认证更加安全。 **差异化**： 华为支持10种认证方式并可多认证组合，这方便客户按需进行认证选择；而业界同类产品仅支持6-8种认证方式，有的还不支持认证组合，这些不足使其无法适应企业的各种复杂认证需求。
方案特色6	**构建包括终端安全、接入安全、传输安全、网关安全、内部安全的整体安全防护，用户远程接入安全无忧** **客户价值**：全面的攻击防护种类，可以有效保护客户网络，不会因为应用型、流量型攻击而导致网络故障 **差异化**：现网攻击种类复杂多样，往往一种攻击即可攻瘫用户网络，丰富的攻击防御种类可确保用户免除各种攻击威胁。业界同类非独立DDOS产品，仅能支持Flood类等几十种场景攻击，不具备应用型攻击防御能力
关键技术	✓ 安全数传对CIFS/NFS文件共享和网络扩展都支持，并提供基于关键字的文件内容控制，同时采用加密传输。 ✓ 终端安全浏览器基于移动安全沙箱，个人与企业数据安全隔离禁止数据相互拷贝。在下载文件时，系统会对产生的临时文件自动加密，应用关闭时会清除记录，达到访问零痕迹，防止隐私数据泄漏。 ✓ 安全pushmail提供了邮件终端安全管控，防止公司邮件被非法访问，用户可在移动终端上安全阅读，并根据角色不同设置不同权限，如可设定只允许看邮件标题，或者只允许在线读邮件但是不能保存。

【2】防攻击 Key Message (4/4)

KM4:国际领先的入侵检测精度

方案特色7	**精准的入侵特征识别库，高达80%的默认签名开启率** **客户价值**：全面的防护用户系统，避免客户遭受针对应用层漏洞的攻击手段； **差异化**：NIP产品提供的应用层防护功能，改变了当前业界IPS系统偏重于网络层攻击、忽视应用层攻击的现状。
方案特色8	**2~7层DDoS防护，自动配置阈值，精准防护DDoS攻击** **客户价值**：全面的攻击防护种类，可以有效保护客户网络，不会因为应用型、流量型攻击而导致网络故障 **差异化**：现网攻击种类复杂多样，往往一种攻击即可攻瘫用户网络，丰富的攻击防御种类可确保用户免除各种攻击威胁。业界同类非独立DDOS产品，仅能支持Flood类等几十种场景攻击，不具备应用型攻击防御能力
关键技术	✓ NIP采用了基于漏洞的入侵特征检测技术，该技术大大降低了签名的数量，提高了签名的效率，对未知攻击行为有很好的防护效果。

【3】防IT特权滥用 Key Message(1/2)

KM1：业界最强运维平台满足客户不同运维场景

方案特色1	提供业界最强支持统一C/S和B/S运维平台 **给客户带来的价值：**满足客户不同运维操作习惯，实现对所有IT运维操作的审计，防止误操作或TT特权滥用 **差异化：**提供统一的C/S和B/S运维操作平台，字符运维终端（TELNET、SSH）单点登陆支持所有字符终端属性（VT100，VT102，VT220，LINUX，ANSI，XTERM等），图形终端(RDP/VNC/X11)单点登录支持所有微软远程桌面软件客户端。
关键技术	✓单点登录技术：字符终端（TELNET、SSH）单点登陆和图形终端（RDP、VNC、X11）单点登陆支持目标服务器序号选择和IP输入选择功能，目标服务器IP输入选择功能支持智能提示，自动过滤目标服务器；单点登陆支持用户、目标主机、目标账号、扩展动作等复杂权限关联，根据用户进行权限设置和权限控制。 ✓集中审计技术：多种审计技术包括逻辑命令自动识别技术、跳转登录操作智能审计技术、操作现场全程录像技术等帮助记录发生在重要信息系统中的各种会话和事件。

【3】防IT特权滥用 Key Message(2/2)

KM2：完备syslog输出能力支撑企业集中运维审计

方案特色1	完备syslog输出能力支撑企业集中运维审计，防止IT特权滥用 **给客户带来的价值**： 对IT运维过程进行完全跟踪和记录，对IT运维违规操作进行集中审计，同时确保企业符合法律法规要求的安全策略 **差异化：**支持完备的syslog输出，包括字符终端实时操作命令输出；登录、登出事件syslog输出；违规操作、非法操作、告警日志syslog输出；数据库运维SQL语句识别结果syslog输出等。
关键技术	华为统一运维平台实现对所有运维操作过程的文本记录和视频记录，同时支持细粒度查询，避免恶意运维操作，实现责任定位，确保运维可见可控可查

【4】安全管理 Key Message

KM： 业界领先的日志采集、安全事件智能分析帮助提升安全运营管理效率

方案特色1	全面的设备日志采集，为企业实现集中化的日志管理 **给客户带来的价值**：提供全网设备的日志采集管理，对于非主流设备的日志提供快速定制接入，统一采集管理 **差异化**：支持160多种设备的日志采集和管理，包括各主流的主机系统、数据库、网络设备、安全设备和存储设备等，对于非主流设备的日志提供快速定制接入，实现日志的集管理。
方案特色2	领先的事件采集性能，实现海量数据的收集和分析 **给客户带来的价值**：帮助客户实现海量日志数据的即时高效的收集和分析 **差异化**：采用采用独有的并行方式对日志数据同时进行收集和分析；在相同的系统性能下，其效率优于传统的关系型数据库，真正实现海量数据的即时高效收集和分析.
方案特色3	强大的关联分析引擎，及时预警安全风险，并帮助客户快速定位IT安全事件 **给客户带来的价值**：对安全事件进行智能分析并及时预警，降低企业安全风险 **差异化**：强大的关联分析引擎，能够跨设备、跨类型对多条事件进行关联分析；内置了230条关联规则，可对常见的安全威胁进行识别和告警；华为还可根据用户实际环境，提供现场定制客户化的关联规则，满足客户特定场景的安全需求。
关键技术	✓安全强大的关联分析引擎，能够跨设备、跨类型对多条事件进行关联分析 ✓采用专用的日志加密技术进行加密存储，且有内部时间戳防篡改标志，以确保一旦数据被写入数据库就无法被改变

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY