业务安全无忧
网络卓越高效

——华为数据中心网络安全与
应用优化解决方案

华为技术有限公司

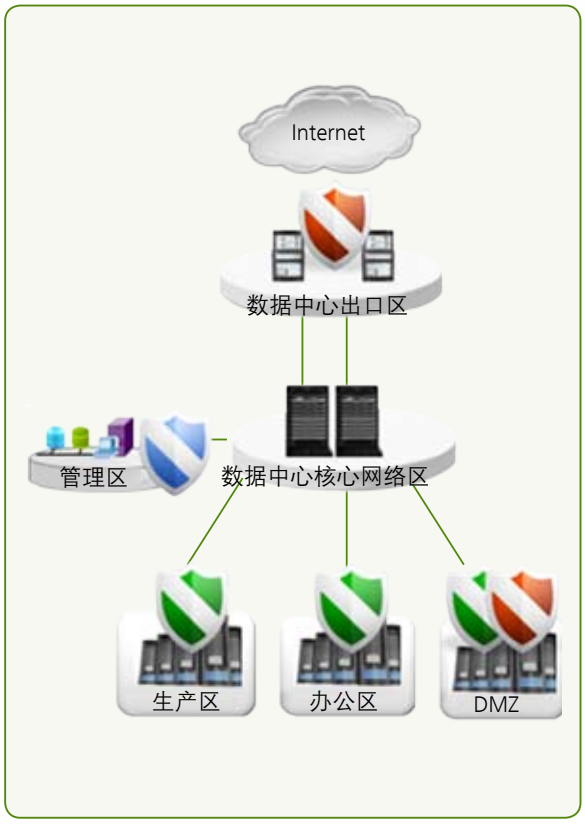
HUAWEI

数据中心承载着用户的核心业务和机密数据，同时为内部、外部以及合作伙伴等客户提供业务交互和数据交换。作为业务应用核心和敏感数据的汇集点，数据中心永远是攻击者最感兴趣的目标。以下问题一直困扰用户的数据中心建设：针对服务器的拒绝攻击如何抵御？层出不穷的入侵如何防范？高压力时服务器的响应速度如何提高？持续不间断业务如何保证？

作为全球领先的网络解决方案供应商，华为长期致力于数据中心网络安全与应用优化解决方案的研究和开发，为用户提供高性能、一体化、层次化安全部署和端到端的应用优化解决方案，打造“安全无忧，卓越高效”的数据中心。

华为数据中心网络安全解决方案

—— 高性能安全，层次化安全，一体化安全



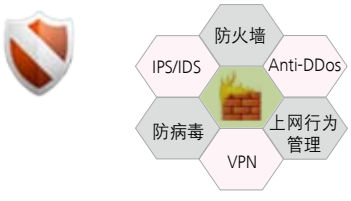
高性能安全产品

- 业界领先处理能力：200Gbps吞吐量，80,000,000并发连接，5,000,000/秒新建连接数
- 最高VPN性能及容量：320,000并发IPSec隧道，120Gbps加密解密性能，VPN双机热备
- 最可靠性：双机热备，双主控，业务板均衡与热备，部件热插拔，交换网与电源冗余

分区域层次化安全策略部署

- L2-L7层次化深度防护
- 边界控制与入侵防御
- 内部区域隔离
- 管理区安全与事件管理与审计

统一的网络级别业务级安全



高性能安全

- IPS技术：高达80G吞吐量；IPS指纹库全球最大、IPS指纹库增新最快、升级服务器范围最广；支持HTTP, SMTP, POP3, IMAP, FTP, DNS, P2P/IM等多种协议
- 业界领先的处理性能：万兆线速转发，高达200Gbps吞吐量的业界最高性能，轻松应对WEB2.0带来的流量挑战；并发连接跨越千万门槛，最高可达8000万，通过多核技术实现连接数与整体性能的协调，真正支撑WEB2.0应用；500万/秒新建连接数，从容应对上网峰值和DDoS等突发网络时间，保障网络的可用性。
- 最高VPN性能及容量：最高提供32万并发IPSec隧道；最高提供120Gbps(DES/3DES)加密解密性能；支持VPN双机热备；支持IKEv2协议，强化了用户认证、报文认证、NAT穿越等功能，消除了中间人攻击和拒绝服务攻击隐患，并且扩展支持EAP-SIM、EAP-AKA等无线鉴定协议，从而更高效地对无线网络提供安全保护。
- 高可靠性：双机热备及BYPASS，双主控多交换，业务板间负载均衡与热备，跨板端口绑定、部件热插拔、关键部件（电源、风扇）冗余等多项高可靠性设计，全面提升设备可靠性。从2008年上市至今，Eudemon 8000E未发生一起网上事故。

安全需求	设备类型	部署位置	解决主要问题	型号
安全保障	防火墙	数据中心安全域边界	网络安全域划分，隔离与问控制	Eudemon 1000E-X
		数据中心接入边界	接入网侧的准入控制和安全风险防御	Eudemon 8000E-X
	IPS&IDS	数据中心安全域边界	应用层攻击防御	Eudemon 1000E-X
		数据中心外联		NIP 1000
		Internet出口		Eudemon 8000E-X
	DDOS流量清洗网关	Internet出口	泛洪型和应用型DDOS攻击防御	Eudemon 1000E-I&D
管理维护	网络安全管理中心	数据中心管理区	安全设备管理，安全日志收集，过滤，分析.风险呈现，安全事件紧急报警，事前预警， 事后分析	iSoc
	统一运维审计	数据中心管理区	实现IT系统统一管控，满足法规审计要求	UMA

层次化安全

针对Internet等具有安全威胁的外部流量，部署Anti-DDoS系统进行恶意流量清洗，部署防火墙进行边界访问控制；数据中心内部则按照不同业务划分安全区域，在各区域之间部署安全隔离和访问权限控制，不同安全区域部署不同的安全策略，在关键业务服务前部署IPS设备，或者激活防火墙内置的IPS模块；在管理区，对管理用户进行统一的安全身份认证，并对操作过程做记录审计，同时针对网络设备、安全设备、操作系统、数据库等系统的安全日志，进行安全事件的关联分析，形成事前预警，事后审计的内控体系。

1、Intranet接入区

安全风险主要是非法业务访问，采用防火墙双机备份、直路部署的方案，通过防火墙策略保证内网用户与数据中心区域交互的高安全性。

2、WAN接入区

安全风险及部署同Intranet接入区。

3、Internet接入区

主要有DDoS流量攻击、来自Internet的非法业务访问等安全风险和内部IP地址暴露、VPN安全接入、互联等安全需求。在出口部署独立的Anti-DDoS系统，清洗异常攻击流量，防火墙直路部署，控制外网访问内网的流量，同时提供NAT地址转换功能，交换机旁挂SSL VPN设备，满足远程用户安全接入需求。Anti-DDoS和防火墙策略能够保证数据中心区域安全性，同时防火墙、SSL VPN设备双机备份保证方案的高可靠性。

4、合作伙伴接入区

安全风险主要是非法业务的访问，安全需求主要是VPN安全接入。采用防火墙设备双层直路部署方案，避免流量迂回，提高转发效率，可靠性安全性都得到有效保障。外层防火墙隔离合作伙伴到前置机的非法访问流量，同时具备VPN功能，实现合作伙伴的安全VPN接入需求；内层防火墙隔离前置机到内部业务服务区间的非法访问流量。

5、数据中心服务区

安全风险主要是非法业务访问和黑客攻击行为，采用防火墙旁路部署，按需引入流量进行策略控制，可信流量直接通过交换机转发；核心服务器上游部署独立的IPS设备或者激活防火墙内置IPS模块，进行应用层攻击防御，通过防火墙策略保证不同服务器区合法互访、IPS保障服务器免受黑客攻击。防火墙、 IPS均采用双机备份方式证方案的高可靠性。

6、网管维护区

网管维护区的安全风险及管理要求有：

- 安全设备管理问题、安全故障快速处理
- 共享账号、非法访问、恶意操作
- 信息安全事件孤岛、海量安全日志、安全趋势分析不全面

部署方案为：

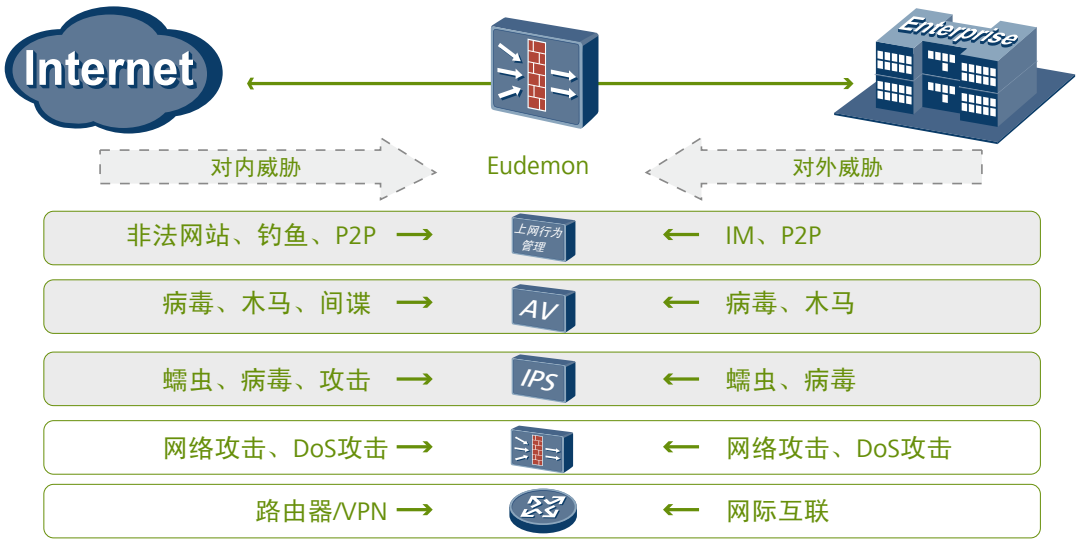
- 防火墙设备直路部署，仅允许堡垒主机、网管及iSoC系统与区域外部的互访
- 部署安全设备管理系统，对安全设备和配置进行统一的管理
- 通过部署堡垒主机，提供运维唯一入口
- 部署iSoC安全运营中心，提供全面的安全态势分析

安全设备管理系统，管理所有的安全产品，更加细致地实现安全策略和VPN业务，协助管理员定位安全设备故障；堡垒主机实现统一运维入口，集中帐号管理，实现单点登录，严格控制帐号权限；通过iSoC及堡垒主机系统的事前安全告警、事中安全运维、事后追踪审计输出数据中心全面准确的安全态势报告。

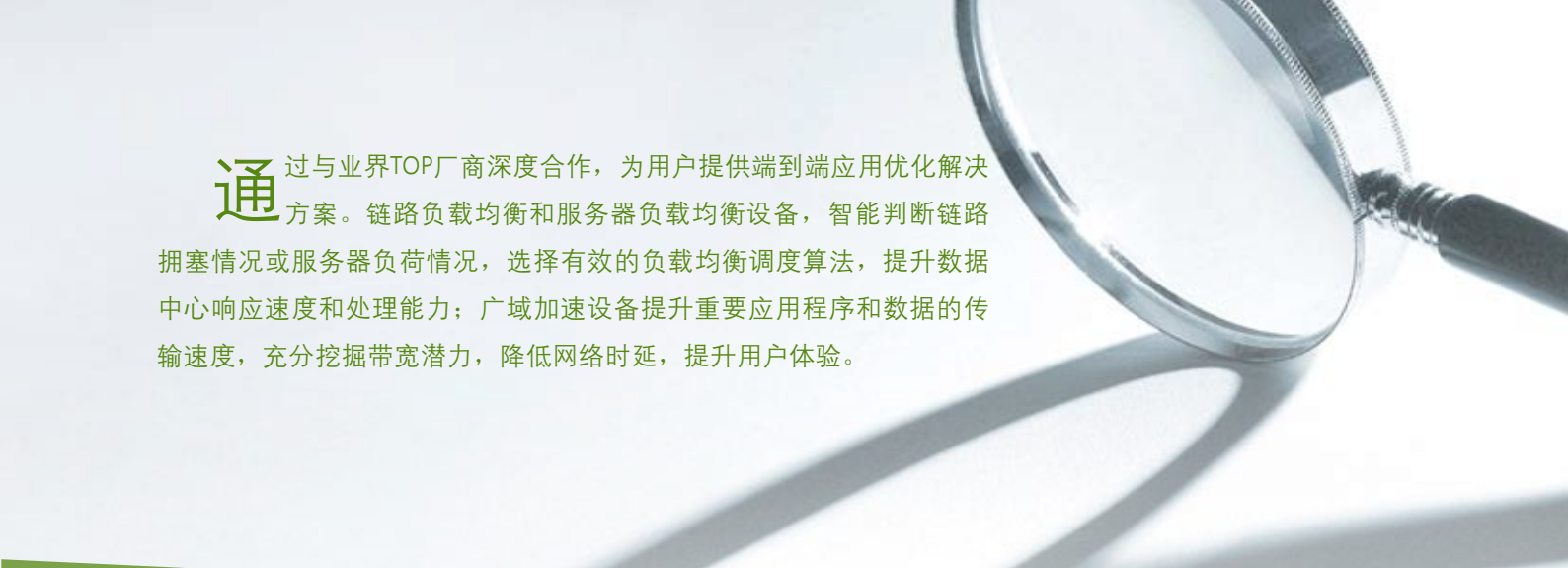
安全区域	存在问题及风险	风险级别	部署建议	部署价值
Intranet	非法业务访问	中-	部署防火墙	解决内网用户非法访问问题
WAN接入区域	非法业务访问	中-	部署防火墙	解决分支接入非法访问问题
Internet接入区	DDoS流量攻击/非法业务访问/NAT地址转换/VPN安全接入	高	部署防火墙、Anti-DDoS、SSL VPN设备	解决DDOS攻击、业务非法访问、远程用户安全接入问题
合作伙伴接入区	VPN安全接入/非法业务访问	中	双层部署防火墙	解决业务非法访问问题、合作伙伴的VPN安全接入问题
业务服务区	非法业务访问/黑客攻击行为	中+	部署防火墙、IPS设备	解决业务非法访问、黑客攻击问题
网管维护区	非法业务访问/缺乏安全事件管理/缺乏安全设备管理/缺乏安全运维审计	低	部署防火墙、iSoC系统、安全设备管理系统、堡垒主机	解决业务非法访问、安全事件关联、安全设备管理与运维审计问题

一体化安全

华为Eudemon系列防火墙设备可提供多种安全技术，集防火墙、IPS/IDS、防病毒、安全VPN、Anti-DDos、上网行为管理于一体，为数据中心提供全面保护。集成化设备降低客户设备投资，简化网络维护和管理。



在数据中心出口处以及需要部署边界控制与入侵防御的区域，部署集一体化的安全防御设备，实现包括边界防护（Anti-DDos、VPN网关）、深度防御（防火墙、IPS入侵防御网关）和统一安全管理等功能在内的全面安全防护，抵御来自L2~L7全方位的安全威胁。



通过与业界TOP厂商深度合作，为用户提供端到端应用优化解决方案。链路负载均衡和服务器负载均衡设备，智能判断链路拥塞情况或服务器负荷情况，选择有效的负载均衡调度算法，提升数据中心响应速度和处理能力；广域加速设备提升重要应用程序和数据的传输速度，充分挖掘带宽潜力，降低网络时延，提升用户体验。

华为数据中心网络应用优化解决方案

—— 端到端优化

负载均衡

- 数据中心多出口接入不同运营商，使用链路负载分担技术，实现内网访问公网的流量智能分析目的地运营商，选择对应运营商出口负载均衡。
- 服务器负载分担技术有效降低单台服务器的性能压力，降低服务器硬件升级成本，并且提高业务可靠性，单台服务器故障不会导致业务瘫痪。
- 多数据中心网络环境下，通过全局负载分担技术，使用户总能快速访问“距离最近”的数据中心业务，有效解决网络拥塞问题，提高服务器响应速度，服务就近提供，达到更好的访问质量。

广域优化

广域网带宽远小于局域网，且费用高，同时广域网延迟大、丢包多，应用系统访问慢，使得分支机构不得不增加本地的服务器部署；异地的主备数据中心之间同样面对带宽小、费用高和时延大的问题。针对广域网的上述问题，已经有很多成熟的技术手段来优化解决，使广域网的应用体验得到了极大提升。

- 带宽不足：通过数据压缩、缓存和消除重复数据的方式，减少在广域网上传输的数据量；
- 延迟大：通过协议优化（加速TCP、HTTP、CIFS、NFS等）、预先请求、代理应答等技术手段解决。
- 丢包：通过拥塞控制、FEC（Forward Error Correction）、报文重排序等技术解决。

华为技术有限公司
深圳市龙岗区坂田华为基地
邮编：518129
电话：+86 755 28780808

www.huawei.com