深圳市智博通电子有限公司

网络安全等级保护2.0

智博通路由解决方案

共同打造智能、安全、高效的未来网络服务平台

2020/7/7

bī zbī zbī zbī zbī zbī	zbī zbī zbī zbī zbī zbī
de zbr zbr zbr zbr zbr	
三 表	◆ 等级保护制度发展介绍b
CONTENTS	◆ 等级保护制度2.0的变化
CONTENTS	◆ 等级保护2.0解决方案
	◆ 部分产品模块介绍
	zb7 zb7 zb7 zb7 zb7 zb7 zb7

网络安全法等级保护发展历程



bī zbī zbī zbī zbī zbī zbī	zbī zbī zbī zbī zbī zbī zbī
bt zbt zbt zbt zbt zbt	
目录	◆ 等级保护制度发展介绍
CONTENTS	◆ 等级保护制度2.0的变化
CONTENTS	◆ 等级保护2.0解决方案
	◆ 部分产品模块介绍

等保2.0相对等保1.0的升级

强制执行力度加大

确立法律地位, 法律责任实质化

安全保护措施强化

- 技术措施趋向主动、动态;
- 测评尺度更为精准、严格

等级 力度 措施 对象 动作

工作内容要求细化

- 五个规定动作+三同步;
- 增加监测预警、应急处置等要求

保护能力等级提升

- 第三级对象 (重要网络) 范围扩大;
- 安全保护能力提升

保护对象范围扩大

- 更多网络运营者被纳入等保监管;
- 覆盖云、移、物、工、大等新场景

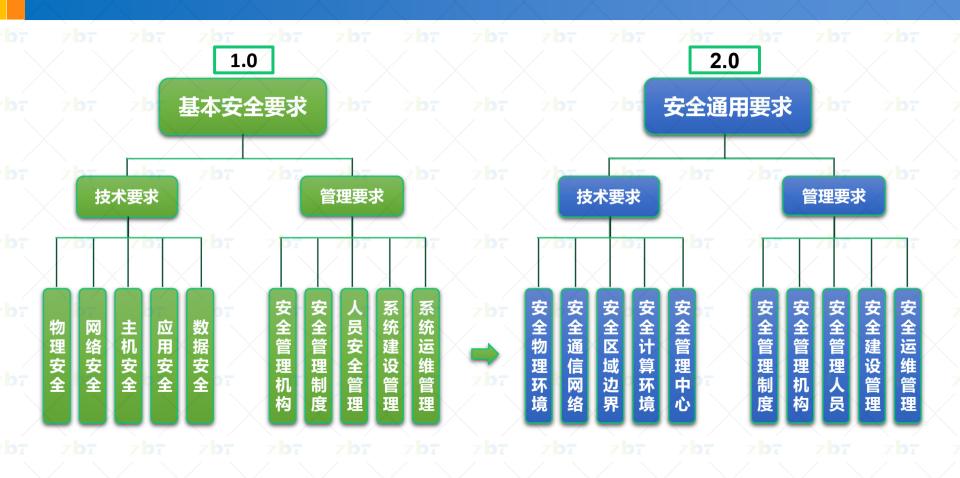
b7 zb7 zb7 zb7 zb

强制执行力度加大

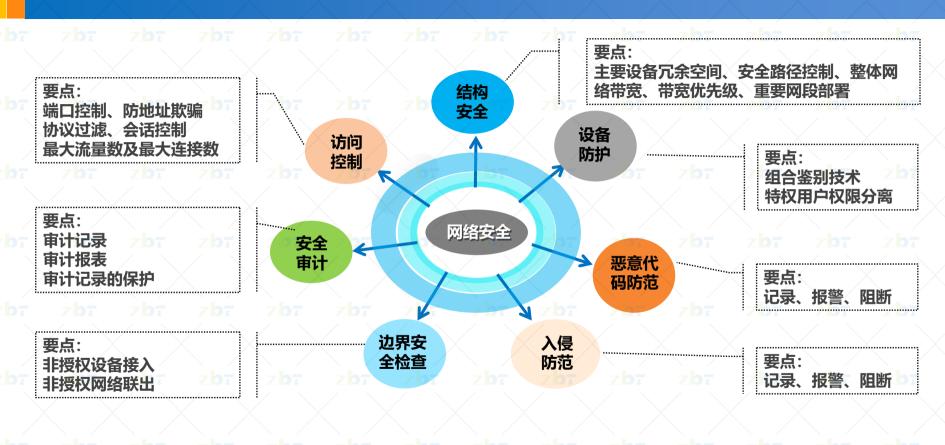
我国山西、广东、上海、四川、重庆、安徽、黑龙江、湖南等地已经出现了网络安全等级保护相关案例,涵盖教育、互联网、医疗、公共服务等领域。被处罚对象发生了未定级备案、未按期进行等级测评、未按规定留存网络日志、未采取防范网络威胁的技术措施、未采取数据保护措施等违法行为。

序号	时间	处罚	行为	,	处罚对象	处罚]措施	执法机关	处	罚依据			
1,	2017.6	未采取防剂 网络攻击、 害网络安全	6	2017.8.30	未按照网络安全制度的要求落实 主体责任,存在	实网络?	安全 业技	滨方正县农 术推广中心 的"方正农	令整改,并	型龙江省哈尔 市公安局网	((XXI ZX, ++	※ 第 21 条、第	zb7 zb
		施。存在 S 严重威胁网			漏洞并被黑客珍造成严重后果	10	2017.12.13	未落实网络安全 制度。附属医防		湖南省长沙医学	警告、责令改正	湖南省长沙市、县 (区)两级公安网	《网络安全法》第21条、第
2	2017.7.20	三级以上到期开展网络			未建立网络安全 措施、网络日志		2017.12.13	系统存在任意文 隐患漏洞情况	件上传等	院	青山、贝文以正	安部门	59 条第 1 款
) L		791717181-1-1	7	2017.9.28	六个月,未采耳重要数据备份		/ 10	未落实网络安全		湖南中科智谷教	约谈法人代表及 网站系统管理	湖南省株洲市、区	《网络安全法》第21条、第
3	2017.7.22	未进行定约 评。存在高			施,致使系统名生身份信息泄露	11	2018.3.26	5 制度,未履行网络安全保护义务		育科技有限公司	员; 警告、责令改正	公安网安部门	25 条、第 59 条第 1 款
οź	7	站发生被黑	b		未落实网络安	07	7 k	未采取防范计算	机病毒和	b7 7	对封丘县图书馆	HCHARD H	7 b 7 7 b
4	2017.8.1	未依法留 ⁷ 网络日志	8	2017.10.17	任,网站被入侵 病毒	12	2018.1.12	网络攻击、网络 害网络安全行为	F侵入等危 的技术措	河南省新乡市封 丘县图书馆网站	给予罚款 20000 元、对直接责任 人处以警告,并	封丘县公安局、封 丘县文化广电旅 游局	《网络安全法》第 21 条、第 59 条第 1 款
5	2017.8.12	未进行网约定级备案、	9	2017.12.12	未进行网络安全 的定级备案、等 工作,未落实际 级保护制度,对 安全保护义务	等级测i 网络安全	全等 浏阳	施,致使网站遭 市烟花爆竹 网站系统 警	告、责令	长沙市公安月技支队、浏阳市	罚款 5000 元 局网 第 21 条、第 2 名 安 三 数 律 研	25条、第59条	zbī zb
/						的主管 5000 元	100000000000000000000000000000000000000				h= - h		

安全控制措施分类结构的变化



等级保护安全解读



bī zbī zbī zbī zbī zbī	zbī zbī zbī zbī zbī zbī zbī
b7	
目录	◆ 等级保护制度发展介绍
CONTENTS	◆ 等级保护制度2.0的变化
b	◆ 等级保护2.0解决方案
DT 7DT 7	◆ 部分产品模块介绍

等级保护防护框架

建设"一个中心"管理、"三重防护"体系,分别对计算环境、区域边界、通信网络体系进行管理,实施多层隔离和保护,以防止某薄弱环节影响整

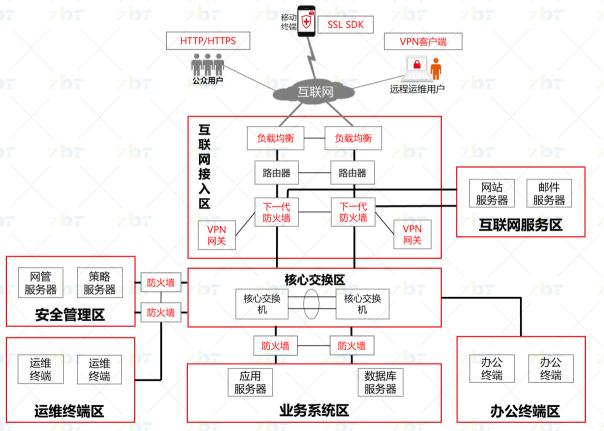
重点对操作人员使用的终端、业务服务器等<mark>计算节点进行安全防护,控制</mark>操作人员行为,使其不能违规操作,从而把住攻击发起的源头,防止发生攻击行为

分析应用系统的流程,确定用户(主体)和访问的文件(客体)的级别(标记),以此来制定访问控制安全策略,由操作系统、安全网关等机制自动执行,从而支撑应用安全

一个中心、三重防护



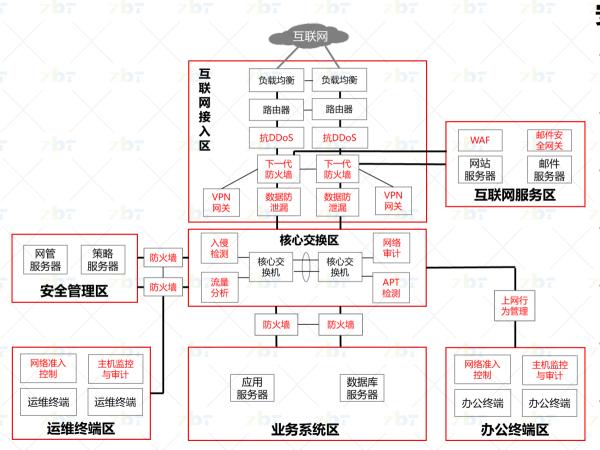
安全通信网络



安全通信网络建设要点

- 路由器、交换机、防火墙等网络 设备的业务处理能力满足业务高 峰期需要;
- 网络带宽满足业务高峰期需要;
- 提供通信线路、关键网络设备和 关键计算设备的硬件冗余,保证 系统的可用性;
- 重要网络区域与其他网络区域之间采取可靠的技术隔离手段;
- 采用密码技术保证通信过程中数据的保密性及完整性。

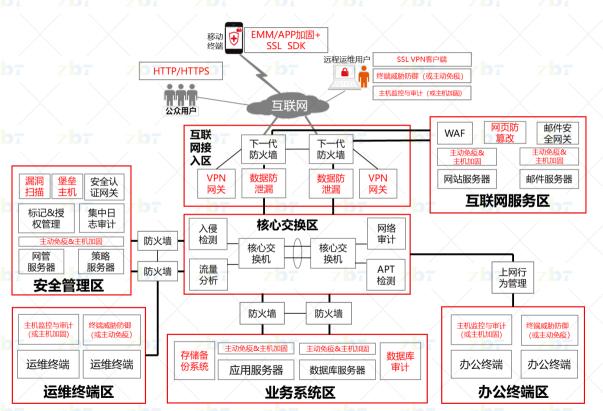
安全区域边界



安全区域边界建设要点

- 对非授权设备私自联到内部网络的行为 讲行控制;
- 对内部用户<mark>非授权联到外部网络</mark>的行为 进行控制;
- 对进出网络的数据流实现基于应用协议 和应用内容的访问控制;
- 在关键网络节点处检测和/或防御从外部/内部发起的网络攻击行为;
- 对网络攻击特别是新型网络攻击行为进行检测分析,事件告警;
- 对垃圾邮件进行检测和防护,并及时升级和更新;
- 对用户的远程访问行为、互联网访问行为等进行审计和数据分析。

安全计算环境



安全计算环境建设要点

- 采用口令或生物技术结合密码技术对用户进行身份鉴别;
- 采用基于角色/属性或安全标记的访问控制 技术对操作系统、数据库、应用用户进行权 限管理;
- 对重要的用户行为和重要安全事件进行集中 审计;
- 采用漏洞检测、终端管理结合补丁管理、终端威胁防御、主动免疫可信验证、主机加固等技术保障终端及服务器等计算资源的安全;
- 采用<mark>密码技术、容灾备份</mark>技术等保障重要数 据的完整性、保密性、可用性;
- 网页防篡改;
- 敏感数据和个人信息保护。

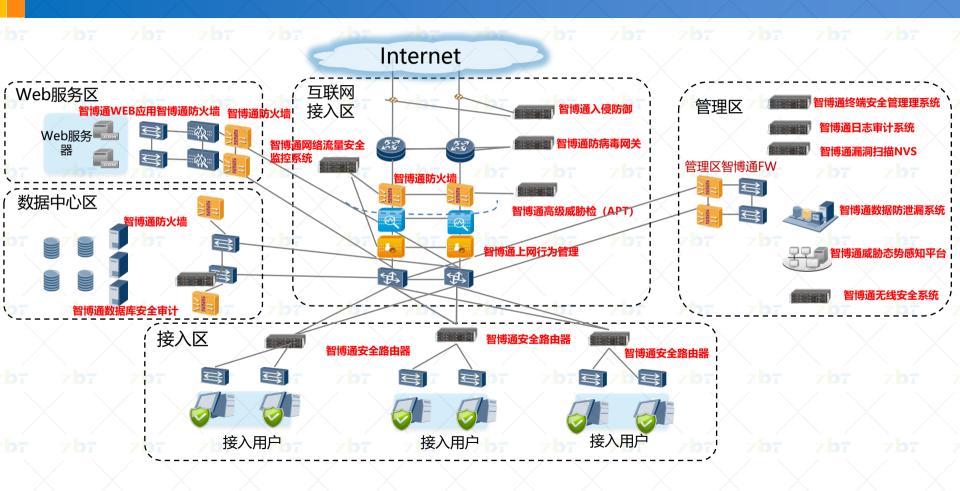
安全管理中心



安全管理中心建设要点

- 划分不同管理角色,并提供集中的身份鉴别、访问授权和操作审计;
- 对网络和信息基础设施的运行状况进行集中监控;
- 对分散在网络中的审计数据进行收集汇总和集中分析;
- 对安全策略、恶意代码、补丁升级等进行集中管理;
- 部署态势感知和安全运营平台,支撑安全监测、分析、预警、响应、处置、追溯等安全管理和运维工作。

整体解决方案



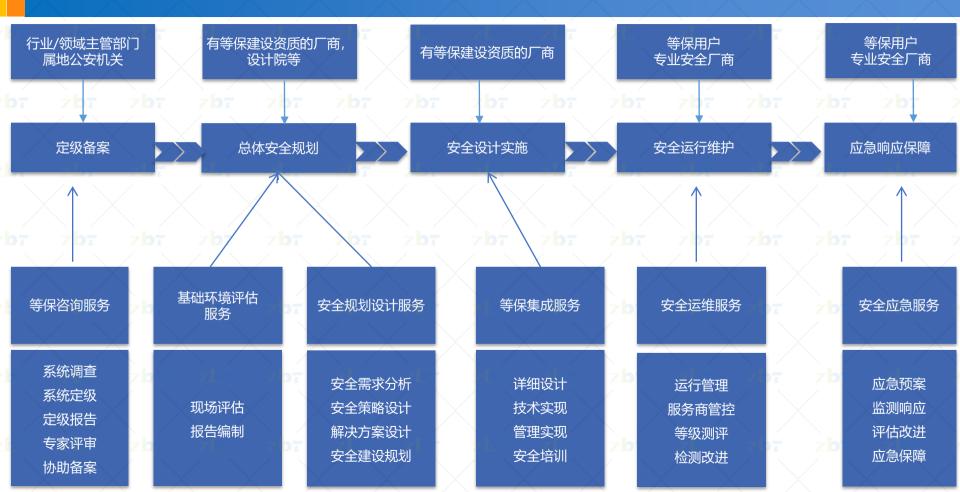
二级/三级等保(基础版)套餐设计

二级等保 (基础版) 套額	
智博通防火墙/智能网关	必选
智博通入侵防御IPS	必选
智博通日志收集与审计分析系统	必选
智博通网络流量安全监控系统	必选
智博通终端安全管理系统	必选
智博通上网行为管理UBA	可选
bo 综合评分 bo	75+ z

三级等保 (基础版) 套餐	Z OI
智博通防火墙	必选
智博通安全路由器	必选
智博通日志收集与审计分析系统	必选
智博通网络流量安全监控系统	必选
智博通终端安全管理系统	必选
堡垒机	必选
智博通漏洞扫描NVS	必选
智博通上网行为管理UBA	必选
智博通WEB应用智博通防火墙	可选
智博通数据防泄漏	可选
综合评分	80+

三级等保 (增强版) 套餐设计

bī zbī z	bī zbī zbī zbī	须垒 伊	(增强版) 套餐	b
	智博通防火墙/智能网关	必选	智博通主机入侵防御HIPS可选	
	智博通入侵防御IPS	必选	智博通数据防泄漏可选	
	智博通DDoS防护系统	必选	IAM身份鉴别平台 可选	
	智博通上网行为管理UBA	必选	智博通网络空间资产治理系统可选	
	智博通APT	必选		
	智博通日志收集与审计分析系统	必选		
	智博通网络流量安全监控系统	必选		
	智博通漏洞扫描NVS	必选		
	智博通终端安全管理系统	必选		
	智博通威胁态势感知平台	必选		
	智博通WEB应用防火墙	必选		
	运维堡垒机	必选		
	网络准入控制系统	必选		
	综合评分		85+	



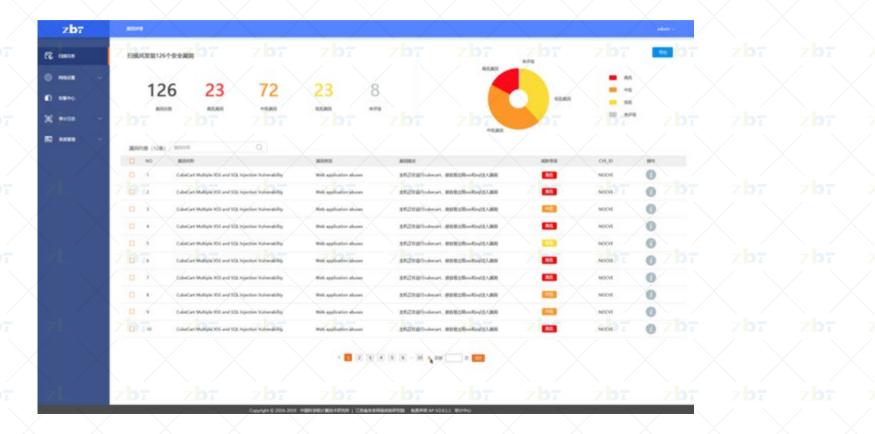
b7 zb7 zb7 zb7 zb7 zb7	zbī zbī zbī zbī zbī zbī zbī
bt zbt zbt zbt zbt zbt	
目表	◆ 等级保护制度发展介绍 pb7 pb7 pb7
CONTENTS	◆ 等级保护制度2.0的变化
CONTLINIS	◆ 等级保护2.0解决方案
	◆ 部分产品模块介绍

1、智博通入侵防御/检测 (IPS/IDS)

- · 记录并保存拦截到的入侵事件, 对异常流量进行监测并告警,
- 仅限于指定的授权用户访问事件数据,禁止其他用户对事件数据的操作。
- 覆盖35个大类5W+种攻击行为,用于区域边界与计算环境的入侵防御、智博通入侵防御。



• 拥有漏洞扫描知识库包含5W+的漏洞规则, 10W+CVE漏洞记录, 用于内网资产安全管理。



支持文件还原和病毒检测,病毒库规模800W+,用于恶意代码防护与清除,桌面病毒防范。



筛选	TA -										用时0.148	8秒,约566条证	录
Nº	还原时间	源地址	目的地址	源第口	目的端口	协议	应用层协 议	告營类型	文件名		大小	同凝告警数	详情
1	2018-11-30 15:44:13	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	8
2	2018-11-30 15:44:12	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	目
3	2018-11-30 15:33:19	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	
4	2018-11-30 15:33:18	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	
5	2018-11-30 15:22:25	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	日
6	2018-11-30 15:22:24	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	
7	2018-11-30 15:11:31	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	艮
8	2018-11-30 15:11:30	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	目
9	2018-11-30 15:00:37	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	8
10	2018-11-30 15:00:36	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	
11	2018-11-30 14:49:43	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	
12	2018-11-30 14:49:42	153.3.235.83	192.168.88.30	80	51995	TCP	http	可疑文件	rsPass.dll		132K	1634	



4、智博通日志收集与审计分析系统

支持WEB、流媒体、语音、邮件、文件等业务系统操作记录分析与事件审计。

1 2019-09-27 20:36:11 2 2019-09-27 20:08:33	license@cnsun huangbiyuan@	wenjigang@cnsunet.com zhouli@cnsunet.com		192.168.2.206 192.168.3.53	113.96.232.106 113.96.200.115	0		key生成,来自1 : 整理收集的我(
2 记录时间	发件人	收件人	登入状态	源地址	目的地址	附件总个数	邮件标	<u>.</u>		
								已生成	成 SMTP 业务列表,共	2条记录 统计
		搜索邮件标题或附件标题			Q					
凍車传於trn据文个数· ()	最大数据段长度mcc· 1460	window scale: 7	海 动窗门最大 值·14600		test protect	4774.24		151/		
次握手建立时间:	流持续时间: 36毫秒407微秒	是否支持sack: 支持	超时引起的tcp重传报文个数:		test_protocol	175秒前	127 室砂	2.5K	TCP Q	
					adns	175秒前	1章秒	154	UDPQ	
文大小占比: 55.22 %	rtt最大值: 36章秒407微秒	rtt最小值: 36室秒407微秒	平均rtt延时: 36 字秒 40 7 微秒		ans and	175秒前	1章秒	154	UDPQ	7
- 误包个数所占比: 0.00 %	错误包大小所占比: 0.00 %	拥塞率: 0.00 %	报文数占比: 50.00 %		adns adns	175秒前 175秒前	1 室砂	178 178	UDP Q UDP Q	
误报文大小: 0 Byte	rst报文所占比: 0.00 %	重传包个数所占比: 0.00 %	重传包大小所占比: 0.00 %		<u>adns</u>	175秒前	1 室砂	158	UDP Q	
p报文总大小: 74 Bytes	payload报文大小: 0 Byte	重传报文大小: 0 Byte	乱序报文大小: 0 Byte		<u>a</u> dns	175秒前	1 室砂	142	<u>UDP</u> Q	
传:0	乱宗:0	错误 0	sack: 0		₩ General_UDP	175秒前	25 室秒	218	UDP Q	ZB
n: 1	fin: 0	纯ack: 0	payload: 0		a dns −	175秒前	1 室秒	168	UDPQ	-
rg: 0	ack: 0	psh: 0	rst: 0		test protocol	175秒前	98 章秒	415	TCP Q	
的端口: 22080	tcp: 1	cwr: 0	ece: 0		Ontp	174秒前 175秒前	1 室砂 1 室砂	90	UDPQ	
					adns adns	174秒前	1 毫秒	142 158	UDP Q UDP Q	
录时间: 2020-02-29 14:54:45	源地址: 192.168.2.248	源端口: 58387	目的地址: 114.115.239.9		General_UDP	174秒前	25 室秒	207	UDPQ	ZK
S S2C					≥ dns	174秒前	1 室秒	168	UDP Q	
					snmp	174秒前	7 章秒	1.7K	UDP Q	
v.cnsunet.com:30443/w	eb/trafficView/userPkg/getT	ransportLayerDetail.action?rowk	ey=0&flowID=679875823	31255146463&n	Q adns adns	174秒前 174秒前	1 室砂 1 室砂	176 176	UDP Q UDP Q	
议详细信息 - Google Chrom	ie			- 0	× snmp	174秒前	46 室秒	12.6K	UDP Q	/
3.	2020-02-29 14:54:45	192.168.2.248 a0:ec:f9:3b:22	c0 34131 114.11		<u>a</u> dns	174秒前	1 室砂	166	UDP Q	7
2.	2020-02-29 14:54:45	192.168.2.248 a0:ec:f9:3b:22	c0 36867 114.11	4.114.114 53	≥ dns	174秒前	1 電秒	150	UDP Q	
1.	2020-02-29 14:54:45	192.168.2.248 a0:ec:f9:3b:22		5.239.9 220		174秒前	37 室秒	134	TCP Q	

5、智博通网络流量安全监控系统

识别主流网络应用2500种以上,支持的资产业务种类大于2300种,用于数据采集分析与异常流量检测。





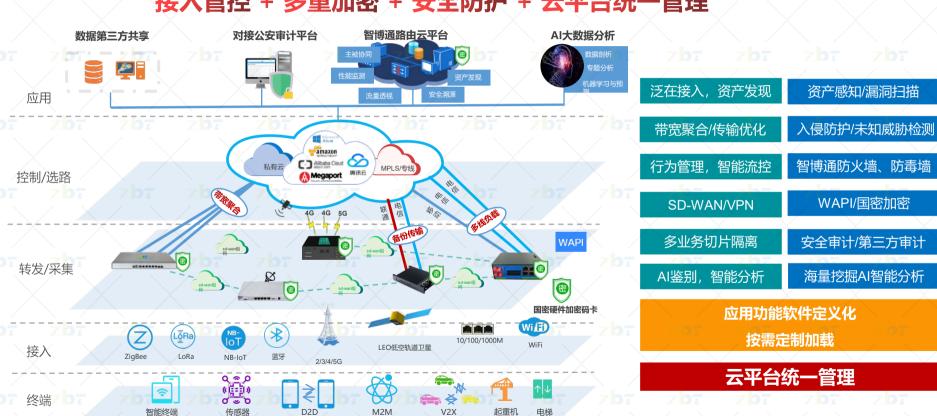




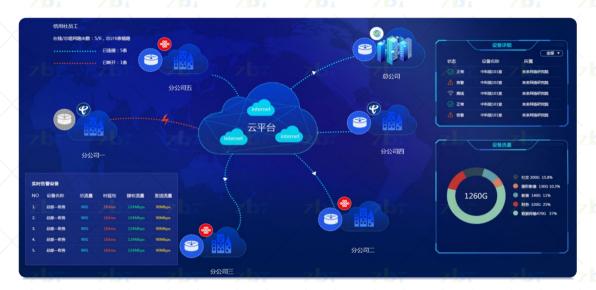


6、智博通安全路由器

接入管控 + 多重加密 + 安全防护 + 云平台统一管理



7、智博通虚拟专用网VPN



- 通过加密通道的方式实现异地间安全 可靠的连接自组网
- 身份鉴别、访问控制、可信验证、日 志审计、数据加密
 - 支持网关/隧道状态监控与告警



通过云平台关联设备即可选择设备组网, 方便快捷, 无需聘请专业IT人员运维。

8、智博通回溯分析系统

支持2-7层全流量保存与在线解码分析,实现数据保存、取证分析。

1		☆ 情輸入你要过	Annual Company of the Company	of management of the second second	过滤	
	(財何: 2020-04-15 09:27:00 源地址: 192.168.4	4.185 目的地址: 220.17	70.181.140 源嶷口: 5630	8 目的端口: 80 协议: TCP		· 李 % 辨选 🖳上传 🛡 信息
).	源地址	目的地址	时长	协议	长度	損要)
1	220.170.181.140	192.168.4.185	0.000000	TCP	66	http > 56308 [SYN, ACK]
2	192.168.4.185	220.170.181.140	0.001523	♥ TCP	\$ 0	56308 > http [ACK] Seq=0.
3	192.168.4.185	220.170.181.140	0.002016	Ö TCP	200	[TCP segment of a reasse
4	220.170.181.140	192.168.4.185	0.011047	O TCP	B0 7	http > 56308 [ACK] Seq=1.
	220.170.181.140	192.168.4.185	0.056149	HTTP	354	HTTP/1.1 200 OK (text/pla.
E	rame 5: 354 bytes on wire (2832 bits), 354 bytes or	aptured (2832 bits)				
8	thernet II, Src: 44:8a:5b:f5:91:da (44:8a:5b:f5:91:d	a), Dst: a0:ec:f9:3b:22:c	0 (a0:ec:f9:3b:22:c0)			
In	ternet Protocol Version 4, Src; 220.170.181.140 (2	20.170.181.140). Dst: 1	92.168.4.185 (192.168.4.	185)		
П	ransmission Control Protocol, Src Port: http (80), D	st Port: 56308 (56308),	Seq: 1, Ack: 146, Len: 30	0 7 0 7	707 707	707 707
Н	ypertext Transfer Protocol	/ / / / / / / / / / / / / / / / / / / /				
Li	ne-based text data: text/plain					
3	220.170.181.140	192.168.4.185	0.056151	ОТСР	6 0	http > 56308 [FIN, ACK] S
	 					
计进	0 ec f9 3b 22 c0 44 8a 5b f5 91 da 08 00 45 00	ASCII编码	_			
	11 54 b6 20 40 00 38 06 33 eb dc aa b5 8c c0 a8	; * . D. [
	4 b9 00 50 db f4 e8 f5 93 11 09 a5 d4 93 50 18		P.			
30 O	0 aa bd e2 00 00 48 54 54 50 2f 31 2e 31 20 32		P/ 1. 1. 2			
	0 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64	00. OK Da				
	te 20 31 35 20 41 70 72 20 32 30 32 30 20 30 31	, . 15. Apr.				
	a 32 36 3a 35 38 20 47 4d 54 0d 0a 43 6f 6e 74	: 26 : 5 8. GM				
	5 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70	ent - Type:				
	c 61 69 6e 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 e 67 74 68 3a 20 38 0d 0a 43 6f 6e 6e 65 63 74	lainCon				
	9 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 53 65 72 76	ion:.clos				
	5 72 3a 20 6e 67 69 6e 78 2f 31 2e 30 2e 31 31	er: . n gi n x				
60 6	0 / Z 38 ZU 08 0 / 09 08 / 0 ZT 31 ZE 3U ZE 31 31					

连接数控制、FTP动态开放端口、DDOS防御及扫描防御、病毒检测等多项功能。



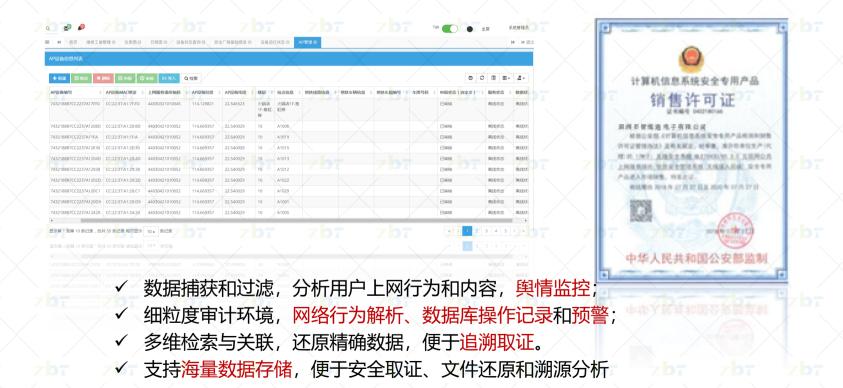
10、智博通上网行为管理UBA

支持身份鉴别、接入认证、安全检测、实名审计、行为管控等多项功能。



11、智博通安全审计平台(综合型)

符合公安部82号令的审计。实现日志采集、储存、分析各系统的人员操作维护信息,及时发现非法、越权操作;同时,可对高危操作实现实时分析、实时监控和阻断。



12、智博通态势感知平台







安全态势



13、智博通综合管理系统

对全网的安全设备、安全事件、安全策略、安全运维进行统一集中的监控、调度、预警和管理。对安全管理员进行身份鉴别,根据权限进行操作及操作审计。



14、智博通工控安全检测系统

- 可对异常工控协议报文进行匹配检测,并定位可其中攻击行为,对安全隐患进行直观的分析。
- 系统内置50000+安全规则库,提供全局数据安全检测分析,包括对工控指令攻击、病毒、木马、攻击参数篡改等攻击行为。





期待与您的合作!