🔎 ADCampus 三期B02宝鸡行政中心全网静态ip地址且终端移动场景配置指导

ADCampus解决方案 **詹继晔** 2020-08-25 发表

组网及说明						
三期B02标准	组网					
配置步骤						
每个业务组样 p网段增加相则 下面以其中一 一、创建一个 网"下即可,让	独配置一个安全组 应个数量的接入场景 个名为"安全组1"的 -二层网络域,名字 这里想创建在vpn-de	, (安全组一、 骨, 然后将这些师 安全组为例进行 为"二层网络域1 sfault下,所以递	安全组二、 並用场景都加 示配置,具体 ",私网这里 轻择vpn-defa	安全组三、安全组内 立用到byod安全组下 不配置步骤如下 3选择这个二层网络如 ault私网。),针对每个 - - 或对应要创建在	安全组的 王哪个"私
名称•	二层网络城1	私	河 *	vpn-default 💌		
VSIMAC *	0000-0000-0001	•				
		DN	SP			
阿关₽ ●	155.0.0.1				400Hpg	
子网捕码*	255.255.255.0	DN	6条目		####	
✓ 員置可法参数 手工設置					_	
ARP核绘则		AF	印代理			
ACIP		19	MP Snooping			
		确定 乡	关闭			

二、增加一个安全组,名字为"安全组1",因为终端都是静态配置ip地址的,所以不用勾选DHCP。

名称 *	安全组1	۲
私网 *	vpn-default	▼ 増加
二层网络城 *	二层网络域1	▼ J增加
VSI接口描述		1
DHCP		
绑定P		

三、增加一个接入组,名字为"接入组1",接入策略绑定到安全组1:

S RESERVE

				×
19. 停改接入第略				
基本信息				-
接入策略名 • 描述	接入组1節略	安全组*	安全组1	▼ Jittiba
接权信息				٠
认证继定信息				۲
用户客户装配置				•
		确定 取消		

8+48				
接入组名 •		1636 ting		
\$P#1192入前M6 *	1000 - 1000 - 1000			
發生单张弓梁大练空终调数*	0	\$P\$雪柳怀马在36数量段刻。	0	
单目繁计在场最长时间(分钟)	0			
() () () () () () () () () () () () () (○元卿和以道の		
10.) 15.00.51 W				
260-4190714				
700 a				
88	接入版相	6.7.5	仰政	50.02
未找到符合很终的记录。				
		82 F.A		

四、接入条件管理à终端ip地址分组中,增加一个基于终端ip的接入场景,名字为"二层网络域1静态ip场景":

9。增加终端IP地址分组		×
增加终端IP地址分组		
终端P地址分组名	二层网络城1静志ip场暴	
起始地址*	155.0.0.1	
终止地址。	155.0.0.254	
	敵定 取消	

五、在接入策略中, 创建一个名字为"二层网络域1静态ip策略", 并且选择"安全组1"

					×
12 增加接入策略					
基本值息					-
接入策略名 • 描述	二层网络城1静志ip 第略	安全组*	安全组1	- addatu	
授权信息					+
认证绑定信息					٠
用户客户装置置					٠
		确定 取消			

六、在byod接入组中,增加一个名字为"二层网络域1接入场景",选择前面创建的接入策略和终端ip地址分组:

· 搬入场展名称 *	二层网络城1接入场最		
接入条件			
揭入位置分组(where,how)*	不限	-	18250
SSID分组(where, how)*	不限	-	18250
终端P地址分组(whose) *	二层网络城1静志ip场最	-	18250
终端MAC地址分组 (whose) *	不限	-	18200
终端厂商分组 (what) *	不限	-	retor
终端操作系统分组 (what) *	不限	-	,#250
终端关型分组 (what) *	不限	-	18200
AP分组(where,how) *	不限	-	1850
接入时段策略(when)*	不限	-	18250
接入策略			
接入策略 *	二层网络城1静志ip 策略		182ba
安全组	安全目1		
单帐号最大绑定终端数*	0		
单帐号在线数量限制*	0		

创建成功后,结果如下:

多·伊孜接入组				
基本信息				-
· 接入结名 •	byod	服务后属		
\$28111 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	byod - style			
\$P\$6996.000+(10)	0	\$289.98% 员不能数量因利。	0	
· 自然计在线最长时间(分钟)*	0			
編述		■ 无償知认证 ⑦		
and.				
接入场最列表				=
natio				
名称	接入策略	优先跟	修改	建纹
二层网络城1接入场景	二层网络城1静态6.策略	± +	B	8
		教室 取消		
型.增加限入用户				
接入信息				
甩 ^向 姓名•	静态用户1 法师 增加用户			
秋号名 *	静 信用/*1 ②			
200 *		- 10m200		
423716		先会时间		
最大河間时长(合体)		在城戰量陸制		1
重录编示信息				
摘入组				
		1015-01		10.0
byod				可由調
11		61		可申请
□ 8		12		可如波
n k		hik		可申請
hxHAM				司申 査
N=				
☑ №2.801				
静念上程度入组				可由通
#248				
#09		无6030		
1+3840.4380:		MCBE		
♥損示				
过意:在文本框中输入多录信息时,每行只能	846人—派信章。			
		8 8章 8 82月17日 第26		激活 Wind 转到 控制调制

七、创建一个账号"静态用户1",并绑定到"接入组1"

八、终端在mac认证中要携带用户ip地址,才能被接入场景ip匹配成功,这就需要在对应leaf下行口配置mac-authentication carry user-ip,如果终端会移动到其它leaf下行口,则其它leaf下行口也要配置: [leaf-GigabitEthernet1/0/1]dis this

#

interface GigabitEthernet1/0/1 port link-mode bridge port link-type trunk port trunk permit vlan all port-isolate enable group 1 qos apply policy zwn inbound qos apply policy zwn outbound mac-based ac dot1x mac-authentication mac-authentication carry user-ip mac-authentication domain h3c port-security free-vlan 1 3503 to 3504 3506 to 3509 3511 to 3515 4094 # 验证结果 1、使用一台静态配置ip地址为155.0.0.15的电脑接入access,在leaf的动态AC可以看到终端进入了对 应的安全组,并且下发了授权url和acl: [leaf-GigabitEthernet1/0/1]dis mac-au con Total connections: 1 Slot ID: 1 User MAC address: 0cda-411d-4be6 Access interface: GigabitEthernet1/0/1 Username: 0cda411d4be6 User access state: Successful Authentication domain: h3c IPv4 address: 155.0.0.15 Initial VLAN: 101 Authorization untagged VLAN: N/A Authorization tagged VLAN: N/A Authorization VSI: vsi3515 Authorization ACL ID: 3001 Authorization user profile: N/A Authorization CAR: N/A Authorization URL: http://110.0.5.93:8080/byod?usermac=%m&userip=%c&userurl=%o Termination action: Default Session timeout period: 86400 s Online from: 2013/01/15 00:21:20 Online duration: 0h 0m 30s 在Director侧查看在线用户也可以看到:

2008/*										
\$360340	0.000									
9.98	Ľ				ML-7488		9*8			
14875	SHITSE ZBOSHED	24FE 24FE 24	R GH H							
	教司名:	登泉器 1	用户结名。	服务名	潜入时间:	增入时任::	記録戸橋16.0	ROPEL :	安全状态。	SPARNIN:
	byodanonymous	0cda411d4be6	byod	byod	2010-03-09 15:27:11	089	110.0.5.4	155.0.0.15	无需安全认证	
共和语	记录,1100年1-1,161/1元。									e (

2、终端随意打开1.1.1.1网站,成功跳转到认证页面,输入"静态用户1"的用户名密码后上线成功: 在leaf上也可以看到认证上线了:

欢迎登录BYOD解决力 HBC Itol94478444 HBC Intelligent Managemen	5案 It Center
BYOO解决方面为用户提供一种输入网络的方式。这种方式为每个用户建立了一个考慮着	第20年度日
面。	特殊系型
bSIRR会,所有在这个网络中被信题。将输、处理。以及开始的信息和数据(包括个人信	デオ商 H3C
息),都会在一定范围内委到运会。转相反馈。	設計系統 Windows 8.1
来经想受我用的运用网络可能会导致产量后常,均量用成合约关系终止,产量的可能还要	MACME 0CDA41:1D.49 E6
承担相应的限制成并重要任。	>> 認知人運動計算法

[leaf-GigabitEthernet1/0/1]dis mac-au con Total connections: 1 Slot ID: 1 User MAC address: 0cda-411d-4be6 Access interface: GigabitEthernet1/0/1 Username: 0cda411d4be6 User access state: Successful Authentication domain: h3c IPv4 address: 155.0.0.15 Initial VLAN: 101 Authorization untagged VLAN: N/A Authorization tagged VLAN: N/A Authorization VSI: vsi3515 Authorization ACL ID: N/A Authorization user profile: N/A Authorization CAR: N/A Authorization URL: N/A Termination action: Default Session timeout period: 86400 s Online from: 2013/01/15 00:28:24 Online duration: 0h 0m 4s 在Director上在线用户也可以看到认证通过后正确上线了:

96 8	368°											4 M87x
	s secure na	8										和 花堂马
	696	1				用作分组		5/B				94 BR
	348732 8	INTER MINISTER	8 842 24ME	胞腺导出								
		8981	098.1	RPER +	重作品	BARR :	MARK 1	KRAPHUL I	ROPEST 1	安全状态。	SPRENNR (10/1
		BS/8/*1	0x5H1154be5	BS/8/1	803.801	2018-03-09 15:34:05	09	110.0.5.4	155.0.0.15	无期向会认证		
	共和語记录	. 2008/01-1 , 361/17	ι.								14 H	1 > > 50 *

3、验证终端移动的场景,移动前在access的g1/0/1,所在接口vlan为101,此时上线成功:

在純用户详细信息			
业 都在30月中14日代息			
基本信息			
核号名	静态用户1	用户姓名	静态用户1
登录名	Ocde411d4be6	服務名	接入组1
用户分组	#G18	继入巅略	担心相1.销略
私有预性下发策略	不使用	安全相	安全111
接入信息			
接入时间	2018-03-09 15:46:48	接入时长	089
用户即触过	155.0.0.15	用户MAC地址	0CsD4x41:1Dx48:£6
会活标识	OGmD2DZp	ak 图4系统	
设备IP地址	110.0.5.4	设备启动时间	2012-12-31 23:59:45
设备信号	1	设备子信号	0
2000	1	药法设备1P	110.0.5.3
直接设备第口	GigabitEthernet1/0/1	设备无关	
上次便新时间	2018-03-09 15:46:48	VLAN ID/内层VLAN ID	101
外班VLAN ID		TRVLAN	
上传字节数	0	下编字书数	0
THESED		NAS ID	leaf
计算机名称		Windows It:	
客户装进宫		80988	
\$P\$\$0		设备NAT IPM/定	110.0.5.4
代理类型	设备至本地	代證證入職址	110.0.5.4
イモ王軍を与けた時ため		代證明戶名	豚 恋用户1
客户装定制时间		设备库利号	
IMSHE	0C-DA-41-1D-48-E6	终端类型	
地址厂网	H3C	终端数件系统	Windows 8.1
IMERIE		硬盘煤列号	

版本信息			
眼号名	静态用户1	用户姓名	静态用户1
登录名	Ocda411d4be6	服务名	接入3 组1
用户分组	未分相	接入巅略	建筑入3组1 無時間
私有预性下发演感	不使用	安全组	安全相1
夏入信息			
输入时间	2018-03-09 15:55:11	建入时长	016
用户即触症	155.0.0.15	用户MAC继续	0C:D:As41:1D:48:E6
会副标识	ASH2YGH4	後援極限	
() 翻IP時北	110.0.5.4	设备启动时间	2012-12-31 23:59:45
设备信号	1	设备子槽号	0
2890	1	前许Gasp	110.0.5.3
自然设备第日	GigabitEthernet1/0/2	设备无关	
上次更新时间	2018-03-09 15:55:11	VLAN ID/内回VLAN ID	102
外层VLAN ID		TRVLAN	
上传字节数	0	下端字符数	0
Ka§\$SID		NAS ID	leaf
计算机名称		Windows H	
客户荣语言		客户读版本	
客户保留口号		设备NATIP账址	110.0.5.4
「「「「「「」」「「」」「「」」「「」」「」」「」」	设备至本地	代理接入触址	110.0.5.A
(注意是多多生的)。		代理用户名	静态用户1
8户操定制时间		设备库列号	
IM SI 号 Fil	0C-DA-41-1D-48-E6	他論実型	
1930年1月	H3C	他續續作系统	Windows 8.1
		24 (P) (56 (2)	

后续这台电脑随意挪到了access接口的g1/0/2,所在vlan为102,不用重新认证,能够无感知上线:

配置关键点

carry user-ip配置优化

每个leaf下行口都需要手工下发mac-authentication carry user-ip,这个太麻烦,可以在imc自定义leaf下行口策略,统一自动下发。步骤如下:

1、业务—通用—自定义动作,添加这个动作:

增加自定义动作 - Google	Chrome			- • ×
0 192.168.1.15:8080/ii	mc/campus/commgroup/actio	onUserDefined_con	itent.xhtml	
自定义动作				
动作名称*	carry user-ip			
动作类型*	按□类 ▼			
动作描述				
	mac-authentication ca	arry user-ip		
动作内容*				
可恢复	✓	le		
	undo mac-authentica user-ip	tion carry		
恢复动作内容*				
+ 1870				
动作名称	动作类型	可恢复	动作描述	删除
voice vlan	接口类	是		
carry user-lp	接口类	是		畲
共有2条记录,当前第1-2	2,第1/1页。		« < 1 >	» 50 •

2、在leaf下行口----组策略中添加carry user-ip这个动作:

 「現示 (1)Spine/Leaf/Access (2)環边接口到接口過的 (3)从组内觀除接口时。 	设备间的互通地口,应加入到 1,会自动下发退策略的动作; 会自动下发退策略的修复动作	对应角色描凸分组。 如是如人到LearFr行口,刘同时会不死二层网络城田长彩星,清重组织 :如果从LearFr行口制件,刘同时会相称二层网络城田长彩星,清重	藝作生! 長國政務行生!			
	+ 戦約 0 脱鉄 炭型 0	描述	细菌略	的联结果	修改	B
Access上行接口	系统预定义	Access设备上的上行接口,需要Trunk所有VLAN。	45-	Ξ.	B	
P电话接口组	自定义		45-	5	B	8
leaf上行接口	系统预定义	Leaf设备上的上行接口组。	4).		R	
	系统预定义	Leaf设备上的下行接口组。	44	5	R	
leaf下行接口		SpinalOB H00TUF#EDig	4 <u>5</u>		P	
eef下行接口 ipine下行接口	系统预定义	abused m Trat Latite radie				

Leat トロ接口,根据组织在	→ 出版記録 802.1X配置 MAC	NANDERGER WITE.				
+ 瑞加 C 刷新	① 192.168.1.15:8080/imc/sr	nc/groupPolicy/ext/gpE	xtCfg.jsf?beanNan	ne=campusGroup	StrategyBe	an&gpMode=0
名称 AA Trunk VLAN bb ARP限速配置 802.1X配置	基本信息 須昭名称* 須昭温近 功作配置	Georg Perfort - Shire & W		5716.G		
	 所有助作取得为行 所有助作取得为行 所有助作取得力行 原存在一个动作执行 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ <lp>・ </lp>	。但如果存在在一切作参数。 。但不执行动作参数不合法。 成功即可。不执行动作参数	不言法,则所有却作品的动作。 药动作。 不合法的动作。	87-94 7 .		
	49月1日7月3日 通岸动	n=				

192.168.1.15:8080/imc/scc/stra	tegy/actionSelectContent.jsf?beanName=smcGpExtBean&alarr
选择动作	
动作名称	描述
802.1X配置	接口使能802.1X认证
ARP限速配置	ARP限速配置
carry user-ip	
Hybrid VLAN	配置接口为Hybrid,并设置PVID、Tagged VLAN、 Untagged VLAN
MAC认证配置	接口使能MAC认证
Trunk VLAN	配置接口为Trunk接口,并设置允许VLAN
voice vlan	

4、最后查看部署结果可以看到leaf下行口自动下发成功:

相名 Lear下行第日 18時日			已下发遗口总数: 1				
				操作结果 全部		搜索设备19	撤销
接口名称		策略/二层网络线	方法参数	完成时间		操作结果	40.3
•Ten-GigabitEthen	net2/0/20(9.4.1.99)						
Trunk VLAN		mca	允许VLAN:1-4094 PVID:1	2018-03-13 17:18:57		成功	
MACILIERE		mca	域名由3c Guest VXLANs4090	2018-03-13 17:19:32		成功部署文件内容	
接口探索路进		mca	RE编8810:1	2018-03-13 17:25:34		成功問題文件内容	
开启DHCP Snot	oping家项记录	mca		2018-03-13 17:26:09		成功問題文件内容	
carry user-ip		carry user-ip		2018-03-23 10:06:59		成功部署文件内容	
部署创建服务实	491	test	VS1名称5wi3502 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第回第四目214 第 第四目214 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第	2018-03-13 17;38;35		sth [®]	
部署也建成历史	1 91	byod	VSI名称tvsi3504 指日第91:214 部日第127en-GigabitEthernet2/0/20 服务生例43504 以大月和(日本時)4504 回数分量以LAN-3504 細胞(appen)5884 細胞(appen)5884	2018-03-14 10:52:42		stad D	