旁路部署 ACG1000 吴君 2023-01-09 发表

^{组网及说明} 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为ACG1000系列应用控制网关: ACG10X0、ACG1000-AKXXX等。

注:本案例是在ACG1040的Version 1.10, Release 6614版本上进行配置和验证的。

1.2 配置需求及实现的效果

如下组网图所示,需要在原有的网络中增加ACG1040来审计内网用户上网行为,为最小程度避免影响原有网络,所以ACG1040采用旁路模式部署进原有网络;





组网说明:ACG1040旁路部署连接在二层交换机1/0/1接口,因为用户需要有通过网络访问ACG的需求,所以需要再连一条网线到交换机用于跨网段管理ACG使用。

1配置步骤

1.1 登录设备管理界面

设备管理口 (ge0) 的默认地址配置为192.168.1.1/24。默认允许对该接口进行PING, HTTPS操 作。将终端与设备ge0端口互联,在终端打开浏览器输入<u>https://192.168.1.1</u>登录设备管理界面。 默认用户名与密码均为admin。



1.2 配置旁路接口

#选择"网络配置">"基础网络">"部署方式"> "旁路部署"中勾选ge1接口,在弹出的对话框中选择" 确定"。

| HBC 9 | cPath ACG1000 ER REPHO REACE ROMEN REACE | MET | |
|---------------|--|-----|----|
| MORE | CONF AREX | - | |
| - BARR | 93088 | KO | 88 |
| - ZICHE | 1 pr0 | • | 0 |
| -DICHER | 2 pri | 0 | 8 |
| - 01580% | 3 942 | • | |
| 一点用暖行 | 4 pc] | • | |
| | 5 pr4 | • | |
| -Mark | 6 pr1 | • | |
| | 7 pe6 | • | |
| - DVANUE - DE | 8 ga7 | • | |
| - IVELIN | 9 pr8 | • | |
| | 10 pr9 | • | |
| | 11 pe00 | • | |
| | 12 pell | • | |
| | 13 get2 | • | |
| | 14 get3 | • | |
| | 15 pe14 | • | |
| | 16 pelS | • | |
| | 17 pet6 | • | 0 |

1.3 配置管理接口

#选择"网络配置">"接口配置">"物理接口"中将ge0接口IP地址修改为192.168.1.11/24。

- 注:修改完成后与ACG管理界面断开,需要将管理电脑
- 连入交换机后使用https://192.168.1.11重新登录ACG1040进行管理。

| нзс | SecPath ACG1000 | | - | | | | ٥ | n • | ▲ ④ |
|---------|-----------------|-----------------|-------------------|------------|-----------|-------|--------------|-------|------|
| HORE | 100001 7803 | MARCI MARCI R | MER CHAR CREE | 61796 | | | | | |
| - | Q. #H | | | | | | | | |
| - Ewper | 8368 | RA PRE | PARE PACES | INR: NI | H HE(Mos) | SMM5 | RONE | BRHS. | 18-5 |
| | 1 940 | 16.08.142.03724 | 3(8)404(2)79 | route full | 1000 | 10 | 40 | ٥ | 07 |
| | 2 get | | 31:36:40:46:37.78 | route ful | 1990 | down | 60 | 0 | 100 |
| | 3 gel | 77.1.1.2/24 | 3c/bi-40.4e 21/7p | route full | 1800 | down | 40 | 0 | 08 |
| | 4 gcl | 5.1.1.094 | 31:36:40:46:37.31 | route ful | 1000 | down | 100 | 0 | 68 |
| | 5 get | | 3:0:40.4e.2f.30 | apped full | 1800 | down | combo(HEC2) | 0 | 68 |
| | 4 pd | | 3c.8c.40.4e.26.7e | apped full | 1000 | down | combo(/BEII) | 0 | 68 |
| | 7 arti | | 3(8)40.4e(2).7 | tute full | 1800 | down | combo(HBCI) | • | C/F |
| | 8 ge7 | | 3e de 40 4e 3f dú | route ful | 1800 | down | combo(RECI) | 0 | 18 |
| | 9 ad | | 3c8c40.4e281 | with full | 1000 | down | 80 | • | C/F |
| | 20 ge9 | | 3x 8x 40.4e 37.82 | suth ful | 1900 | down | 90 | 0 | 68 |
| | 11 geb1 | | 3:3:4:4:2:0 | route full | 1000 | down | - | 0 | 0r |
| | 12 get1 | | 3c8c40.4c.2584 | apped full | 1,000 | down | 10 | 0 | GR . |
| | 13 ge12 | | 3:3:42.42.25 | apped full | 1900 | down | 40 | ۰ | 08 |
| | 14 get3 | | 3cmc40.4e.2f.86 | route ful | 1000 | down | 160 | 0 | GR |
| | 15 ge14 | | 3c8c40.4e.3/87 | route ful | 1800 | down | 18(3 | 0 | 08 |
| | 16 get5 | | 3:3:42.42.27.08 | routo ful | 1900 | down. | 40 | 0 | CP . |
| | 17 ge16 | | 3c8c40.4e.2180 | route ful | 1800 | down | 40 | 0 | GP |
| | 18 get2 | | 3:3:4:4:3:4:358 | later ful | 1900 | down | 40 | ٥ | C/F |
| | 19 ge18 | | 3:16:40.4e.208 | suite ful | 1000 | down | (C) | ٥ | 08 |
| | 20 ge19 | | 3:3:42.42.25 | apped full | 1900 | down | 40 | 0 | 10 |

| НЗС | SecPath ACG1000 | | 北河 | 889140 | TRACE | RPHH. | Rear | - | |
|------------------|-----------------|--|-----------|---------------------|----------------|--------|------------------|------|--|
| | PRAME | | | | | | | | |
| - VIN Bistons | 基本设置 | | | | | | | | |
| | | 640. 94 | 0 | | (3c.8c.40.4e.2 | 81:79) | | | |
| 配置关键点 | | 1962 | | | (0-127 1935) | | | | |
| | | 広利 | | | | | | | |
| | | Distribution in the second sec | v4 IPv | 6 | | | | | |
| 1.1 注意事项 | 5 | | 151 | 1955 • \$185 | ent Or | DHCP | O PPPOE | | |
| | | | HPC: | 開起 192.1 | 68.1.1124 | (# | 80 : 192.168.1.1 | (24) | |
| | | | LA MARTIN | and a second | | | | | |

应用审计功能需要购买特征库激活文件并激活后才能使用,如果特征库授权未激活或者特征 库授权过期则无法保证应用审计功能正常使用。

#在"系统管理">"系统维护">"授权管理"中可查看授权是否为已授权状态。

| | | 土页 | 数据中心 | 策略配置 | 用户管理 | 网络配置 | 系统管理 |
|-------------|-----------|----------|-----------|-----------|------|------|-------|
| ●系统设定 | 15纪11日 | | | | | | |
| | 0 导入许可证 | | | | | | |
| 一系统運用 | 模块名 | | | | 授权状态 | | 剩余时间 |
| - 023010311 | 应用监控升级服务 | s/URL分类的 | ■升级服务/恶意U | 4.分與库升级服务 | 未授权 | | 授权已过期 |
| 一系统告誓 | 入侵防御升级服务 | 5 | | | 末授权 | | |
| 一系统诊断工具 | 病毒防护升级服务 | 5 | | | 未授权 | | |
| 制約丁具 | 非经SDK功能投资 | ž. | | | 未授权 | | |

#选择"网络配置"。"路电管理"字静命整出。音调建"户创建静奋路由,日的推扯和掩码都设置为:0.0.0.0(代表所有网段),下一跳地址配置192.168.1.254(路由器下联接口地址),配置完成后点击提交。

| 正 P+400-0000 第日 VPF VOF VOF VOF ● 前月 ● 前月 ● 百日 ● 前月 ● 五市 ● 日本 ● 日 | Secrati | ACG1000 | 主页 数据中心 | 并略配器 | 用戶管理 | 网络配置 | 新統體 |
|---|-----------------|---|---------------------------|-------------------|------------------|------|-----|
| mana manaa mana manaa manaaa manaaa manaaaaaaaaaa | | IPv4静念器由 | | | | | |
| Control Control No.00 Control Control <thcontrol< th=""> <thcontrol< th=""> <thcon< td=""><td></td><td>+ 952 × 558 VRF root</td><td>· O B用 C</td><td>前用 Q 查询</td><td></td><td></td><td></td></thcon<></thcontrol<></thcontrol<> | | + 952 × 558 VRF root | · O B用 C | 前用 Q 查询 | | | |
| YP22冊 1 0.0.0.0 0.0.0.0 10.88.140.1 pm ⁻⁰ 設計曲 第時 可能量 可能量 可能量 目前 目前 目前 目前 目前 目前 目前 目前 目前 目前 | | 8634842 | 推四 | 下一號 | | 出接口 | |
| | | | 00000 | 20.00.1 | χ ₂ λ | Geo | |
| | '由 | | | | | | |
| ◎用 ✓ | 由 | | | | | | |
| | 曲 宣用 目的地址 | 0000 | • | 1 | | | |
| 2月 ご 目的3世紀社 00000 子内別時時 00 | 由 | ✓ ○ ○ ○ ○ ○ ○ | | 1 | | | |
| 四時 2 2 2 3 3 3 3 5 3 3 5 5 5 5 5 5 5 5 5 5 5 5 5 | 由 | 2 0000 0 3〇 第一可 ④ | 11按口 |] | | | |
| 版用 目的地址 0.0.0.0 子网编码 0 下一號/出線□ ●下一號 ○出線□ 下一號 192.168.1.254 | 曲 | ■ 0.0.0.0 0 ● 下一跳 ○ E 192.168.1.254 | | | | | |
| 周用 目的地址 子例独码 0 下一號(出線□ ●下一號 ○出線□ 下一號 192.168.1.254 7 変重 1 (1-255) | 由 | ○ ○ ○ 下一跳 ○ と 192.168.1.254 1 | * * * (1-2) | 5) | | | |
| 周用 ■ 目的地址 0.0.0.0 子网独码 0 下-姚/出線□ ●下一姚 ○出線□ 下一姚 192.168.1.254 変麗 1 (1-255) 距离 1 (1-255) | 由 | ■ 0.0.0.0 0 ● 下一跳 ○ E 192.168.1.254 1 | 出版口 * (1-2) * (1-2) |) (5) (5) | | | |
| 周用 目的地址 子树釉码 0 下一號/出線□ 下一號/出線□ 下一號 192.168.1.254 0 1 (1-255) 距离 1 (1-255) | 曲 | ■ 0.0.0.0 0 ● 下一跳 ○ E 192.168.1.254 1 1 | 当编□ (1-2) |) (55) (55) | | | |

注: 这步操作是保证ACG可以被其他网段终端管理。

1.5 配置IPV4策略审计用户流量

1.4

#选择"策略配置">"IPV4策略">"新建"中创建审计策略。 注:该配置自行按需求选配



#选择对应的源地址 (可新建地址组)

588#

| | - | The second | 710.000 | |
|------|---|---|----------|--|
| R12 | | Numero de | CS20791R | |
| ()用户 | | + #it • (7 ## x #h) 29 | 用户 | |