

知 ACG1000 日志分析与管理平台下发配置模版失败

ACG1000 曾招维 2023-10-31 发表

组网及说明

ACG1000-AI-10通过ipsec vpn纳管到ACG1000 日志分析与管理平台。

问题描述

ACG1000 日志分析与管理平台下发配置模版后显示ACG1000-AI-10离线，删除配置模版后重新上线。
同一个配置模版下发到多台ACG1000，现场只有这台有异常。

版本信息：ACG1000-AI-10 R6614P10、平台版本 R0306P01

现象如图：未下发配置时显示正常上线，下发配置后显示“未下发、离线”

The image contains two screenshots of the H3C ACG1000 management interface. The top screenshot shows a list of 11 devices. Device 2, '设备2', is highlighted with a red box and shows a status of '未下发' (Not Deployed) and '离线' (Offline). The bottom screenshot shows the same list after configuration template deployment. Device 2 is now highlighted with a red box and shows a status of '未下发' (Not Deployed) and '离线' (Offline), while other devices show '上线' (Online) status.

序号	设备名称	设备IP	设备版本	配置模板	状态	CPU	磁盘	操作
1	设备1	3.5.13	i-Ware software Ver...	默认配置模板(已部署)	在线	4%	-	操作
2	设备2	3.5.14	i-Ware software Ver...	默认配置模板(未部署)	未下发	5%	-	操作
3	设备3	3.5.15	i-Ware software Ver...	默认配置模板(已部署)	在线	5%	-	操作
4	设备4	3.5.12	i-Ware software Ver...	默认配置模板(已部署)	在线	6%	-	操作
5	设备5	3.5.9	i-Ware software Ver...	默认配置模板(已部署)	在线	3%	-	操作
6	设备6	3.5.4	i-Ware software Ver...	默认配置模板(已部署)	在线	3%	-	操作
7	设备7	3.5.10	i-Ware software Ver...	默认配置模板(已部署)	在线	3%	-	操作
8	设备8	3.5.11	i-Ware software Ver...	默认配置模板(已部署)	在线	7%	-	操作
9	设备9	3.5.7	i-Ware software Ver...	默认配置模板(已部署)	在线	3%	-	操作
10	设备10	3.5.6	i-Ware software Ver...	默认配置模板(已部署)	在线	9%	-	操作
11	设备11	3.5.17	i-Ware software Ver...	默认配置模板(已部署)	在线	3%	-	操作

过程分析

1、平台侧信息：配置模版中只有审计策略和安全策略，规则都是全选、对象any，安全策略默认通过；有正常打3000个数量授权、ACG1000-AI-10不属于高端款型。

序号	授权类型	授权数量	有效期	设备数量	基本类型	授权状态
1	数量授权	3000	永久	3000	正在授权	未授权

2、ACG1000-AI-10设备侧显示正常，担心相关策略对纳管有影响，我直接测试下发一个全局白名单，但是故障依旧。

序号	策略名称	地址	模式	状态	操作
1	全局白名单	地址	模式	状态	操作

3、ping和tcp syn测试正常。

基础配置

目的地址: (4-253)

探测包数目: (1-10)

探测包大小: (64-65500)

Ping结果

4、ACG1000-AI-10通过ipsec vpn纳管到ACG1000 日志分析与管理平，查看系统日志，有IPsec vpn隧道重新建立过程。

2162	30419	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 50] 老化，源目IP为 196.165(500)，感兴能流为(14.0/24:0-0.0/24:0 proto[0])
2174	30420	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 50] 在隧道tunnel0上建立成功，源目IP为 196.165(500)，感兴能流为(4.32:0->1.0/24:0 proto[0])
2175	30421	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 50] 在隧道tunnel0上建立成功，源目IP为 196.165(500)，感兴能流为(4.0/24:0->1.0/24:0 proto[0])
2176	30422	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 54] 在隧道tunnel0上建立成功，源目IP为 196.165(500)，感兴能流为(4.32:0->1.0/24:0 proto[0])
2177	30423	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 55] 在隧道tunnel0上建立成功，源目IP为 196.165(500)，感兴能流为(4.32:0->1.0/24:0 proto[0])
2178	30424	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID=51] 老化，源目IP为 96.165(500)
2179	30425	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID=50] 老化，源目IP为 96.165(500)
2180	30426	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID=49] 老化，源目IP为 96.165(500)
2181	30427	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID=48] 老化，源目IP为 96.165(500)
2182	30428	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 51] 删除！源目IP 196.165(500)，感兴能流为(14.32:0->1.0/24:0 proto[0])
2183	30429	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 50] 删除！源目IP 196.165(500)，感兴能流为(14.0/24:0->1.0/24:0 proto[0])
2184	30430	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 49] 删除！源目IP 196.165(500)，感兴能流为(14.32:0->1.0/24:0 proto[0])
2185	30431	2023/10/31 16:34	5	IPSEC	IPsec-阶段SA [ID: 48] 删除！源目IP 196.165(500)，感兴能流为(14.0/24:0->1.0/24:0 proto[0])

解决方法

经确认当 ipsec vpn 断开，相关平台注册流量就会走默认路由，生成一个NAT会话，vpn重新建后nat 这条会话还未老化，vpn恢复正常后匹配反向会话，导致平台下发配置模版异常，虽然平台一直显示在线，只是在保活周期内，后面报文序上来，可能底层已经断开了。

解决方法： NAT策略的目的ip里排除一下平台IP地址x.x.1.5，还需要命令行ACG# clear ip connection all 配合清除历史会话 使用。



