RBM设备升级后IPS策略丢失典型案例分析

双机热备 孔凡安 2023-10-16 发表

组网及说明

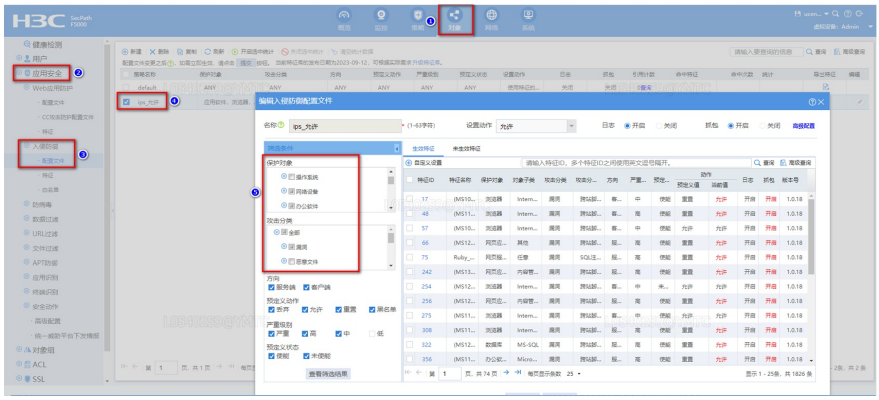
不涉及

告警信息

不涉及

问题描述

客户升级前防火墙对象—应用安全—入侵防御—配置文件，新建的配置文件，保护对象和攻击分类全选。升级之后发现部分配置丢失，保护对象和攻击分类随机勾选。



过程分析

首先查看客户操作完设备之后是否进行了保存配置操作，发现有正常保存配置的习惯。因此排除没有及时保存配置的原因。

对比CFGLOG和logfile文件查看用户重启之前的操作，可以发现客户重启设备的时候先重启的主机RBM_P，然后重启的RBM_S。由于RBM重连之后要向对端同步配置，发现RBM_P有删除配置的操作，猜测RBM_S和RBM_P的配置在重启前就是不一致的。

%@23656%Sep 27 18:10:51:570 2023 W1D1G07-WAN-FW03 RBM/1/RBM_KEEPALIVE: Local IP=1.1.1.153, remote IP=1.1.1.154, status=Connected ----重启之后RBM重新连接

%@23657%Sep 27 18:10:51:898 2023 W1D1G07-WAN-FW03 RBM/6/RBM_RUNNING_STATUS_CHANGED: RBM running status changed to standby.

%@23658%Sep 27 18:10:51:899 2023 W1D1G07-WAN-FW03 OSPF/6/RBM_ADJUST_COST: RBM notified cost adjust to 5000.

%@23659%Sep 27 18:10:52:535 2023 W1D1G07-WAN-FW03 LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/1/6 (IfIndex 11), neighbor's chassis ID is 642f-c7d8-8130, port ID is Ten-GigabitEthernet1/1/6.

%@23660%Sep 27 18:10:52:536 2023 W1D1G07-WAN-FW03 LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/1/7 (IfIndex 12), neighbor's chassis ID is 642f-c7d8-8130, port ID is Ten-GigabitEthernet1/1/7.

%@23661%Sep 27 18:10:53:867 2023 W1D1G07-WAN-FW03 SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=**; Command return in view shell failed to be matched.

%@23662%Sep 27 18:10:53:874 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is system-view

%@23663%Sep 27 18:10:53:887 2023 W1D1G07-WAN-FW03 SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=**; Command _switchto vsysAdmin in view system failed to be matched.

%@23664%Sep 27 18:10:53:893 2023 W1D1G07-WAN-FW03 SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=**; Command system-view in view system failed to be matched.

%@23665%Sep 27 18:10:53:913 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is interface GigabitEthernet1/0/0

%@23666%Sep 27 18:10:53:966 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is return

%@23667%Sep 27 18:10:53:979 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is system-view

%@23668%Sep 27 18:10:53:988 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is ips policy ips_允许

%@23669%Sep 27 18:10:54:039 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target ApplicationSoftware Any

%@23670%Sep 27 18:10:54:103 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target ApplicationSoftware Backup ----***代表设备执行shell操作，判断是RBM在同步配置

%@23671%Sep 27 18:10:54:158 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target ApplicationSoftware Download

%@23672%Sep 27 18:10:54:229 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target ApplicationSoftware MediaPlayer

%@23673%Sep 27 18:10:54:296 2023 W1D1G07-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

ApplicationSoftware Other

%@23674%Sep 27 18:10:54:399 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

ApplicationSoftware Security

%@23675%Sep 27 18:10:54:488 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Botnet Any

%@23676%Sep 27 18:10:54:561 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Browser Any

%@23677%Sep 27 18:10:54:645 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Browser MozillaFirefox

%@23678%Sep 27 18:10:54:714 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Browser Other

%@23679%Sep 27 18:10:54:775 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Database Any

%@23680%Sep 27 18:10:54:819 2023 W1D1G07-WAN-FW03

SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo protect-target

Database DB2

解决方法

问题原因：由于RBM_S特征库版本与RBM_P不一致，导致和特征相关的IPS策略部分下发失败。

解决方案：RBM_S特征库升级到最新版本

延伸：

部署HA前，请先保证主/备设备软件环境的一致性，具体要求如下：

- 主/备设备的系统软件环境及其版本必须一致，如：Boot包、System包、Feature包和补丁包等等。
- 主/备设备的系统时间一致。--为了实现自动同步（https://zhijiao.h3c.com/Theme/details/221746）
- 主/备设备上被授权的特征库和特性环境必须一致，如：特征库的种类，每类特征库的版本、授权时间范围、授权的资源数等等。
- 主/备设备上的资源文件必须一致，比如：公钥信息、ISP地址库文件等。
- 主/备设备的接口编号必须一致。
- 主/备设备之间建立HA通道的接口类型、速率和编号等信息必须一致，推荐使用聚合接口。
- 主/备设备上聚合接口的编号、成员接口编号必须一致。
- 主/备设备相同位置的接口必须加入到相同的安全域。
- 主/备设备的HASH选择CPU模式以及HASH因子都必须相同（即forwarding policy命令）。

进一步分析之前RBM_S和RBM_P配置不同步的原因，发现RBM_S同步配置的时候命令执行失败。因此两边配置不同。

%@1294959%Sep 27 16:50:02:391 2023 W1D2K04-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is system-view

%@1294960%Sep 27 16:50:02:396 2023 W1D2K04-WAN-FW03 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is ips policy ips_允许

%@1294961%Sep 27 16:50:02:425 2023 W1D2K04-WAN-FW03 SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=**; Command protect-target ApplicationSoftware Any in view ips-policy-ips_允许 failed to be matched.

通过以上分析判断RBM_P下发IPS策略的时候，RBM_S无法下发配置。猜测原因可能与设备版本不一致或者特征库版本不一致优选。