

KillTest

높은 품질, 더 나은 서비스



연습 문제

<https://www.killtest.kr>

1년간 무료 업데이트 제공

Exam : H12-723

**Title : HCNP-Security-CSSN
(Constructing Service
Security)**

Version : DEMO

1.下列哪些是 URL 过滤失效的可能原因？

(Select 3 Answers)

- A.URL 过滤域间应用方向错误或关联策略错误
- B.分类服务器不能访问
- C.未开启 bypass 功能
- D.URL 过滤策略未提交编译

Answer: A B D

2.关于下列命令，说法正确的是？

<USG> display rbl-filter global-configuration

```

RBL filter           : Enable
RBL enabled profile  : Pre-define
RBL server IP address : 192.168.1.10, 192.168.1.11
RBL whitelist        : Enable
RBL blacklist        : Disable
  
```

(Select 3 Answers)

- A.使用的是预定义的 RBL 过滤
- B.开启了 RBL 白名单
- C.RBL 服务器地址是 192.168.1.10 和 192.168.1.11
- D.DNS 服务器地址是 192.168.1.10 和 192.168.1.11

Answer: A B D

3.某 TSM 客户端进行认证时，发现认证不通过提示“无法与服务器建立连接”。



通过故障诊断工具进行问题定位，提示以下信息。请问可能是由什么问题引起？

(Select 3 Answers)

- A.TSM 服务器宕机或重要服务未启动。
- B.TSM 客户端中的 SC 服务器设置有误。
- C.TSM 客户端与 TSM 服务器之间网络可达性存在问题。
- D.硬件 SACG 未启用 detect 命令，导致多通道协议的数据交互被阻断。

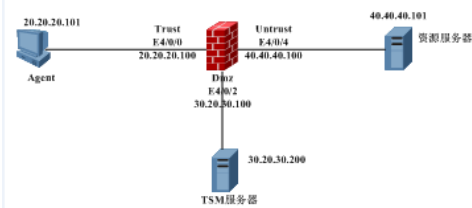
Answer: A B C

4. 防火墙 DPI 知识库升级失败的原因可能为: (Select 3 Answers) A. 未配置 DNS。
 B. 升级时网络业务量大, 带宽不足导致知识库文件下载失败。
 C. 防火墙与 sec 网站之间路由不通。
 D. 升级时选择的知识库文件错误。

Answer: A B C

5.

综合案例题。以下组网为路由模式下 SACG 与 TSM 服务器联动的典型组网图。假设 Agent 在 trust 域, TSM 服务器在 dmz 域 (认证前域), 受保护资源在 untrust 域 (认证后域)。要求 Agent 在认证前只能访问认证前域的 TSM 服务器, 认证通过以后可以访问认证后域的资源服务器。



问题一: SACG 配置完成后, 发现联动不成功。在 SACG 上进行 DEBUG 调试, 输出如下信息:

```
<SACG>terminal debugging
```

```
<SACG>debugging
```

```
right-manager all
```

```
0.4642700 SACG %%01SACG/8/debug(d): EVENT from COPS module connect to 40.40.40.101.
```

```
0.4647700 SACG %
```

```
%01SACG/8/debug(d): EVENT from COPS module connect to 40.40.40.101.
```

通过上面的调试信息, 判断下述解决方法 (思路) 中正确的是: Select 3 Answers

- A. 通过 PING 检查 secospace 的 IP 是否可达。
 B. 检查 TSM 服务器 3288 端口是否处于 listening 状态, `netstat -nao | find "3288"`。
 C. 检查 SACG 的内存和 CPU 资源是否过高。
 D. 查看是否是 SACG 阻断了 3288 端口, 需要在 SACG 上打开从 SACG 到 TSM 服务器方向的 3288 端口。或者打开 local 域到 TSM 服务器所在域的包过滤规则。

Answer: A B D