

# Real4Exams

Real4exams

Latest updated materials, Daily Updates!



ORACLE®



<http://www.real4exams.com>

Real IT Certification Exam Study guide/Braindumps

**Exam** : **H12-731-CN**

**Title** : **HCIE-Security (Huawei Certified Internetwork Expert-Security) (H12-731 中文版)**

**Vendor** : **Huawei**

**Version** : **DEMO**

**QUESTION NO: 1**

某企业新建的园区网中,在某个接入交换机下有普通 PC 用户和哑终端用户同时联网的需求。建议在该交换机上部署哪种认证方式？

- A. 802.1X 认证
- B. Portal 认证
- C. MAC 旁路认证
- D. MAC 认证

**Answer:** C

**QUESTION NO: 2**

边界网络安全,关于规划部署建议优先考虑项有以下哪些选项？

- A. 安全域隔离
- B. IPS 实时入侵防御
- C. 开启 DDoS 功能
- D. 部署 VPN
- E. 开启设备虚拟化功能

**Answer:** A,B,C

**QUESTION NO: 3**

某网络 IPsec 状态信息如下, [USG A] display ike sa  
current ike sa number: 2

-----  
conn-id peer flag phase vpn  
-----

```
40006 <unnamed> NONE v1:2 public
40004 1.1.1.2 RD|ST v1:2 public
2012-08-08 15:05:15 USG %%01IKE/4/WARNING (I): phase2: proposal or pfs dh-gro up
mismatch, please check ipsec proposal and pfs dh-group configuration.
*0.1921499990 USG IKE/7/DEBUG: got NOTIFY of type NO_PROPOSAL_CHOSEN
以下哪个选项是可能的故障原因？
```

- A. ACL 配置有误
- B. IPsec 提议不匹配
- C. IKE 预共享密钥不匹配
- D. PFS 配置不一致

**Answer:** B,D

**QUESTION NO: 4**

RADIUS 和 HWTACACS 协议的主要区别包括:

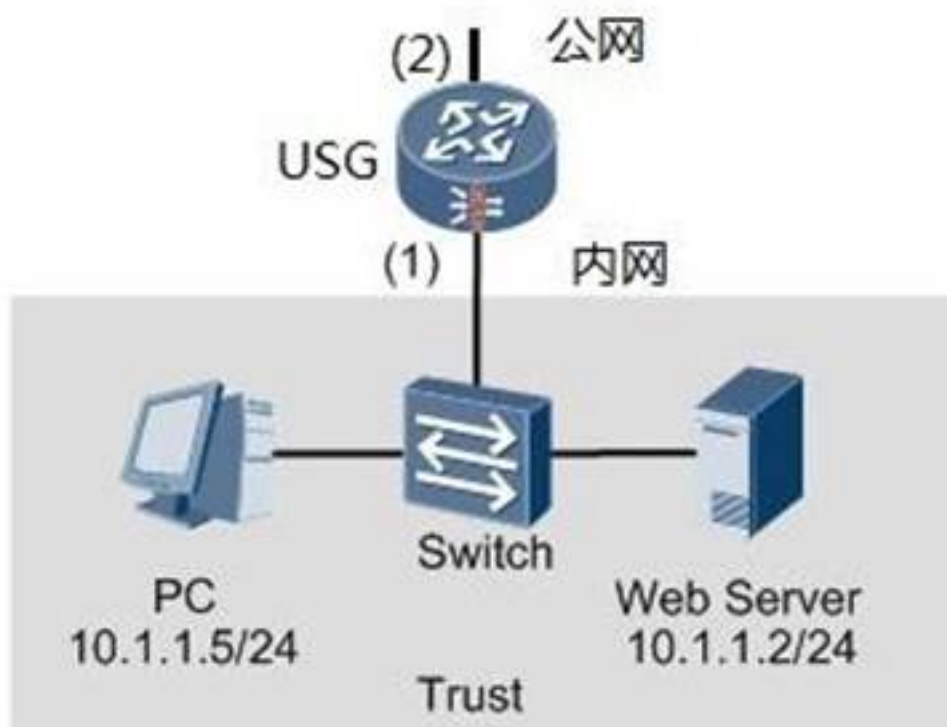
- A. RADIUS 认证与授权分离, HWTACACS 认证与授权一起处理。
- B. HWTACACS 支持对配置命令进行授权, RADIUS 不支持对配置命令进行授权。
- C. HWTACACS 对报文主体全部进行加密, RADIUS 只是对认证报文中的密码字段进行加密。
- D. RADIUS 使用 TCP 协议,网络传输更可靠, HWTACACS 使用 UDP 协议。

**Answer:** B,C

**QUESTION NO: 5**

如图的组网中, PC 访问 Web Server 的流量必须经过防火墙, Web Server 回应给 PC 的流量的必须经过防火墙。

在防火墙上正确配置了域内双向 NAT 后,以下对数据包 IP 地址的描述可能正确的是:



- A. Web 服务器收到的 PC 访问其 Web 服务的数据包的源 IP 地址为接口 ( 1 )的 IP 地址。
- B. PC 机收到 Web 服务器回应的数据包的源 IP 地址为 10.1.1.2 。
- C. 厂 PC 机收到 Web 服务器回应的数据包的源 IP 地址为接口 ( 2 )的 IP 地址。
- D. Web 服务器收到的 PC 访问其 Web 服务的数据包的源 IP 地址为 10.1.1.5 。

**Answer:** A,C

**QUESTION NO: 6**

如下配置,当接口 G0/0/1 物理状态 down 后,交换机 switch 将发生什么变化

PC ----- (G0/0/1) FW (G0/0/2) ----- Switch

```
#
interface GigabitEthernet0/0/1
link-group 1
interface GigabitEthernet0/0/2
link-group 1
#
```

- A. Switch 接口地址的 ARP 表项将老化失效。
- B. 防火墙发免费 ARP 给上行设备 Switch 更新 MAC 地址。
- C. 没有变化。
- D. Switch 接口地址的 ARP 表项被立即删除。

**Answer:** D

**QUESTION NO: 7**

防火墙双机热备的场景下, IPsec VPN 不支持隧道的实时备份。

- A. FALSE
- B. TRUE

**Answer: A**

**QUESTION NO: 8**

VGMP 统一管理 VRRP 备份组状态, VGMP 管理组 Active 的优先级为 65001 , Standby 优先级为 65000 。当 VGMP 管理组通过 VRRP 备份组或直接监测到接口 Down 时,会重新计算 VGMP 管理组优先级,每个接口 Down 时, VGMP 管理组优先级降低 2 。

- A. TRUE
- B. FALSE

**Answer: A**

**QUESTION NO: 9**

某管理员是国内某城市银行信息安全主管,企业近年来业务发展迅猛。公司领导层越来越关注企业法规遵从,以下哪些标准是企业必须遵从的。

- A. SOX 法案
- B. ISO2700X 信息安全系列
- C. 商业银行信息技术风险科技指引
- D. 信息系统安全等级保护条例

**Answer: C**

**QUESTION NO: 10**

在配置 IKE 提议时,下面哪 3 个参数是必须配置的 ?

- A. PFS
- B. Hash 算法
- C. security acl
- D. DH-group
- E. 加密算法

**Answer: B,D,E**

**QUESTION NO: 11**

USG 中 URL 过滤功能中, URL 匹配方式有哪些 ?

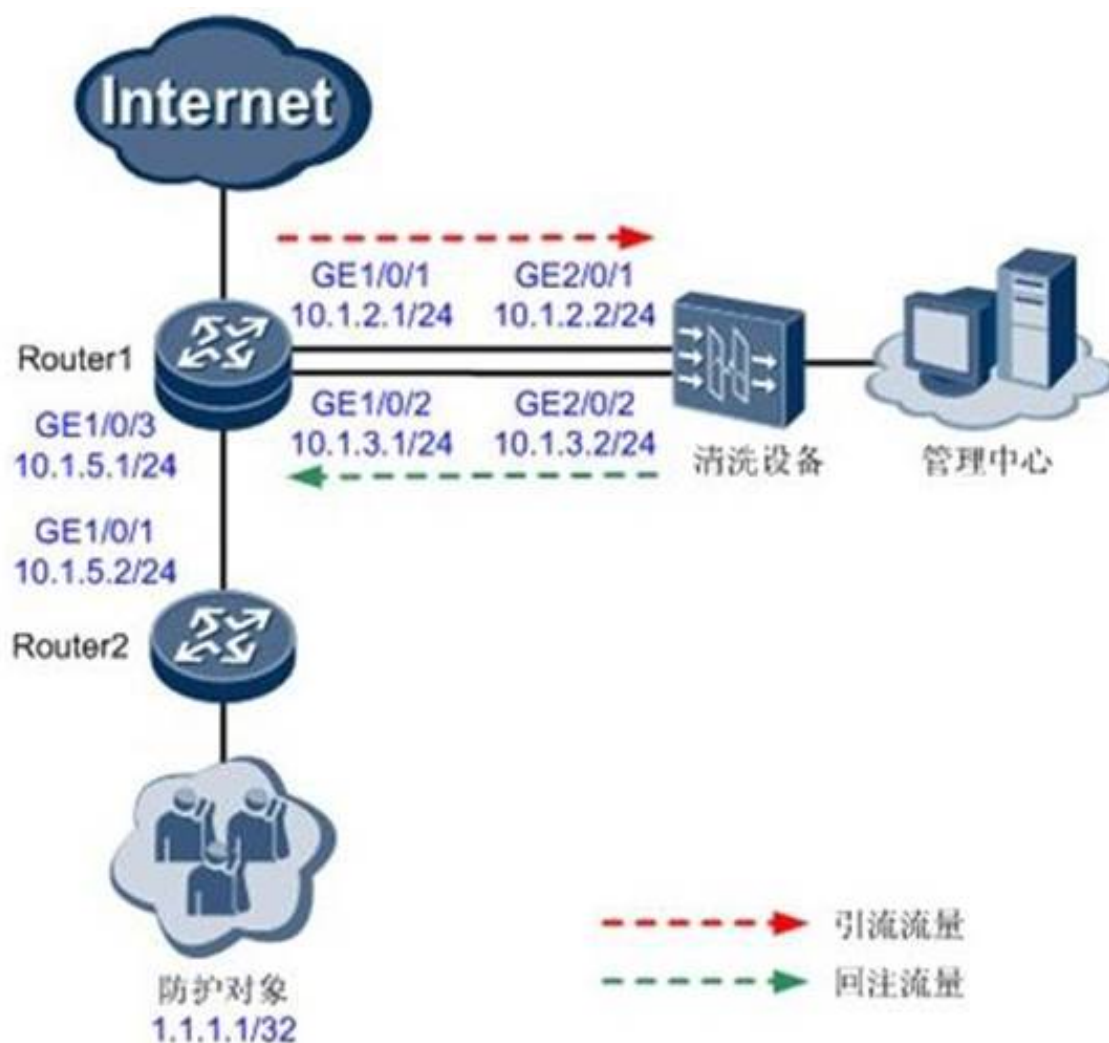
- A. 精确
- B. 后缀
- C. 关键字
- D. 参数
- E. 前缀

**Answer: A,B,C,E**

**QUESTION NO: 12**

根据以下组网,某客户在清洗设备上使用了以下配置,以下说法正确的是:

```
ip route-static 0.0.0.0 0 10.1.2.1
```



- A. 该默认路由用于流量回注
- B. 该默认路由用于发送攻击防范的探测流量
- C. 该默认路由用于 BGP 引流
- D. 该默认路由用于静态路由引流

**Answer:** B

#### QUESTION NO: 13

IKEv1 和 IKEv2 的区别,下面哪些描述是正确的?

- A. IKEv1 默认支持 DPD ,只要在一端配置 DPD ,另一端就可以响应 DPD 报文。IKEv2 不可以。
- B. 建立 IKE SA 和 IPsec SA , IKEv2 使用 4 条消息, IKEV1 主模式使用 9 条消息。
- C. IKE SA 的完整性算法仅 IKEv1 支持。
- D. IKEv2 可以借助 AAA 服务器分配私网 IP 地址, IKEv1 无法提供此功能。

**Answer:** B,D

#### QUESTION NO: 14

在 IPsec 协商失败的过程中,打开 IKE 的调试开关,显示如下信息: got NOTIFY of type NO\_PROPOSAL CHOSEN 或 drop message from A.B.C.D due to notification type NO\_PROPOSAL CHOSEN ,应该如何处理?

- A. 如果第一阶段没有协商成功,可能配置的 pre-share-key 不对。
- B. 如果是第二阶段没有协商成功,可能是 ACL 没有匹配。
- C. 如果第一阶段没有协商成功,可能是 ike 提议不匹配。
- D. 如果是第二阶段没有协商成功,可能是 ipsec 提议没有匹配。

**Answer:** C,D

#### QUESTION NO: 15

管理员在使用 USG 网关的 SSL 功能,快速、安全地访问企业内网的所有资源,不仅仅是 Web 资源,并保证客户端和虚拟网关之间的通信采用 SSL 安全协议,而且必须保证 SSL 客户端不影响访问其他网络资源,可以直接访问 Internet 资源。

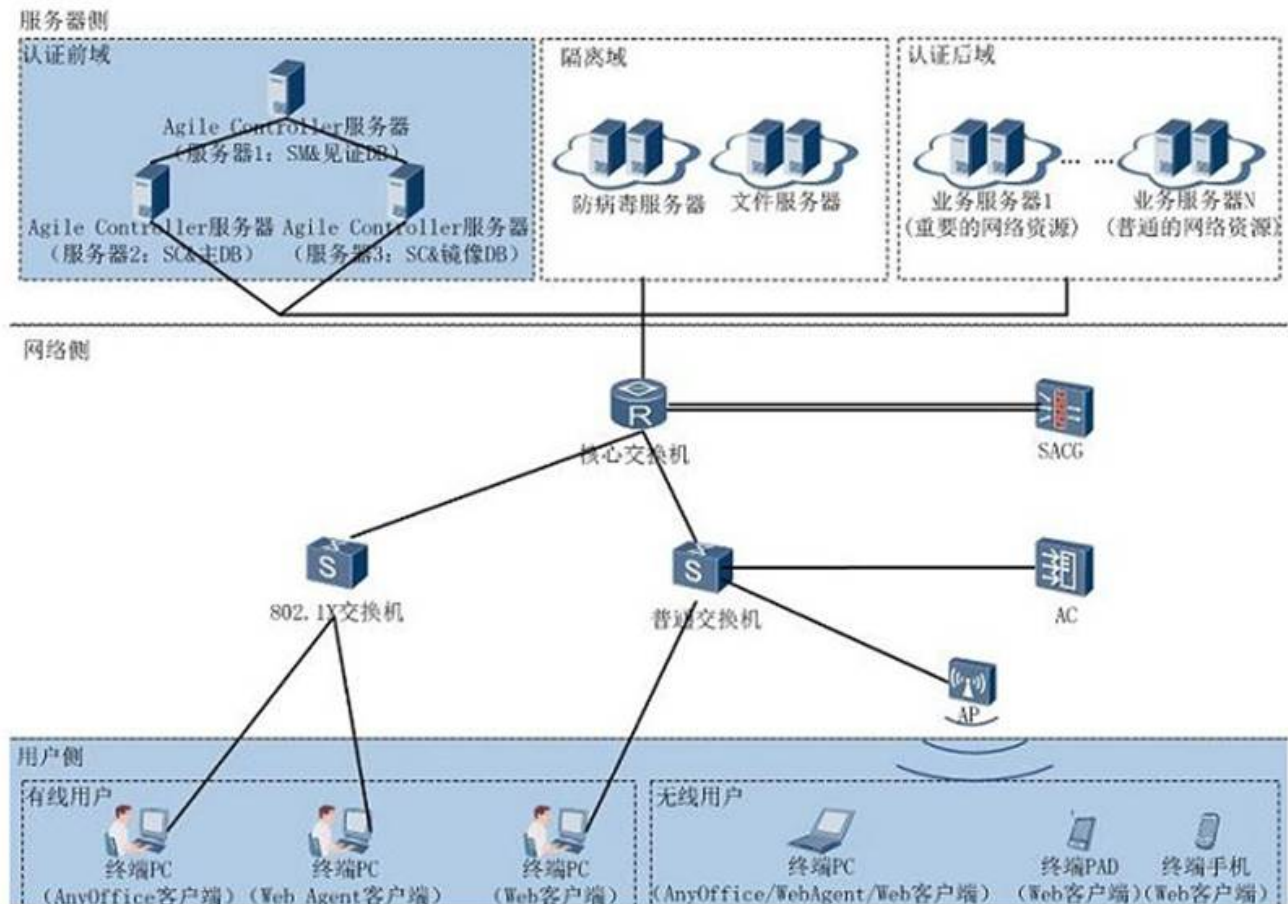
- A. 手动模式的网络扩展
- B. 分离模式的网络扩展
- C. 全路由模式的网络扩展
- D. 端口转发

**Answer:** A

#### QUESTION NO: 16

三台服务器集中组网方案,如图,管理员发现资源池中三台 Agile Controller 控制器只有一台是存活的。

在这种情况下,下面几个描述哪个是正确的？



- A. 此时可以尝试重新启动存活的 Agile Controller 控制器,在重启时修复数据库服务器。
- B. 三台数据库服务器均无法正常工作,资源池中三台 Agile Controller

控制器只有一台是存活的。在这种情况下, Agile Controller 业务全部转移至存活的 Agile Controller

制器并且能够正常运作,终端身份认证、接入控制、软件分发、补丁安装、资产管理不会受到影响。

- C. 在 Agile Controller 控制器启动后,每一台 Agile Controller 控制器会立即读取数据库并以缓存的方式保存在本地硬盘。如果所有数据库因故障变得不可用,则 Agile Controller 控制器以当时保存的缓存为数据源继续维持 Agile Controller 业务的运转。
- D. 此时防火墙上的逃生通道已经打开。

**Answer:** B,C

#### QUESTION NO: 17

以下关于 IP-Link 的描述哪个是错误的 ?

- A. 根据 ICMP 回显请求或 ARP 请求,实现链路探测。
- B. 提供毫秒级的快速可达性检测。
- C. 能够为静态路由、 VRRP 等多个业务模块提供可达性检测。
- D. 静态路由与 IP-Link 联动可以自动检查,当发现链路故障时,会对对端的静态路由进行相应的调整。

**Answer:** B,D

#### QUESTION NO: 18

针对 USG 状态检测防火墙的基本转发处理流程描述正确的是:

- A. 针对首包先进行基于单包的攻击防范检测再进行包过滤处理。
- B. 数据包进入防火墙首先进行黑名单匹配,然后进行会话表匹配。
- C. 需要源地址网络地址翻译时,先进行 NAT 再进行域间策略匹配检测。
- D. 需要目的地址 NAT 时,先进行 NAT 再进行域间策略匹配检测。

**Answer:** A,D

#### QUESTION NO: 19

L2TP over IPsec 拨号支持哪几种认证方式 ?

- A. TSM 认证
- B. PEAP 认证
- C. 支持本地认证
- D. LDAP
- E. Radius

**Answer:** C,D,E

#### QUESTION NO: 20

通过查看现网运行正常的一台 USG 防火墙配置信息,获取到如下信息:

```
#
ip service-set http 8080 type object
service 0 protocol tcp destination-port 8080
#
security-policy
rule name untrust_to_dmz1
```

```
source-zone untrust
destination-zone dmz
service ftp
destination-address 192.168.5.3
32
action permit
rule name un_trust_to_dmz2
source-zone untrust
destination-zone dmz
service service-set http_8080
destination-address 192.168.5.2
32
action permit
#
```

以下说法不正确的是:

- A. 外网用户可以使用 80 端口访问地址为 192.168.5.2 的服务器的 www 服务。
- B. 外网用户可以使用端口 21 与地址为 192.168.5.3 的服务器建立 ftp 连接。
- C. 外网用户可以使用非 21 端口与地址为 192.168.5.3 的服务器建立 ftp 连接。
- D. 外网用户可以访问地址为 192.168.5.2 的服务器的 8080 目的端口。

**Answer:** A,C