



d、精确匹配

e、路经匹配

答案：bcd

解释：

URL 匹配方式表

匹 配 方 式	定 义	条 目	匹 配 结 果
前 缀 匹 配	匹配所有以指定字符串开头的 URL。	www.example.com*	匹配所有以 www.example.com 开头的 URL，如： www.example.com www.example.com/soluCons.do
后 缀 匹 配	匹配所有以指定字符串结尾的 URL。	*aspx	匹配所有以 aspx 结尾的 URL，如： www.example.com/news/soluCons.aspx www.example.com/it/price.aspx 10.1.1.1/sports/abc.aspx
关 键 字 匹 配	匹配所有包含指定字符串的 URL。	*sport*	匹配所有包含 sport 的 URL，如： sports.example.com/news/soluCons.aspx sports.example.com/it/ 10.1.1.1/sports/
精 确 匹 配	只匹配指定字符串。	www.example.com/news	只匹配 www.example.com/news。 www.example.com/news/soluCons.aspx、 www.example.com/news/en/等

3. 防火墙的 ip 报文分片重组需要对报文中哪几个字段进行分析？

a、标识符 Idenfier

b、标志 Flags

c、片偏移

d、总长度

e、生命时间

答案 abc

4. 使用 NGFW 进行 SSLVPN 连接， 使用证书认证， 证书可以选择，但是点击登录后，无法登录到资源页面，经过在 NGFW 上使用 debug 检查， 提示证书错

误。

```
<NGFW>debugging 551 error
```

```
<NGFW>terminal debugging
```

```
<NGFW>terminal monitor
```

```
*0.10012266 U5G2130 55L/7/error:
```

```
55L 3.0 , Alert, write, fatal bad certificate.
```

但是检查证书是完整的，证书内容都是正确的。

这个证书验证错误的可能原因是？

- a、系统时钟正确，但证书过了有效期
- b、使用不支持的浏览器
- c、证书在有效期内，但系统时钟错误，系统时钟设在有效期内
- d、证书在过了有效期，系统时钟非当前时间，而是配置在证书的有效期内

答案：bc

5. 客户有一台 usg6000，远端 pc 想实现通过 l2tp over ipsec 接入访问内网，通过 vpn client 软件拨号不成功。（单选）

1 拨号过程中查看 ike:

```
<USG60000>dis ike sa
```

```
20:54:36 2013/06/19
```

```
Current ike sa number :2
```

```
Conn-id peer flag phase vpn
```

```
40051 unnamed none v1:2 public
```

```
40050 2.2.2.2:12485 rd v1:1 public
```

```
-----
```

2 debug ipsec error:

```
2013-06-19 20:54:21 usg2100 %%01IKE/4/WARNING(1):phase2: security acl mismatch
```

```
-----
```

- a、ACL 配置错误
- b、IPSec 的 IKE 阶段 1 策略配置错误
- c、没有配置 IPSec 策略
- d、HASH 算法不匹配

答案 a

6. 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、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。
- b、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。
- 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。

答案 ad

7. 现网正常运行的 USG 防火墙执行一下配置命令，但仍看到 arp 报文交互，以下哪几条命令需要补充？

```
<USG> system-view
```

```
[USG] info-center enable
```

```
lUSG] info-center source arp channel console debug level debugging
```

```
[USG] info-center console channel console
```

```
<USG> debugging arp packet
```

- a、<USG>terminal monitor
- b、<USG>terminal debugging
- c、<USG>info-center console channel 0
- d、<USG>info-center source default channel 0

答案 ab

8. 为了保证设备正常运行、不受安全威胁，需要对设备进行安全加固，考虑正确的是：

- a、从 untrust、trust、dmz 区域到 local 区域的安全策略只打开 icmp、ssh 登陆、snmp 等端口。
- b、snmpv2 版本和网管通信。
- c、设置 console 密码、并且设置管理员界面的登陆超时时间和认证次数限制。
- d、使用 telnet 协议进行设备管理

答案 ac

9. 下列关于双机热备说法正确的是？

- a、防火墙上行链接路由器，下行链接 2 层交换机，可以采用 ospf+vrmp 方式实现负载均衡。
- b、在链路状态检测打开的情况下，并且来回报文分别经主和备 usg 转发，usg 不开启快速备份，tcp 业务可以顺利通过。
- c、active 组的默认优先级为 65001，standby 组的默认优先级为 65000。
- d、两台设备的物理插卡的槽位号可以不一致。

答案 ac

10. L2TP over IPSec 拨号支持哪几种认证方式？

- a、支持本地认证
- b、LDAP
- c、Radius
- d、TSM
- e、PEAP

答案 ac

11. 防火墙使用 IPSec 功能，需要开放哪些协议和端口？

- a、协议为 AH 和 ESP 的 IP 报文。

- b、源端口为 500 和 4500 的 UDP 报文
- c、目的端口为 500 和 4500 的 UDP 报文。
- d、目的端口为 1701 的 UDP 报文。

答案：abc

12. 某管理员是国内某城市银行信息安全主管，企业今年来业务发展迅猛，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、商业银行信息技术风险科技指引
- c、ISO2700X 信息安全系列
- d、信息系统安全等级保护

答案：d

13. 华为 NIP5000 产品是基于签名的安全防范

- a、true
- b、false

答案：a

14. 在双机热备组网中，如果两台防火墙工作于负载分担方式下，不支持 utm 功能。如果两台防火墙工作于主备备份方式下，支持 utm 功能。

- a true b、false

答案：b

15. 防火墙诊断转发类故障手段有哪些？

- a、报文失踪

- b、Debug ip Packet
- c、基于 5 元组的丢包统计
- d、纤细丢包分类统计
- e、查看会话表

答案：bcde

16. 根据《GB / T 22240-2008 信息安全技术信息系统安全等级保护定级指南》信息系统按照不同级别共分为五级，其中五级的保护能力包括：（单选）

- a、
- b、
- c、
- d、为定义

答案：d

17. MPLS Spoke-Hub 的组网中，在 Hub-PE 与 Spoke-PE 之间采用什么路由协议交互路由？

- a、EBGP
- b、IBGP
- c、OSPF
- d、RIP

答案 b

18. 某公司的出口网关双链路分别接入不同的运营商，并有以下需求：用户能够通过两个运营商访问 internet，当通往两个运营商的链路都工作正常的情况下，流量全部由主链路(isp1)转发，当主链路发生故障时，流量全部由备链路(isp2)转发，以下选项正确的是？（单选）

主链路地址 g0/0/2 为 200.1.1.1，网关 200.1.1.8 备链路地址 g0/0/3 为 234.1.1.1，网关 234.1.1.8

a、[USG] ip-link check enable

```
[USG] ip-link 1 destination 200.1.1.8 mode icmp
```

```
[USG] ip-link 2 destination 234.1.1.8 mode icmp
```

b、[USG] ip-link check enable

```
[USG] ip-link 1 destination 200. 1.1.8 mode icmp
```

```
[USG] ip-link 2 destination 234. 1.1.8 mode icmp
```

```
[USG] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/2 200.1.1.8  
preference 30 track ip-link 1
```

```
[USG] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/3 234.1.1.8  
preference 20 track ip-link 2
```

c、[USG] ip-link check enable

```
[USG] ip-link 1 destination 200. 1.1.8 mode icmp
```

```
[USG] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/2 200.1.1.8  
track ip-link 1
```

```
[USG] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/3 234.1.1.8
```

d、[USG] ip-link check enable

```
[USG] ip-link 2 destination 234.1. 1.8 mode icmp
```

```
[USG] ip route-staic 0.0.0.0 0.0.0.0 GigablEthernet 0/0/2 200.1.1.8  
preference 20
```

```
[USG] ip route-staic 0.0.0.0 0.0.0.0 GigablEthernet 0/0/3 234.1.1.8  
preference 30 track ip-link 2
```

e、[USG] ip-link check enable

```
[USG] ip-link 1 destination 200.1. 1.8 mode icmp
```

```
[USG] ip route-staic 0.0.0.0 0.0.0.0 GigablEthernet0/0/2 200.1.1.8  
preference 20 track ip-link 1
```

```
[USG] ip route-staic 0.0.0.0 0.0.0.0 GigablEthernet0/0/3 234.1.1.8  
preference 30
```



答案：e

19. 使用 802.1x 认证方案一般要求终端安装特定的客户端软件，对于客户端软件的大规模部署，可采用的方案有哪些？

- a、启用 guest vlan，让用户在 guest vlan 能获取安装包。
- b、在交换机上配置 free-rule 和 web 推送功能，向用户推送安装包。
- c、通过 u 盘相互拷贝安装包。
- d、由管理员每个用户安装。

答案 ab

20. 在异常流量清洗方案中自动引流是指检测设备检测到流量异常后上报管理中心，管理中心自动生成引流任务，并自动下发引流任务到清洗设备，一般需要哪种具体的引流技术实现自动引流？（单选）

- a、BGP 引流
- b、静态路由引流
- c、策略路由引流
- d、GRE 引流

答案 a

21. 关于 SACG 设备接入网络的方式，如下描述正确的是？

- a、SACG 设备要求与终端二层互通
- b、SACG 通常侧挂在核心交换机设备上，采用策略路由方式引流。
- c、SACG 支持旁挂在非华为的设备上。
- d、SACG 设备要求与 Agile Controller 二层互通

答案：bc

22. 在 usg 状态检测防火墙上，如果管理员设置安全策略从 trust 到 untrust 的数据报文为 permit，而反方向的数据报文安全策略为 deny，那么最终的结果是：

- a、trust 区域内的终端可以主动向 untrust 区域内的终端发起连接，即使是 untrust 返回的报文也可以正常通过。
- b、untrust 区域内的终端不能主动向 trust 区域内的终端发起连接，但是 trust 区域内返回的报文可以正常通过。
- c、trust 区域内的终端可以主动向 untrust 区域内的终端发起连接，但是 untrust 返回的报文不可以正常通过。
- d、untrust 区域内的终端不能主动向 trust 区域内的终端发起连接，只能被动接受 trust 区域内的用户发起的连接。

答案：abd

23. 虚拟防火墙技术原理说法正确的是：

- a、不同的虚拟防火墙有相同的路由表，因此在不同的虚拟防火墙上不支持地址重叠。
- b、虚拟防火墙和根防火墙不能访问。
- c、每个虚拟防火墙系统可以支持 trust、untrust、dmz、local 等安全区域，接口灵活划分和分配。
- d、虚拟系统资源独立分配，安全业务独立提供，支持 vpn 多实例。

答案 cd

24. 在如图的组网中，在 Web 服务器未配置访问外网的缺省网关，为保证外网用户通过 NAT server 正常访问 Web 服务器，以下对防火墙的配置规划哪一项是正确的： DMZ (web server) 192.168.1.5——192.168.1.1 (FW) 202.20.1.5——2.2.2.5 (internet 用户) Untrust web 服务器内网真正 ip 为 192.168.1.5，外网 ip 为 202.20.1.5

- a、需要在防火墙配置 DMZ 到 Untrust 方向的源 NAT，让 Web 服务器可以访问外网，这样 Web 服务器回应报文才能返回到外网用户。
- b、需要在防火墙上配置 nat server，保证外网用户能够通过访问 202.20.1.5 访问 web 服务器。
- c、需要在防火墙上配置 Untrust 到 DMZ 方向的源 NAT，将外网用户访问 Web 服务器的数据包 of 的源地址转换为 192.168.1.1。
- d、需要在防火墙上为外网用户配置 des-nat，将访问的 web 服务器公网地址转换成内网地址。

答案 bc

25. 华为 usg 防火墙中，内容过滤包含哪些功能？

- a、文件内容过滤
- b、应用内容过滤
- c、文件扩展名过滤
- d、邮件过滤

答案 ab

26. 在防火墙上使用 nat 地址池时，nat 地址池地址与外网出接口 ip 不在同一个网段时，需要在下一跳路由器上配置到地址池的路由。

- a、true
- b、false

答案：a

27. 网络上一台服务器近期响应非常慢，通过查看其运行状态，发现其 cpu 和内存占用比率很高，但这些 tcp 会话连接中数据传输量很小或几乎没有数据传输，针对此问题现象的下述判断，请选择出最佳一项：（单选）

- a、服务器正受到 SYN flood 攻击。
- b、服务器正受到 http post 慢速攻击。
- c、服务器正受到 udp flood 攻击。
- d、服务器正受到 tcp 欺骗攻击。

答案：b

28. 当 pc 收到一个分片包如下图所示，根据如下包信息，以下选项正确的是？

IdenCficaCon: 0x0cae (3246)

flags: 0x01 (more fragments)

Fragment offset: 0

Time to live: 128

Protocol: icmp (1)

- a、还有后续 ip 分片
- b、三层 ip 头部的标志位是 1
- c、ip 头部的协议号是 2
- d、偏移位是 0

答案：abd

29. 双机热备份组网时，根据此配置 pc2 发出的 arp 请求 ip 10.100.30.8 的 mac，  
以下哪个选项是正确的？（单选）

PC2 连接防火墙的 g0/0/2 接口，NGFW\_A 为主，NGFW\_B 为备。

```
Sysname NGFW_A
```

```
Hrp enable
```

```
Hrp interface g0/0/3
```

```
#
```

```
Interface g0/0/1
```

```
Ip address 192.168.10.2 255.255.255.0
```

```
Vrrp vrid 1 virtual-ip 192.168.10.1 active
```

```
#
```

```
Interface g0/0/2
```

```
Ip address 10.100.30.2 255.255.255.0
```

```
Vrrp vrid 2 virtual-ip 10.100.30.1 active
```

```
#
```

```
Nat address-group 1
```

```
Section 0 10.100.30.8 10.100.30.9
```

```
#
```

```
Nat-policy
```

```
Rule name trust_to_untrust
```

```
source-zone trust
```

```
desCnaCon-zone untrust
```

```
source-address 192.168.10.0 24
```

```
action nat address-group 1
```

a、NGFW\_A 用 VMAC 响应此 ARP

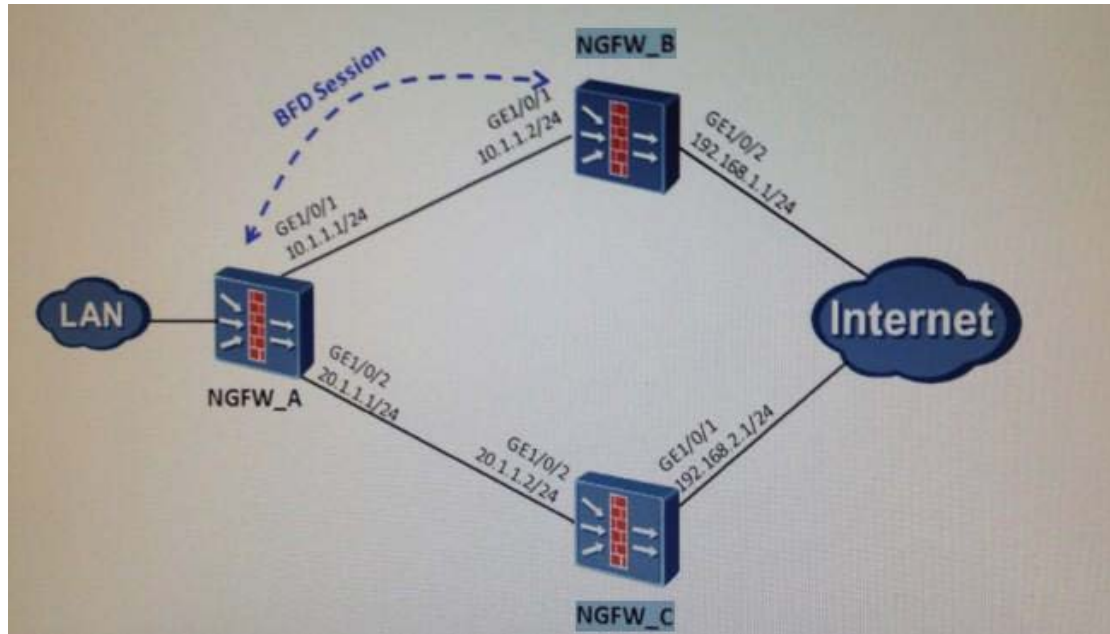
b、NGFW\_B 用 VMAC 响应此 ARP

c、NGFW\_A 用接口的 MAC 响应此 ARP

d、NGFW\_B 用接口的 MAC 响应此 ARP

答案: c

30. NGFW\_A 与 NGFW\_B, NGFW\_A 与 NGFW\_C 分别配置静态路由。NGFW\_A->NGFW\_B 为主链路, NGFW\_A->NGFW\_C 为备份链路, 要求主链路出现故障时能够快速将流量切换到备份链路上, 主链路恢复能够切换到主链路上, 以下配置正确的是哪个?



a、[USG\_A]bfd

```
[USG_A] bfd ab bind peer-ip 10.1.1.2
```

```
[USG_A-bfd-session-ab] discriminator local 10
```

```
[USG_A-bfd-session-ab] discriminator remote 20
```

```
[USG_A-bfd-session-ab] commit
```

```
[USG_A] ip route-static 0.0.0.0 0 10.1.1.2 track bfd-session ab
```

```
[USG_A] ip route-static 0.0.0.0 0 20.1.1.2 preference 100
```

b、[USG\_A]bfd

```
[USG_A] bfd ab bind peer-ip 10.1.1.2
```

```
[USG_A-bfd-session-ab] discriminator local 10
```

```
[USG_A-bfd-session-ab] discriminator remote 20
```

```
[USG_A-bfd-session-ab] commit
```

```
[USG_A] ip route-static 0.0.0.0 0 10.1.1.2
```

```
[USG_A] ip route-static 0.0.0.0 0 20.1.1.2 preference 100 track  
bfd-session ab
```

c、[USG\_B]bfd

```
[USG_B] bfd ab bind peer-ip 10.1.1.1
```

```
[USG_B-bfd-session-ab] discriminator local 20
```

```
[USG_B-bfd-session-ab] discriminator remote 10
```

```
[USG_B-bfd-session-ab] commit
```

d、[USG\_B]bfd

```
[USG_B] bfd ab bind peer-ip 10.1.1.1
```

```
[USG_B-bfd-session-ab] discriminator local 10
```

```
[USG_B-bfd-session-ab] discriminator remote 20
```

```
[USG_B-bfd-session-ab] commit
```

答案：ac

31. 关于防火墙 NAPT 技术，以下描述错误的是？（单选）

- a、NAPT 是一种利用第四层信息来扩展第三层地址的技术。
- b、NAPT 理论上可以实现 65535 个私有地址共享一个公网地址访问公网。
- c、NAPT 将源 IP 地址和源端口号都进行了转换。
- d、防火墙配置 NAPT 时，安全策略应该匹配地址转换后的 IP 地址。

答案：d

32. 某局点做信语音(TCP)业务出现延时较大的故障，延时达到 3 秒. 防火墙作为其出口 NAT 网关，配置了 easy-ip 的 nat 方式(单出口)，关闭了链路状态检测，TCP 老化时间为 30 秒，业务流量较小，到语音服务器的会话数接近 5 万. 通过会话可以看到大量的单向访问语音服务器的报文. 造成这一故障的原因及解决方案正确的是？

- a、TCP 会话老化时间太短，防火墙新建会话比较耗时。
- b、防火墙会话老化后，新的连接做 NAT 后的端口与原来和服务器建立连接的端口不一致，导致服务器没有响应，需要客户端超时后再重新建立连接才能发送数据。
- c、解决方案可以将 TCP 老化时间增加到 600 秒。
- d、如果链路不存在来自回路路径不一致，可以开启链路状态检测功能，老化时间默认可以解决这一问题。

答案: abc

33. IKEv1 和 IKEv2 的区别, 下面描述正确的是?

- a、IKEv2 支持 EAP 认证, IKEv1 不支持。
- b、NAT 穿越都是 IKEv1 和 IKEv2 的可选功能。
- c、IKEv1 和 IKEv2 都是用 initial\_contact 来同步本端和对端的 sa。
- d、针对用户认证 ikev1 使用 ike\_auth 交换, IKEv2 使用 x\_auth 交换。
- e、IKEv2 兼容 IKEv1 协议。

答案: ab

34. 在 agile controller 的解决方案中, USG 用语硬件 SACG 接入认证, 根据以下信息:

```
<USG6700>display right-manager role-id rule
Advanced acl 3099,5rules,not binding with vpn-instance
Acl's step is 1
Rule 1000 permit ip (1280 times matched)
Rule 1001 permit ip destination 172.18.11.211.0 (581 times matched)
Rule 1002 permit ip destination 172.18.11.213.0 (77 times matched)
Rule 1003 permit ip destination 172.19.0.0 0.0.255.255 (0 times matched)
Rule 1004 deny ip (507759 times matched)
```

- a、逃生通道已经被开启
- b、用户进入认证后域
- c、用户进入认证前域
- d、用户进入隔离域

答案 d

35. 在 NGFW 中, 若要使用 RBL 黑名单, 网络管理员需要配置一下哪些关键选项?



- a、DNS 服务器
- b、应答码
- c、RBL 服务器 IP 地址
- d、SMTP 服务器 IP 地址

答案：ab

36. 防火墙工作在主备方式的双机热备, 内网服务器提供网页服务, 外网用户访问时经常出现访问速度慢或无法访问的现象. 内网用户访问正常. 可能有哪些原因?

- a、没有开启 Ospf Cost 调整。
- b、业务来回路径可能不一致, 未启用会话快速备份。
- c、tcp-mss 值设置不对。
- d、备份通道故障, 导致部分会话备份失败。

答案：ad

37. 下列哪些是 USG 防火墙支持的 IKE 加密算法?

- a、des-cbc
- b、aes-cbc128|192|256
- c、md5
- d、RSA

答案：abd

38. 关于 portal 认证流程的正确的说法是? (单选)

- a、portal 认证流程只用在 web 认证中。
- b、服务器针对一个终端的 portal 认证只会给一个 portal 设备发送认证消息。
- c、交换机收到 portal 上线消息, 会给 radius 服务器发送 radius 认证请求。
- d、portal 认证流程中不会携带安全检查的结果信息

答案：a

39. 对于已注册的 usb 存储设备，如果管理员限定该设备只能由指定人员使用，那么该设备只能在指定终端上使用；如果管理员没有配置该 usb 存储设备的授权规则，则任何人都不能使用该设备。

a、true

b、false

答案：b

40. USGA g0/0/2 (30.1.1.2) ———— (30.1.1.1)g0/0/2 USGB 某网络采用如上拓扑，并 USGA 和 USGB 建立 BFD，但是发现 BFD 会话无法 Up，下面最有可能的原因是？（单选）

```
<USGA>display bfd session all
```

Local	Remote	Peer IP	Address	Interface	Name	State	Type
60	20	30.1.1.1		G0/0/2		Down	static

```
<USGB> display bfd session all
```

Local	Remote	Peer IP	Address	Interface	Name	State	Type
60	20	30.1.1.2		G0/0/2		Down	static

a、未绑定出接口的 BFD 会话

b、BFD 会话配置没有提交

c、BFD 会话两端的标识符不对应

d、BFD 会话一端配置了 shutdown 命令

答案：c

41. 移动办公员工通过 L2TP over IPSec 隧道接入总部，关于规划部署说法正确

的是:

a、总部 USG 网关 Security ACL 应该是

```
[USG] acl 3000
```

```
[USG-acl-adv-3000] rule permit udp source-port eq 1701
```

b、由于 ikev1 无法分配地址给远程用户，因此必须通过 l2tp 实现地址分配。

c、l2tp 一般使用 NAS-Initialized 模式。

d、不能使用 NAT 穿越功能。

答案: ab

42. 异常流量清洗系统的部署建议正确的是:

a、旁挂部署或直路部署在网络出口处

b、管理服务器对网络设备的监控 telnet

c、管理服务器通过 snmp 协议向网络设备下发策略。

d、检测中心和清洗中心向采集器上报日志。

答案: ad

43. L2TP over ipsec 的报文封装为: (单选)

a、IP 头+ESP 头+UDP 头+L2TP 头+ppp 头+加密 PPP 负载+ESP 报尾+Auth 报尾

b、IP 头+UDP 头+ESP 头+L2TP 头+ppp 头+加密 PPP 负载+ESP 报尾+Auth 报尾

c、ESP 头+IP 头+UDP 头+L2TP 头+ppp 头+加密 PPP 负载+ESP 报尾+Auth 报尾

d、IP 头+ESP 头+L2TP 头+ppp 头+加密 PPP 负载+ESP 报尾+Auth 报尾

答案: a

44. 某客户使用多个分支设备和总部 USG A 设备做 ipsec 对接，采用点到多点 ipsec 子策略方式建立 VPN，多个分支都是固定 IP 地址，大多数分支到总部 ipsec 链路都可以正常通信. 并且内网(分支到总部)之间可以互相通信，唯独其

中一个分支的内网 PC 和总部内网之间不能正常通信，但是 ipsec VPN 隧道已经协商成功，可能有哪些原因？

- a、总部没有达到故障分支的回程路由。
- b、两端的 ipsec 提议算法不一致，导致报文无法加密。
- c、acl 范围配置错误
- d、可能一端使用 ikev2 协商，一端使用 ikev1 协商。

答案：ac

45. 关于 802.1x 认证的触发机制，以下描述正确的有？

- a、802.1x 认证触发只能由客户端主动发起。
- b、802.1x 认证只能由认证设备（如 802.1x 交换机）发起。
- c、802.1x 客户端可以组播或广播方式触发认证。
- d、认证设备可以以组播或单播方式触发认证。

答案：cd

46. 应用行为控制不包括哪些功能？（单选）

- a、post 操作
- b、代理上网
- c、hIps 加密控制
- d、hIp 文件上传

答案：c

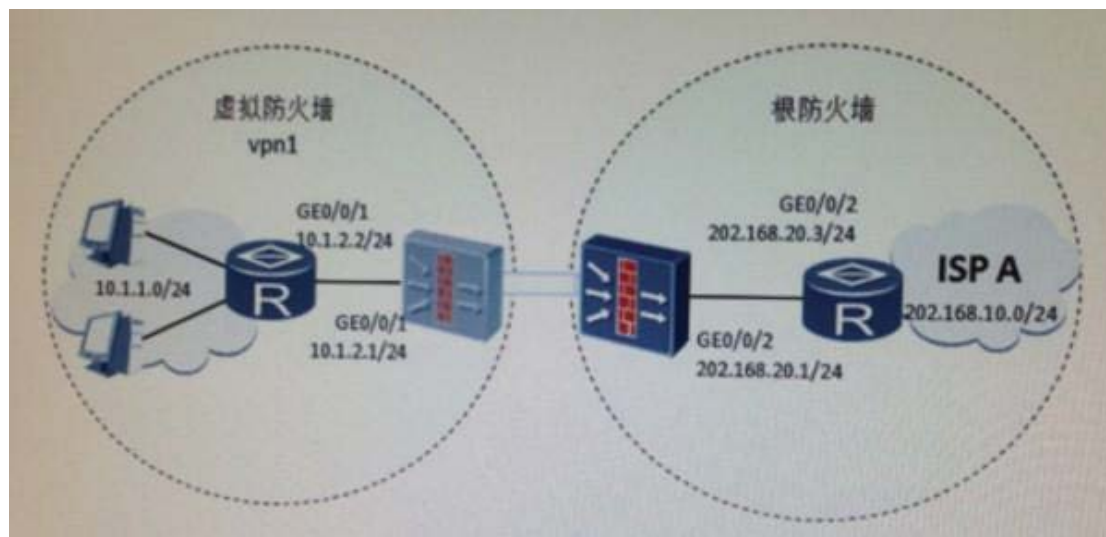
47. 下列关于双机热备说法正确的是？（单选）

- a、抢占操作总是只有在故障恢复或者主 USG 重启完成后才会启动。
- b、抢占时间设置过长，会导致 USG 出现故障时，不是立即执行切换操作。
- c、hrp auto-sync config . 会手动使主 USG 上配置的命令备份到备 USG 。

d、两台 USG 上心跳线对应接口的 vrrp vrid 可以不一致。

答案: a

48. 如图所示需要配置虚拟防火墙 vpn1 与根防火墙之间的路由示例, 下列哪一项是正确的: (单选)



a、

```
[USG-vpn1]ip route-static 202.168.10.0 255.255.255.0 public
[USG]lp route-static 10.1.1.0 255.255.255.0 vpn-instance vpn1 10.1.2.2
[USG]lp route-static 202.168.10.0 255.255.255.0 202.168.20.3
```

b、

```
[USG-vpn1]ip route-static 202.168.10.0 255.255.255.0 192.168.20.3
[USG]lp route-static 10.1.1.0 255.255.255.0 vpn-instance vpn1 10.1.2.2
```

c、

```
[USG-vpn1]ip route-static 202.168.10.0 255.255.255.0 202.168.20.3
vpn-instance vpn1
[USG]lp route-static 10.1.1.0 255.255.255.0 vpn-instance vpn1 10.1.2.2
```

d、

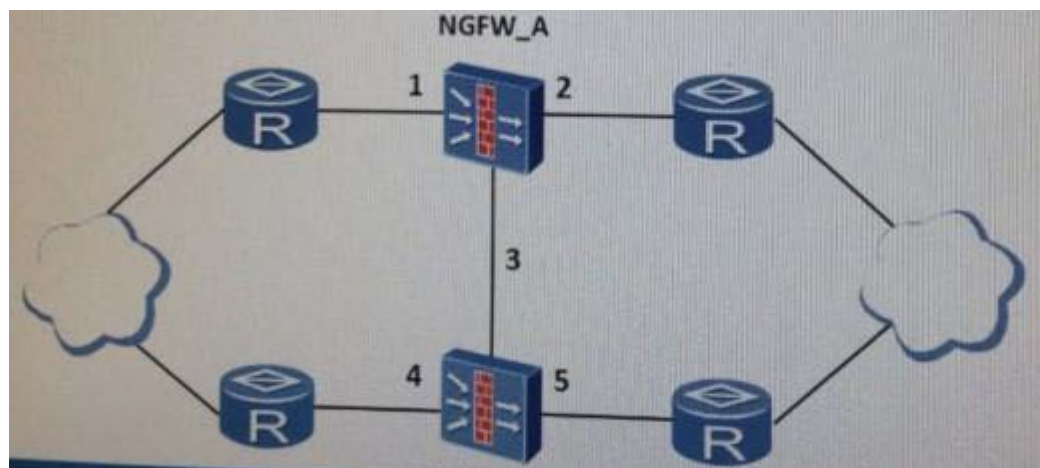
```
[USG-vpn1]ip route-static 202.168.10.0 255.255.255.0 202.168.20.3
public
[USG]lp route-static 10.1.1.0 255.255.255.0 10.1.2.2
```

答案:a

49. 某网络由于网络升级新硬件的 USG，需要替换图中双机热备 USG\_A 和 USG\_B.

在不影响业务的前提下，如何进行升级：（单选）

USG\_A 为 acCve 设备. USG\_B 为 Standby 设备.



以下正确正确割接步骤是？

1. 依次将 5，4 线路连接至新 USG\_B.
  2. 依次将 1，2，3 线路从旧 USG\_A. 连接至新 USG\_A.
  3. 将新 USG\_B 和新 USG\_A 上电，并将配置导入.
  4. 在 USG\_B 输入 undo hrp enable. 并依次切断 4， 5， 3， 线路.
  5. 调整路由花费. 使流量全部通过 USG\_B .
  6. 新 USG\_A 和新 USG\_B 输入 hrp enable. 调整路由花费，使符合预期。
- a、3-4-1-5-2-6 b、3-4-1-2-6-5 c、4-1-5-3-2-6 d、3-4-5-1-2-6

答案: a

50. 在防火墙做了如下配置：

```
[USG-policy-security] rule name trust_local
[USG-policy-seurity-rule-untrust_local] source-zone trust
[USG-policy-seurity-rule-untrust_local] destination-zone local
[USG-policy-seurity-rule-untrust_local] source-address 192.168.5.2 32
```

```
[USG-policy-seurity-rule-untrust_local] destination-address  
192.168.5.1 32  
[USG-policy-seurity-rule-untrust_local] service http  
[USG-policy-seurity-rule-untrust_local] service telnet  
[USG-policy-seurity-rule-untrust_local] action permit
```

请选择以下正确的描述是：

- a、允许防火墙通过 Telnet 方式登录 192.168.5.1 的设备。
- b、允许 192.168.5.2/24 这个 IP 地址通过 Telnet 方式登录防火墙。
- c、允许防火墙通过 Web 方式登录 192.168.5.1 的设备。
- d、允许 192.168.5.2/24 地址段通过 Web 方式登录防火墙。

答案：bd

51. 关于 IPSec 隧道的生命周期下列说法正确的是？

- a、IPsec sa 生命周期可以以流量进行计算。
- b、两端的生命周期配置必须一致。
- c、IPsec 隧道到达生命周期后会重新协商一个新的隧道。
- d、软超时时间是 SA 的生命周期截止时间，硬超时时间是在生命周期截止前启动协商新 SA 的时间。

答案：ac

52. 在如下图的防火墙单点登录认证流程中包括以下的主要环节：（单选）

- a. 在 AD 服务器上查找用户组信息
- b. 设备已经创建在线用户列表，用户直接访问外部资源
- c. 发选用户名用户组等信息到设备
- d. 用户请求认证
- e. 主动给 AD 监控服务发送消息(用户名，用户 IP 地址)
- f. 服务器认证通过

请选择字母与数字的正确对应关系？

PC 用户——ADserver——AD 监控服务程序——防火墙设备

---1--->

<--2----

---3-->

<--4---

---5-->

-----6----->

a、1-d-2-f-3-e-4-a-5-c-6-b

b、1-d-2-f-3-a-4-e-5-c-6-b

c、1-d-2-e-3-a-4-f-5-c-6-b

d、1-d-2-e-3-f-4-a-5-c-6-b

答案:a

53. 在网络出口防火墙上查看会话表信息如下：（单选）

[USG]display firewall session table verbose

15:11:25 2013/12/18

Current total sessions: 40

Http vpn:public→ public

Zone: trust→untrust Il: 00:10:00 Lez: 00:08:59

Interface: Gigabitethernet0/0/1 NextHop: 58.251.159.1

MAC:00-0f-e2-a2-a2-61

< --packets: 144 byte:6340 -->packets:74 byte:3951

192.168.100.28: 1036[58.251.159.112:2048] --> 111.206.79.100:80

以下描述**不正确**的是：

a、防火墙接口 GigabitEthernet0/0/1 属于 untrust 区域。

b、防火墙出接口（**下一跳的 MAC 地址**）MAC 地址为 00-0f-e2-a2-a2-61 。

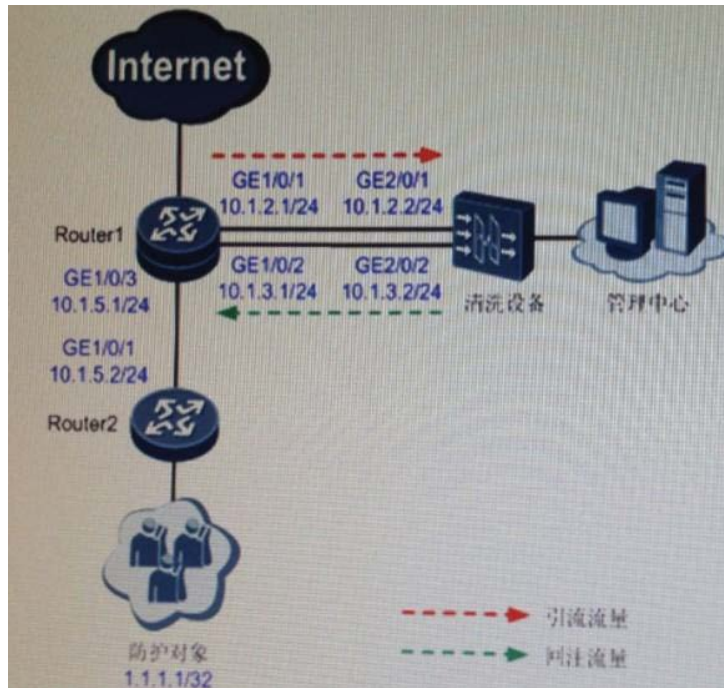
c、内网 192.168.100.28 主机与外网 111.206.79.100 建立 http 连接。



d、NAT 转换后的地址为 58.251.159.112 。

答案: b

54. 根据以下组网，以下配置点说法正确的是：（单选）



- a、如果静态路由回注，必须配置 `firewall ddos bgp-next-hop fib-filter`
- b、建议在清洗设备上，持续启用路由环路检测功能 `anti-ddos loop-check`
- c、如果使用策略路由回注，必须在 `GigabitEthernet2/0/2` 接口上应用策略路由
- d、为了使清洗设备发送探测流量，必须配置相应静态路由。

```
[AntiDDoS] ip route-static 0.0.0.0 0 10.1.2.1
```

答案: a

55. 以下哪些应用不能仅仅使用包过滤机制实现安全防护？

- a、www 服务
- b、telnet 服务
- c、zp 服务
- d、H.323

答案:cd

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

答案: ad

57. agile controller 中配置数据库镜像失败，以下哪些描述是正确的？

- a、这类问题主要是因为 dbmirror 共享出错导致的。
- b、需要各数据库镜像服务器关闭了 windows 的防火墙。
- c、确保主数据服务器、镜像数据库服务器、见证数据库服务器彼此能使用 IP 地址互相访问共享文件夹(只要以 IP 地址能即可)。
- d、如果是服务器未加入域，则需要运行 TsmMaintainTool.bat 工具修改镜像工具的配置参数。

答案: ab

58. 防火墙的双机热备份的命令备份功能中不可以备份以下哪些命令？

- a、IPS 命令
- b、转发策略命令
- c、路由表
- d、ip 地址配置

答案：cd

59. 双机热备组网中，两台 USG 上的管理组状态均为 active，可能的原因是？（单选）

- a、心跳线的物理线路发生故障。
- b、没有配置备份通道接口
- c、没有设置快速会话备份
- d、设置了长的抢占延时

答案：a

60. IKEV1 第一阶段协商不成功，需要检查哪些信息，可能是由哪些原因引起的？

- a、检查物理链路是否正常。
- b、查看 ike debug 信息和 udp500 端口的报文会话统计数。
- c、检查 ACL 配置是否匹配
- d、检查 IPSec proposal 参考配置

答案：ab

61. 针对 NIPS5000 和 NIP5000D 的功能比较，以下哪些是正确的：

- a、NIP5000 一般是直路接入。NIP5000D 一般是旁路接入。
- b、NIP5000 可以直接阻断动作。NIP5000D 必须通过防火墙联动，实现阻断的动作。
- c、NIP5000 可以针对应用协议流量进行分析、限流和阻断；NIP5000D 只能对应用流量进行分析
- d、关于 DDOS，NIP5000 支持自动防御和不防御两种模式，而 NIP5000D 只能支持自动防御。

答案：ab

62. 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 zp
destination-address 192.168.5.3 32
action permit
rule name untrust to dmz2
source-zone untrust
destination-zone dmz
service service-set http_8080
destination-address 192.168.5.2 32
action permit
```

# 以下说法不正确的事：

- a、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 zp 连接。
- b、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。
- c、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 zp 连接。
- d、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。

答案：cd

63. 某客户网络拓扑如图所示. PC 和 FW 之间建立 12TP 隧道. PC 作为客户端. FW 作为 LNS 端，管理员完成配置后，发现 12TP 隧道无法建立成功。

在用户视图下执行命令 debug 12tp packet 打开调试开关. 看到如下 debug 信息：

```

USG %%01L2TP/8/L2TDBG(d): L2TP::Check SCCRQ MSG Type 1
USG %%01L2TP/8/L2TDBG(d): L2TP::Parse AVP Protocol version: 100
USG %%01L2TP/8/L2TDBG(d): L2TP::parse AVP Framing capability: 1
USG %%01L2TP/8/L2TDBG(d): L2TP::Parse AVP Bearer capability, value:0
USG %%01L2TP/8/L2TDBG(d): L2TP::parse AVP Firmware revision, value:1280
USG %%01L2TP/8/L2TDBG(d): L2TP::Parse AVP Host name,
value:maple-54b168e59
USG %%01L2TP/8/L2TDBG(d): L2TP::request host isn't in the define l2tp
group , refuse the requested
USG %%01L2TP/8/L2TDBG(d): L2TP::clear calls on tunnel ID=1 Reason=1

```

如图:

```

PC-----internet-----FW-----router-----PC
2.2.2.2 10.1.1.0 10.1.2.0

```

答案: c (l2tp group)

64. 某企业网络中存在多个真实服务器对外提供 FTP 服务. 配置负载均衡功能, 保证流经 USG 的流量负载均衡, 管理员希望通过检测真实服务器状态. 实现每台服务器的负载比例与权值比例相同. 下列合适的配置是: (单选)

a、

# 配置真实服务器加入负载均衡组

```

[USG-slb] group test
[USG-slb-group] metric least-conneticon
[USG-slb-group-test] add server 1
[USG-slb-group-test] add server 2
[USG-slb-group-test] add server 3
[USG-slb-group-test] quit

```

b、

# 配置真实服务器加入负载均衡组

```
[USG-slb] group test
[USG-slb-group] metric roundrobin    简单轮询
[USG-slb-group-test] add server 1
[USG-slb-group-test] add server 2
[USG-slb-group-test] add server 3
[USG-slb-group-test] quit
```

c、

# 配置真实服务器加入负载均衡组

```
[USG-slb] group test
[USG-slb-group] metric srchash      源地址 hash
[USG-slb-group-test] add server 1
[USG-slb-group-test] add server 2
[USG-slb-group-test] add server 3
[USG-slb-group-test]quit
```

d、

# 配置真实服务器加入负载均衡组

```
[USG-slb] group test
[USG-slb-group] metric weightrr
[USG-slb-group-test] add server 1
[USG-slb-group-test] add server 2
[USG-slb-group-test] add server 3
[USG-slb-group-test] quit
```

答案: d

65. 在 USG 防火墙链路状态检功能开启的情况下，当 TCP 会话的首个分片报文和第二个分片报分发送间隔大于会话表老化时间，会话表将会删除，其后续报文将会重新创建会话表。

a、TRUE   b、FALSE

答案：b

66. 在使用 SSL VPN 网络扩展功能时，虚拟 IP 地址也可以和设备内网接口的 IP 地址设置为同一网段，如果虚拟 IP 地址池与内网接口 IP 地址不在同一网段，请在设备上手动配置到地址池的路由，出接口为内网接口，下一跳为内网接口的下一跳。

- a、TRUE
- b、FALSE

答案：a

文档说明：网络扩展地址池可以和设备内网接口的 IP 地址设置为同一网段。如果不在同一网段，需要在设备上手工配置到达地址池的路由，出接口为设备内网接口。

67. L2TP over ipsec 的场景中，如果 LNS 分配的地址池和内网在相同网段，需要配置哪些命令才能保证分支和内部服务器之间的通信正常？（多选）

- a、内网接口配置 arp 代理
- b、地址池的每个地址配置明细路由
- c、使能 l2tp more exam enable
- d、使能 l2fwdfast enable

答案：ab

68. 以下哪些选项属于访客管理的范畴？（考试有可能会反问，单选）

- a、访客账号创建
- b、访客账号审批
- c、访客页面定制
- d、访客使用账号进行认证

- e、访客在注册页面进行注册
- f、访客上网行为审计

答案：abcde

69. 本地 license 无法激活的可能原因有哪些？

- a、ESN 不匹配
- b、设备无法连接 sec.huawei.com
- c、license 中的功能项已过期
- d、设备没有配置激活密码

答案：ac

70. IS027000 系列包括多个安全标准，其中哪些安全标准与信息安全技术风险管理相关：（单选）

- a、IS027002
- b、IS027003
- c、IS027004
- d、IS027005

答案：d

71. 关于 Agile Controller 的集中部署式和分布式部署场景，以下描述正确的是：

- a、如果大部分终端用户集中在一个地区办公，少数终端用户在分支机构办公，推荐集中式部署。
- b、如果大部分终端用户集中在一个地区办公，少数终端用户在分支机构办公，推荐分布式部署。
- c、如果终端用户分散在不同的地域办公，则推荐采用分布式组网方案。
- d、如果终端用户分散在不同的地域办公，则推荐采用集中式组网方案。



答案：ac

72. 采用如下哪种 ipsec 模式和封装方式可以引用于 IPSEC NAT 穿越的应用场景？（单选）

- a、IPSEC 隧道模式+ESP 封装
- b、IPSEC 隧道模式+AH 封装
- c、IPSEC 传输模式+ESP 封装
- d、IPSEC 传输模式+AH 封装

答案：a

73. 华为防火墙反垃圾邮件功能使用的是 RBL 方法，其对 DNS 服务器有哪些要求？

- a、这个 DNS 必须是不被 DNS 劫持的服务器。
- b、这个 DNS 必须是使用递归算法的服务器。
- c、这个 DNS 必须是使用迭代算法的服务器。
- d、不指定 DNS 服务器时则使用系统模式下配置的 DNS 服务器。

答案：ab

74. 根据以下状态信息判断：USG 设备使用了哪项 QoS 技术：（单选）

```
[USG_A] display qos policy interface tunnel 1
```

-----

Policy : dscp

classifier : default-class

rule(s) : if-match any

behavior : be

-----

classifier : server

rule(s) : if-match acl 2001

behavior : server

-----  
classifier : telephone

rule(s) : if-match acl 2003

behavior : telephone  
-----

a、GTS b、CAR c、WRED d、CBWFQ

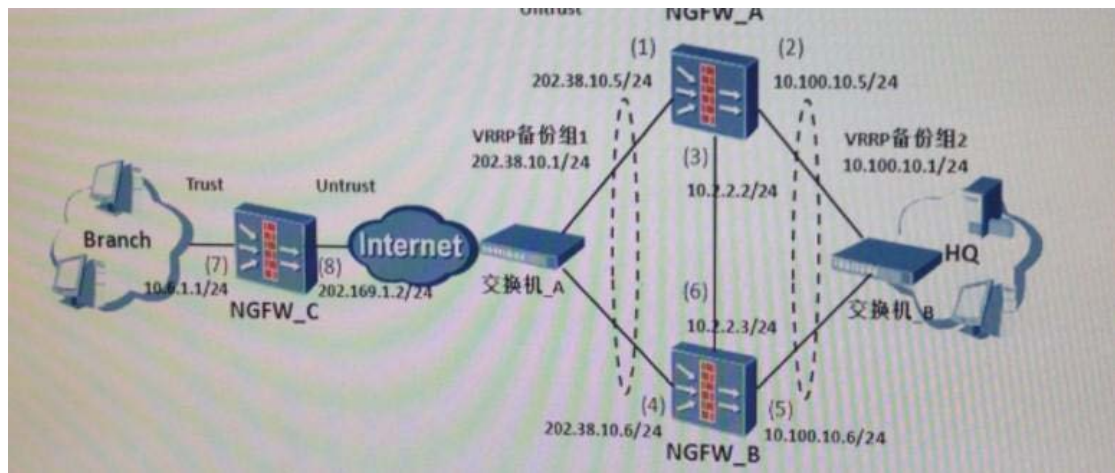
答案:d

75. 对于一些大的 ip 数据包, 为了满足链路层的 MTU (Maximum Transmission Unit)的要求, 需要传送的过程中对其进行分片, 分成几个 IP 包。在每个 IP 包头中有一个偏移字段和一个拆分标志(MF)。其中偏移字段指出了这个片段在整个 IP 包中的位置. 如果攻击者截取 IP 数据包后, 把偏移字段设置成不正确的值, 接收端在收到这些分拆的数据包后, 就不能按数据包中的偏移字段值正确组合出被拆分的数据包, 这样, 接收端会不停的尝试, 以至操作系统因资源耗尽而崩溃. 此种攻击方法是什么? (单选)

- a、teardrop 攻击
- b、winNuke 攻击
- c、TCP 报文标志位攻击
- d、IP 分片报文攻击

答案: a

76. 总部和分支机构之间使用 ipsec 隧道通信, 为了确保数据在 internet 上传输的安全性. 管理员使用的双机热备功能提高总部和分支机构通信的可靠性, 避免总部的一台 USG 出现故障造成分支机构无法访问总部, 根据以下组网图, 下列说法正确的是?



- a、只能使用主备备份方式下的 ipsec 双机热备。
- b、只能采取 esp 和 tunnel 模式封装。
- c、USG\_A, USG\_B 必须开启 NAT 穿越。
- d、USG\_A, USG\_B 和 USG\_C 只需要配置 internet 的路由，无需在 USG\_A, USG\_B 和 USG\_C 配置分支内网和总部内网间路由。

答案：abd

77. IKEv1 和 IKEv2 的区别，下面哪些描述是正确的？

- a、建立 IKE SA 和 IPsec SA，IKE v2 使用 4 条消息，IKEv1 主模式使用 9 条消息。
- b、IKEv2 可以借助 aaa 服务器分配私网 ip 地址，IKEv1 无法提供此功能。
- c、IKE sa 的完整性算法仅 IKEv1 支持。
- d、IKEv1 默认支持 DPD，只要一端配置 DPD，另外一端就可以响应 DPD 报文，IKEv2 不可以。

答案 ab

文档说明：

开启“DPD 状态检测”后，设备会自动发送 DPD 报文检测对端是否存活，以便及时拆除错误的隧道。

可以有两种检测方式：

周期性发送：“检测时间间隔”内未收到对端报文则发送一次 DPD 报文。

需要时才发送：“检测时间间隔”内未收到对端报文，且本端需要通信时发送一次 DPD 报文。

对于使用 IKEv1 的隧道，此功能需要两端同时开启或关闭。在发送 DPD 报文后，在“重传时间间隔”内未收到回应报文，会被记录为一次失败时间。当连续发生五个失败事件后，则认为对端已经失效，设备会自动拆除隧道。

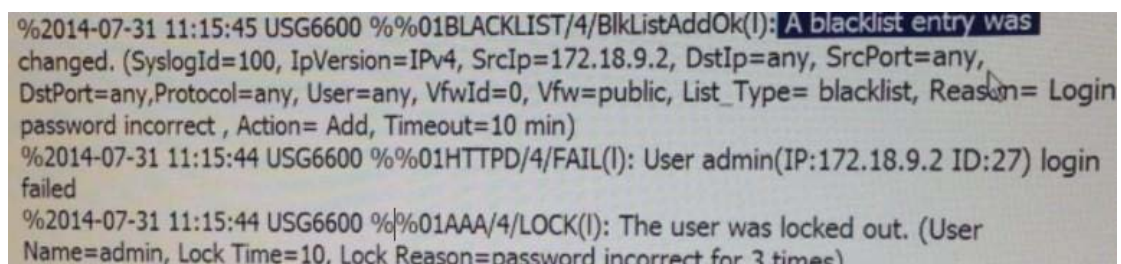
对于使用 IKEv2 的隧道，此功能只需一端开启就可检测成功。发送 DPD 报文的间隔时间不按照“重传时间间隔”，而是以指数形式增长（发送 DPD 报文 1 后，隔 1 秒发报文 2，再隔 2 秒发报文 3，再隔 4 秒发报文 4，依次类推），一直到间隔 64 秒后发送报文 8。如果还收不到回应报文，在报文 8 发送后的 128 秒时，隧道会被自动拆除。整个过程耗时约半个小时。

78. 在双机热备的组网下，业务接口工作在三层，上下行连接交换机；

- a、VGMP 管理组状态为 active，优先级为 65001，VGMP 管理组状态为 standby，优先级为 65000。
- b、当 USG1 和 switch3 的链路中断的时候，VGMP 管理组优先级降低 2。
- c、当发生主备状态切换时，active 设备对外发布 vrrp 备份组虚拟 ip 地址的免费 arp，standby 设备会发布免费 arp。
- d、USG1 整机发生故障或者重启时，USG2 连续 5 次收不到 USG1 发送的 vgmpp hello 报文，则认为 USG1 已经发生故障，立即切换为主用设备。

答案：ab

79. USG 防火墙日志信息输出如下：



```
%2014-07-31 11:15:45 USG6600 %%01BLACKLIST/4/BlkListAddOk(I): A blacklist entry was changed. (SyslogId=100, IpVersion=IPv4, SrcIp=172.18.9.2, DstIp=any, SrcPort=any, DstPort=any, Protocol=any, User=any, VfwId=0, Vfw=public, List_Type= blacklist, Reason= Login password incorrect, Action= Add, Timeout=10 min)
%2014-07-31 11:15:44 USG6600 %%01HTTPD/4/FAIL(I): User admin(IP:172.18.9.2 ID:27) login failed
%2014-07-31 11:15:44 USG6600 %%01AAA/4/LOCK(I): The user was locked out. (User Name=admin, Lock Time=10, Lock Reason=password incorrect for 3 times)
```

以下描述正确的是：

- a、用户只能在 2014-07-31 11:30:45 之后才能再次登陆设备。
- b、用户尝试登陆三次，均输错密码，用户账户被锁。
- c、用户尝试登陆三次，均输错密码，用户 ip 地址被锁。
- d、用户将 ip 地址更换为 172.18.9.3 后可再次尝试登陆。

答案：cd

80. 以下关于 BFD 描述正确的是？

- a、BFD 协议规定发送间隔在接收间隔单位是毫秒级。
- b、可以和策略路由、OSPF、DHCP、FRR、静态路由等联动。
- c、根据 icmp 回显请求或 arp 请求，实现链路探测。
- d、BFD 可以检测非直链链路。

答案：bd

81. 关于 SGCG 内建 ACL，以下描述正确的是？

- a、缺省 acl 规则组号可以任意指定。
- b、缺省 acl 规则组号只能是 3099。
- c、由于 SACG 需要使用 ACL3099-3999 来接收 TSM 系统下发的规则，所以在配置 TSM 联动之前先保证这些 ACL 不被其他功能引用。
- d、管理员需要自定义 ACL（编号 3100-3999）规则来控制不同接入用户的权限。

答案：bc

82. 在配置防火墙安全策略时，以下哪一条配置命令正确的表示匹配 192.168.10.0 网段发出的数据包？（单选）

- a、source-address 192.168.10.0 0.0.0.255
- b、source-address 192.168.10.0 255.255.255.0
- c、destination-address 192.168.10.0 0.0.0.255

d、 destination-address 192.168.10.0 255.255.255.0

答案：a

83. mac 认证适用于以下哪种情况？（单选）

- a、办公用 windows 主机
- b、测试用 linux 主机
- c、移动客户端，如智能手机等
- d、网络打印机

答案：d

84. 防火墙上查看会话表信息如下：

```
[USG] display firewall session table verbose
```

```
icmp vpn_public -->public
```

```
Zone: trust --> untrust TTL: 00:00 :20 Lez: 00:00:15 Interface:
```

```
Gigabitethernet1/0/4 Nexthop: 2.2.2.2 MAC: 00-00-00-00-00-00
```

```
<--packets: 0 bytes: 0 --> packet: 5 bytes: 420
```

```
192.168.1.2:44012[1.1.1.3:6103] → 2.2.2.2:2048 以下描述正确的是：
```

- a、地址为 192.168.1.2 的设备正在对公网地址 2.2.2.2 进行 ping 测试。
- b、地址为 1.1.1.3 的设备正在对公网地址 2.2.2.2 进行 ping 测试。
- c、防火墙配置的 nat 目的的地址一对一地址映射。
- d、防火墙配置了 NAT 源地址多对一地址映射。

答案：ad

85. 在 Remote access vpn 场景下，远程 pc 使用 Secoway VPN client 和防火墙建立 VPN，下面说法正确的是？

- a、默认使用隧道模式

- b、默认使用传输模式
- c、默认使用 l2tp over ipsec 拨号
- d、默认使用 l2tp 拨号

答案：ad

86. 访问的网页内容中如果包含过滤的内容，结果将是如何？（单选）

- a、显示“无法打开网页”。
- b、显示“网页已经被过滤”。
- c、过滤内容被删除，将不被显示。
- d、过滤内容以“\*”代替。

答案：a

87. 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？（单选）

PC,,,,,,,, (g0/0/1 ) FW (g0/0/2 ) ,,,,,,,,,,Switch

#

```
interface GigabitEthernet 0/0/1
```

```
link-group 1
```

```
interface GigabitEthernet 0/0/2
```

```
link-group 1
```

- a、没有变儿。
- b、Switch 接口地址的 ARP 表将老化失效。
- c、Switch 接口地址的 ARP 表项被立即删除。
- d、防火墙发免费 ARP 给上行设备 Switch 更新 MAC 地址。

答案：c

88. USG 启动 HRP 备份功能后，关键配置命令和会话表状态信息会实时间步备份到备用设备的配置命令和状态信息有哪些？

- a、转发策略命令
- b、攻击防范命令
- c、虚拟防火墙命令
- d、接口配置命令
- e、会话表

答案：abce（问的是 USG，不是 NGFW）

89. NGFW 能够对哪些协议进行传输的文件进行病毒扫描和相应处理？

- a、HTTP(Hypertext Transfer Protocol), 超文本传输协议。
- b、FTP(File Transfer Protocol), 文件传输协议。
- c、SNMP (Simple Network Management Protocol ) , 简单网络管理协议。
- d、POP3 (Post Office Protocol 3), 邮局协议版本 3。
- e、HTTPS(Hypertext Transfer Protocol Security) 安全超级文本传输协议

答案：abd

90. 以下哪些报文可以是单播报文：

- a、VRRP Hello。 b、VGMP Hello。 c、HRP Hello。 d、OSPF Hello。 e、BFD。

答案：bcde

91. 华为 USG 防火墙，在双机热备组网下(如图)。PC 通过 SSH 无法登陆备防火墙 FW2 的外网口实 IP 地址， 查看主备防火墙上对应的会话如下，分析下对于这个故障下列哪些说法是对的？

```
HRP_A<E1000-1>display firewall session table verbose source inside  
192.168.22.151 tcp VPN: public -> public
```



```

Zone: trust ->local TTL:00:00:05 Lez: Cmeout
Interface: G0/0/1 Nexthop: 192.168.22.122 MAC: 00-22-a1-06-b3-cb
<-- packets:1 bytes:48 --> packets:0 bytes:0
192.168.22.122:22<--192.168.22.151:4354
HRP_S<E1000-1>display firewall session table verbose source inside
192.168.22.151 tcp VPN: public -> public
Zone: trust ->local TTL:00:00:05 Lez: Cmeout
Interface: G0/0/1 Nexthop: 192.168.22.122 MAC: 00-22-a1-06-b3-cb
<-- packets:1 bytes:48 --> packets:1 bytes:44
192.168.22.122:22<--192.168.22.151:4354
a、由于 SSH 客户端在登陆过程中支持报文重传。
b、PC 登陆备防火墙 FW2 的时候存在来回路径不一致。
c、由于关闭了 hrp mirror session enable 可能导致问题。
d、由于关闭链路状态检测功能 undo firewall session link-state check 导
致的问题。

```

答案: bc

92. 在 Portal 认证中，交换机上必须配置的 portal 参数有？

- a、Portal 服务器 IP
- b、Portal 页面 URI
- c、shared-key
- d、portal 协议版本
- e、设备侦听 portal 协议报文的端口号

答案: abc

93. USG 作为总部网关，出差用户需要使用 internet 建立 vpn 隧道，访问总部资源，且出差用户不需要安装任何拨号软件，以下哪种 vpn 技术最合适：（单选）

a、SSL VPN b、IPsec VPN c、L2tp d、GRE

答案：a

94. 关于防火墙 NAT server 配置命令中的 no-reverse 参数描述正确的是：

a、配置不带 no-reverse 参数的 nat server ，当公网用户访问服务器时；防火墙能将服务器的公网地址转换成私网地址；当服务器主动访问公网时，防火墙也能将服务器的私有地址转换成公网地址。

b、配置带参数 no-reverse 的 nat server ，设备只将公网地址转换成私网地址。不能将私网地址转换成公网地址。

c、配置带参数 no-reverse 的 nat server ，当公网用户访问服务器时。防火墙将服务器的公网地址转换成私网地址；当服务器主动访问公网时，防火墙也能将服务器的私网地址转换成公网地址。

d、配置不带参数 no-reverse 的 nat server. 设备只将公网地址转换成私网地址，不能将私网地址转换成公网地址。

答案：ab

95. 以下哪些功能模块可结合 IP-link 功能使用？

a、DHCP

b、路由策略

c、VRRP

d、OSPF

答案：abc

96. 在 linux 主机上经过 USG 防火墙 **tracert** 某个目的 IP 地址时，发现从防火墙这一跳开始都显示\*号，但确认网络又是没有问题的，请问为了使防火墙本身以及防火墙之后的设备真实显示 ip 地址，在防火墙上下列哪些事必须配置的？

- a、允许经过防火墙转发 **udp** 报文的包过滤策略。
- b、允许经过防火墙转发的 **icmp** 报文的包过滤策略。
- c、undo ip ttl-expires enable 关闭 ICMP 超时报文功能
- d、undo firewall defend tracert enable 命令用来关闭 Tracert 报文攻击防范功能

答案: **ad**

97. IPS（入侵检测）故障需要排查哪几个方面？

- a、是否使能 IPS 全局开关
- b、是否配置 IPS 策略，并应用到域间
- c、配置的策略是否提交编译
- d、查看是否配置 IPS 黑名单
- e、是否配置了覆盖签名

答案: **ace**

98. 防火墙在运行 GRE 时，tunnel 接口必须配置下面哪三个参数？

- a、tunnel 的协议号为 GRE
- b、GRE 的校验和使能
- c、tunnel 的源 ip 地址
- d、tunnel 的目的 ip 地址
- e、key

答案: **acd**

**99.** 某企业有如下需求：Trust 区域中内网用户的是 192.168.1.0/24 网段. 可以访问 Internet. 一共有 50 台主机（192.168.1.1-192.168.1.50），总带宽为 500M，以下规划合理的是：

- a、整体带宽限制为 500M，每个 IP 的最大带宽是 12M。
- b、整体带宽限制为 400M，每 IP 的最大带宽是 12M。
- c、整体带宽限制为 500M，192.168.1.1-192.168.1.50，每 ip 的最大带宽是 12M。
- d、整体带宽限制为 500M，保证带宽是 500M，每 ip 的最大带宽是 10M。

答案：c

100. 防火墙针对接入用户可采用以下几种方式实现用户身份认证：

- a、NTLM 认证
- b、radius 认证
- c、HWTACACS 认证      华为对 TACACS 协议的扩展
- d、LDAP 认证
- e、PEAP 认证

答案：bcd

101. 防火墙部署在无线用户的移动终端和 WAP 网关之间，移动终端在 trust 区域，WAP 网关在 untrust 域，并做了如下配置：（单选）

```
[USG] acl 3000
[USG-acl-adv-3000] rule permit ip 202.10.10.2 0
[USG-acl-adv-3000] quit
[USG] firewall zone trust
[USG-zone-trust] destination-nat 3000 address 200.10.10.2
[USG-zone-trust] quit
```

以下描述正确的是：

- a、该配置还可应用到服务器地址映射场景下
- b、命令 firewall zone trust 应该修改为 firewall interzone trust untrust outbound
- c、防火墙访问 202.10.10.2 网关地址的数据包的目的地址转换为 200.10.10.2

d、命令 `firewall zone trust` 应该修改为 `firewall interzone untrust trust`

答案: c

102. 公司通过互联网从事电子商务, 该企业网络交易平台支持信用卡在线结算, 为满足支付卡行业数据安全标准 PCI-DSS, 该企业要部署华为公司防火墙、VPN、日志设计等安全产品, 目前项目已经完成方案设计和产品采购, 正式上线商用前还需要进行哪些必要的工作?

- a、对网内已有系统进行风险评估。
- b、对方案和产品进行黑盒渗透测试。
- c、对方案和产品进行白盒渗透测试。
- d、对方案和产品进行安全加固。

答案: abd

103. 以下哪几项攻击方式属于网络攻击?

- a、构造错误的 TTL 值的数据包, 导致设备处理异常。
- b、构造大量的 syn 报文, 导致主机资源耗尽。
- c、构造 tcp 标志位异常的数据包, 导致主机处理异常。
- d、构造 ip 分片标志位错误的数据包, 导致主机处理异常。

答案: ad

104. 在防火墙上进行地址集配置时, 配置命令如下:

```
[sysname] ip address-set abc type object  
[sysname-object-address-set-abc] address 192.168.1.1 0  
[sysname-object-address-set-abc] address 192.168.2.0 mask 24
```

以下描述正确的是:

- a、地址集 abc 匹配 192.168.1.1 主机和 192.168.2.0/24 网段。

- b、地址集 abc 中可以通过嵌套地址集的方法增加匹配的网段。
- c、address 192.168.2.0 mask 24 可以使用命令 address 192.168.2.0 0.0.0.255 替代。
- d、地址集 abc 创建成功后，不能再直接增加新的地址或地址段，必须重新创建一个地址集。
- e、地址集中的地址不能有相互包含或重叠的关系。

答案：ac

105. 企业内网用户通过 USG 防火墙上网时，某个 URL 已经加入黑名单，但用户仍然可以访问，造成 URL 过滤功能失效的可能原因是什么？

- a、没有升级远程 URL 名单。
- b、没有将 URL 过滤策略应用在相应的域间方向上。
- c、没有开启 url 远程查询功能。
- d、没有提交 url 过滤配置文件。

答案：bd

106. 比较邮件内容过滤与 RBL 过滤两个技术，说法正确的是：

- a、邮件内容过滤支持对 Webmail 或通过 SMTP/POP3 传输的邮件进行过滤。
- b、RBL 过滤只过滤 POP3 传输的邮件。
- c、邮件内容过滤对邮件内容进行过滤。
- d、RBL 过滤根据 SMTP 连接的目的 ip 地址进行过滤。

答案：ac

107. 在网络流量很大的时候，如果不希望下游网路因为上游发送数据流量过大而造成拥塞或大量报文的直接丢弃，可以在上游设备的出接口限制并缓存流量，使这类报文以比较均匀的速度向外发送，这种技术可以是：

- a、GTS
- b、Car
- c、WRED
- d、CBWFQ

答案：a

108. 使用 USG6600 搭建的双机热备主备方式的组网应用中, 需要重点关注哪几方面的问题?

- a、来回路径应该一致
- b、快速会话备份
- c、NAT 地址与 VRRP 应该绑定
- d、主备的接口 ip 地址应该一致

答案：ac

109. NIP5000 设备支持将部分接口设置为 IDS 模式。

- a、true
- b、flase

答案：a

110. 以下关于 ip-link 的描述哪个是错误的?

- a、提供**毫秒级**的快速可达性检测。
- b、能够为静态路由、vrrp 等多个业务模块提供可达性检测。
- c、根据 ICMP 回显请求或 arp 请求, 实现链路探测。
- 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。

答案: ad

111. 某网络由于网络升级新的 USG\_A 和 USG\_B 的软件版本, 在不影响业务的前提下, 如何进行升级; USG\_A 为 active 设备, USG\_B 为 standby 设备:

1. 通过 telnet 或 ssh 方式登录 USG\_B, 操作如下:

hrp enable

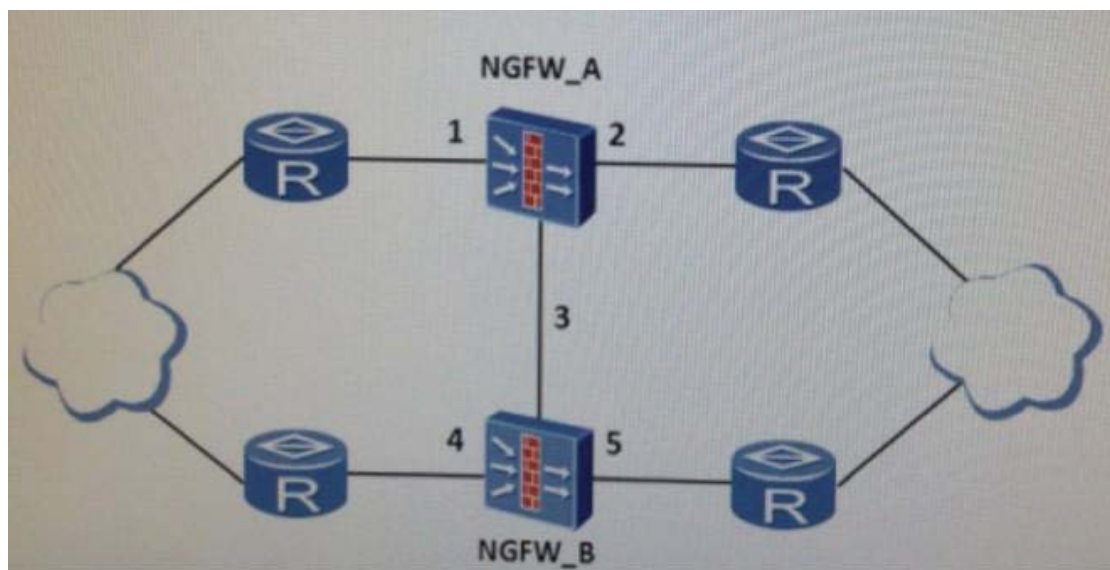
2. 通过 telnet 或 ssh 方式登录 USG\_A, 操作如下:

Undo hrp enable

3. 在 USG\_B 执行 undo hrp enable 命令, 然后升级 USG\_B 的软件版本, 并重启 USG\_B 设备。

4. 升级 USG\_A 的软件版本, 并重启 USG\_A 设备。

5. 测试 USG\_B 业务是否正常。



a、3-2-1-5-4 b、2-3-1-4-5 c、3-2-4-1-5 d、1-5-3-2-4

答案: a

112. 对于 NAT server 的描述, 正确的是? (单选)

a、如果 NAT server 的公网地址与对应的公网接口地址在同一网段时, 可以不用配置黑洞路由。

b、如果 NAT server 的公网地址与对应的公网接口地址不在同一网段时, 可以不



用配置黑洞路由。

c、如果 NAT server 的公网地址为接口地址时，如果配置该地址的黑洞路由，会导致对防火墙自身的业务访问异常。

d、在虚拟防火墙上不可以对根防火墙的用户配置 NAT server。

答案：a

113. 以下哪几项是关于状态检测防火墙转发原理的正确描述：

a、非首包转发基于会话表，匹配会话表才能转发。

b、ICMP 报文不会进行状态检测。

c、处理 udp 协议包时为该 udp 数据流建立连接。

d、防火墙作为二层设备部署时不支持状态检测机制。

e、基于 tcp 连接三次握手进行会话状态检测。

答案：ace

114. 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、开启设备虚拟化功能

d、部署 vpn

e、开启 DDOS 功能

答案：abde

115. 关于防火墙 ip-link 特性，以下描述错误的是：（单选）

a、防火墙向指定的目的地址连续发送 icmp 报文，连续 3 秒（默认）未收到 icmp echo reply，则认为该链路故障。

b、防火墙连续向目标网段发送 arp 请求报文，收到 arp 应答报文，则认为该链

路正常。

c、arp 探测方式只支持探测直链链路。

d、icmp 探测方式可以用于探测跨网段的链路可靠性。

答案：b

116. 以下哪些功能是受 license 控制的

a、url 白名单过滤功能、url 黑名单过滤功能、url 自定义分类过滤功能。

b、url 远程分类服务查询

c、IPS

d、内容过滤

答案：bc

117. 关于 mtu 和 pmtu 说法正确的是？

a、mtu (maximum transfer unit) 指的是在网络中能够传输的最大数据报文的大小，以字节为单位。

b、设备会在入接口检查 mtu，如果数据包大小超过 mtu 值，将被丢弃。

c、在 ip 网络中，从源地址到目的地址可能会经过具体不同的 mtu 值的接口，其中最大的 mtu 值即为该路径的 pmtu。

d、探测 pmtu 是通过探测获取指定目的 ipv4 地址的 pmtu 值，然后使用 mtu 值来发送报文。

答案：ad

118. 关于统一威胁管理，下列说法正确的是？

a、统一威胁管理设备集成了防火墙，IPS，AV，AS，上网行为管理等功能。

b、解决目前串行设备部署的问题，如一条链路上串联了防火墙设备，ips 设备，av 设备等。

- c、随着 utm 技术的发展，utm 设备逐渐开始完全取代传统防火墙。
- d、用户的使用上，降低了网络设备的管理和投资，网管人员只需要掌握单台设备的使用及管理技巧。

答案：abcd

119. 防火墙支持在哪些接口上配置 ipsec 策略？

- a、普通物理接口
- b、virtual template 口
- c、tunnel 口
- d、dialer 口
- e、virtual ethernet 口

答案：abcde

120. 下面哪些功能属于 ssl vpn 的功能？

- a、端口转发
- b、端口映射
- c、网络扩展
- d、文件代理
- e、web 代理

答案：ace

121. 企业现网一台 zp 服务器（DMZ）向外部（untrust）提供 zp 服务，外网口部署了 usg 防火墙，在 zp 服务器上抓包获取到如下信息：

序号 源地址 目的地址 协议 报文摘要

1	1.1.1.1	192.168.1.2	TCP	3318> 21 [SYN] Seq=0 Len=0 MSS=1460
2	192.168.1.2	1.1.1.1	TCP	21>3318 [SYN,ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	1.1.1.1	192.168.1.2	TCP	3318> 21 [SYN] Seq=1 Ack=1 Win=65535 Len=0
.....				
13	1.1.1.1	192.168.1.2	FTP	Request: PASV
14	192.168.1.2	1.1.1.1	FTP	Response:227 Entering Passive Mode (192,168,1,2,4,162)
15	1.1.1.1	192.168.1.2	TCP	3319>1186 [SYN] Seq=0 Len=0 MSS=1460
16	192.168.1.2	1.1.1.1	TCP	1186>3319 [SYN,ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
17	1.1.1.1	192.168.1.2	TCP	3319>1186 [SYN] Seq=1 Ack=1 Win=65535 Len=0

以下描述正确的是：

- a、zp 服务器 zp 服务为主动模式。
- b、主机 1.1.1.1 与 zp 服务器 192.168.1.2 之间已经正常建立数据通道。
- c、防火墙上会自动生成 server map 表项。
- d、防火墙上须完成 nat-policy 的 nat 正确配置。

答案：bc

122. ssl vpn 网络扩展支持哪几种路由分配模式？

- a、全路由模式
- b、手动模式
- c、自动模式
- d、动态模式
- e、分离模式

答案：abe

123. 下列哪些命令是处理 E1/CE1 问题的时候需要用到的接口环回命令？

- a、loopback
- b、loopback local
- c、loopback remote
- d、test loopback

e、loopback check

答案: bc

124. USG 和 router 建立 site-to-site Isec VPN, 通过以下信息, 下列选项说法可能正确的事?

```
<USG>display ike sa
```

```
Current ike sa number:0
```

```
<USG>display ipsec statistics
```

----- 所有的统计数据数也都为 0

- a、域间包过滤配置错误
- b、NAT 策略干扰 ipsec 保护数据流
- c、IKE 对等体私网路由可达性问题
- d、ipsec protocol 配置不一致

答案: abc

125. 某管理员是国内某大型银行安全技术人员, 部门近期要部署一批网络和安全产品用于在线交易平台, 为保证业务系统稳定正常, 以下哪个方案最适合。(单选)

- a、双机热备
- b、冷热互备
- c、双机热备+冷备
- d、双机负载

答案: c

126. 在异常流量清洗方案中回注是指清洗后的正常流量送回原有链路, 并继续转发到防护对象, 为了配置简单, 并且存在多个回注接口的情况, 需要哪些具体的回注技术实现? (单选)

- a、静态路由回注
- b、策略路由回注
- c、GRE 回注
- d、MPLS LSP 回注

答案：b

127. 下列属于应用层攻击的是：

- a、缓冲区溢出
- b、Teardrop 攻击
- c、smurf 攻击
- d、cc 攻击

答案：ad

128. 根据以下组网，某客户使用了 BGP 引流策略路由回注的方式，在清洗设备上，以下哪个配置是必须的？（单选）

- a、`interface g2/0/2 anti-ddos flow-statistic enable`
- b、`ip route-static 0.0.0.0 0 10.1.3.1`
- c、`firewall ddos bgp-next-hop 10.1.3.1`
- d、`firewall ddos bgp-next-hop fib-filter`

答案：c

129. VGMP 统一管理 VRRP 备份组状态，VGMP 管理组 active 的优先级为 65001，standby 的优先级 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

答案：a

130. 关于 802.1x 和 radius 两种技术的关系，以下描述正确的是？（单选）

- a、802.1x 和 radius 是同一种技术的不同名称。
- b、802.1x 是一个技术体系，它包含了 radius。
- c、802.1x 和 radius 是不同的技术，但经常配合在一起使用，共同完成对终端用户的接入控制。
- d、802.1x 和 radius 是完全不同的两种技术，通常不会一起使用。

答案：c

131. Agile Controller 中 SM 组件的主要功能是什么？

- a、做为 Agile Controller 的管理中心，负责制定总体策略。
- b、做为 Agile Controller 的管理界面，对系统进行配置和监控。
- c、做为 Agile Controller 的管理中心，继承有标准的 radius 服务器、portal 服务器、auth 服务器和 network 服务器。
- d、做为 Agile Controller 的安全协防服务器，负责对 iradar 上报的安全事件进行分析。

答案：ab

132. 对已有有线网络准入控制，推荐采用 SACG 认证方案，其优点是？

- a、不需要改变现网拓扑。
- b、不要求安装客户端。
- c、通过适当的策略配置可以实现故障逃生。
- d、能够支持所有的类型的终端。

答案：ac

133. 某企业新建的园区网中，在某个接入交换机下又普通 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？（单选）

- a、802.1x
- b、portal 认证
- c、mac 认证
- d、mac 旁路认证

答案：d

134. 如图所示攻击，相应的防御方法有：



- a、通过关联的 tcp 协议对用户进行认证。
- b、通过源认证的方法防御。
- c、通过 ttl 检查的方法进行防御。
- d、载和检查防御。
- e、指纹检查防御。
- f、

答案：de



135. URL 过滤处理流程顺序正确的是：（单选）

1. NGFW 将 URL 信息与黑名单进行匹配
  2. NGFW 将 URL 信息与白名单进行匹配
  3. NGFW 将 URL 信息与自定义分类进行匹配。
  4. 启动远程分类查询。
  5. NGFW 将 URL 信息与本地缓存中的预定义分类进行匹配。
- a、12345
- b、43512
- c、21354
- d、12354

答案：c

136. 在 Agile Controller 中，关于屏保策略正确的说法是？

- a、可以检查终端是否启用了屏保
- b、可以检查是否启用了屏保密码
- c、仅支持 windows 操作系统
- d、屏保设置不能自动修复

答案：abc

137. 下面哪些三元组可以唯一标示一个 ipsec sa？

- a、协议号（AH / ESP）
- b、序列号
- c、SPI
- d、目的 ip 地址
- e、端口号

答案：acd

138. 管理员在使用 USG 网管的 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 客户端不影响其他网络资源的访问, 可以直接访问 internet 资源。(单选)

- a、全路由模式的网络扩展
- b、分离模式的网络扩展
- c、手动模式的网络扩展
- d、端口转发

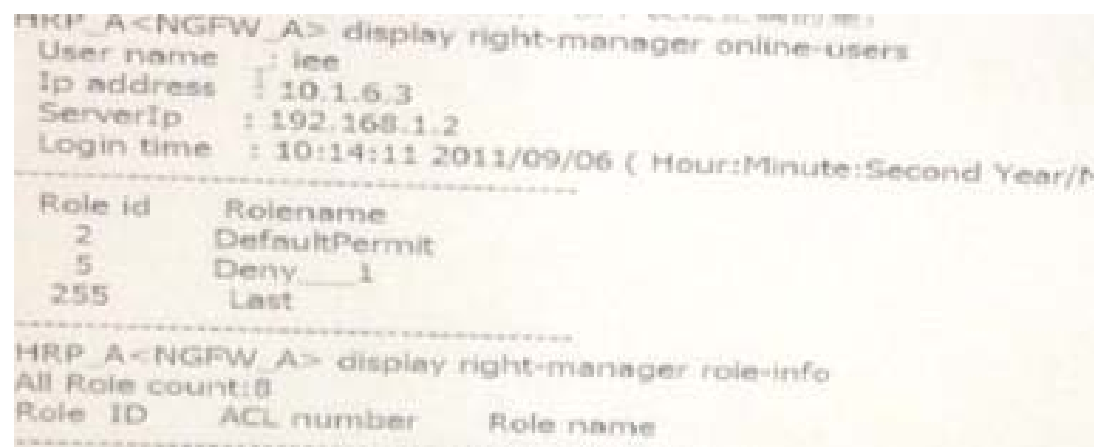
答案: c

139. 防火墙在 diagnose 视图下使用 display diagnostic-information 收集系统诊断信息, 其中不能获取以下哪条命令输出的信息? (单选)

- a、display version
- b、display ip packet
- c、display current-configuration
- d、display history-command

答案: b

140. 某防火墙和 agile controller 联动, 以下说法正确的是: (单选)



```
HRP_A<NGFW_A> display right-manager online-users
User name      : lee
Ip address     : 10.1.6.3
ServerIp      : 192.168.1.2
Login time     : 10:14:11 2011/09/06 ( Hour:Minute:Second Year/Mo:Day)

-----
Role id        Rolename
2              DefaultPermit
5              Deny_1
255            Last
-----

HRP_A<NGFW_A> display right-manager role-info
All Role count:8
Role ID        ACL number    Role name
-----
```

```

Rule 0      3099      default
Rule 1      3100      DefaultDeny
Rule 2      3101      DefaultPermit
Rule 3      3102      Deny_0
Rule 4      3103      Permit_0

Rule 5      3104      Deny_1
Rule 6      3105      Permit_1
Rule 255    3354      Last
Advanced ACL 3099, 4 rules, not binding with vpn-instance
Acl's step is 1
rule 1001 permit ip destination 192.168.1.2 0 (0 times matched)
rule 1002 permit ip destination 192.168.1.3 0 (0 times matched)
rule 1003 permit ip destination 192.168.3.3 0 (0 times matched)
rule 1004 deny ip (0 times matched)

Advanced ACL 3100, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 deny ip (0 times matched)

Advanced ACL 3101, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 permit ip (0 times matched)

Advanced ACL 3104, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 deny ip destination 172.16.1.10 0 (0 times matched)

Advanced ACL 3105, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 permit ip destination 172.16.1.10 0 (0 times matched)

Advanced ACL 3354, 3 rules, not binding with vpn-instance
Acl's step is 1
rule 1 permit ip destination 192.168.1.2 0 (0 times matched)
rule 2 permit ip destination 192.168.1.3 0 (0 times matched)
rule 3 permit ip destination 192.168.3.3 0 (0 times matched)

```

- a、管理员设置缺省禁止规则，在隔离域和后域中的“控制方式”选择“只允许访问列表中的受控域资源，禁止访问其他”使用。
- b、agent 客户端无法访问 192.168.1.2
- c、假设认证后域有台服务器 10.1.1.1，agent 客户端完成安全认证后，防火墙会允许其通过。
- d、防火墙和 agile controller 联动不成功。

答案：c

141. 802.1x 认证中，如果认证点在汇聚层交换机，那么除了 radius、AAA、802.1x 等常规配置外，还需要哪些特殊配置？（单选）

- a、汇聚层和接入层交换机需要开启 802.1x 功能。
- b、接入层交换机需要配置 802.1x 报文透传。

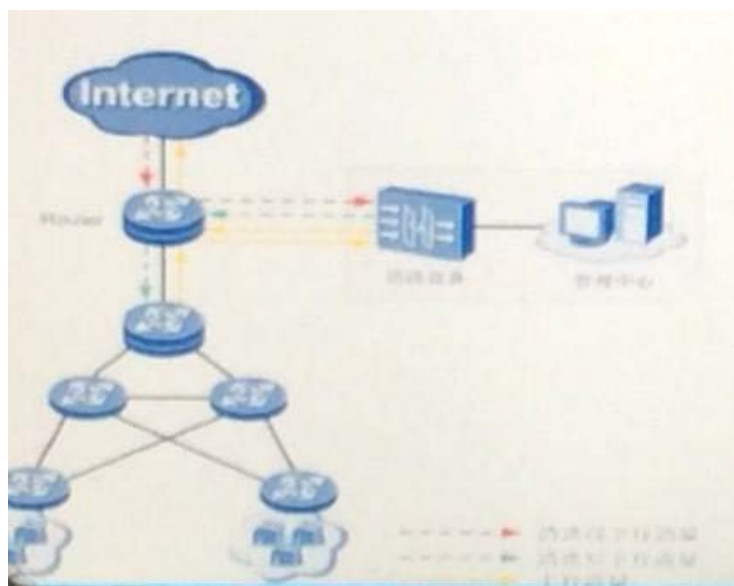
c、汇聚层交换机需要配置 802.1x 报文透传。

d、不需要特殊配置。

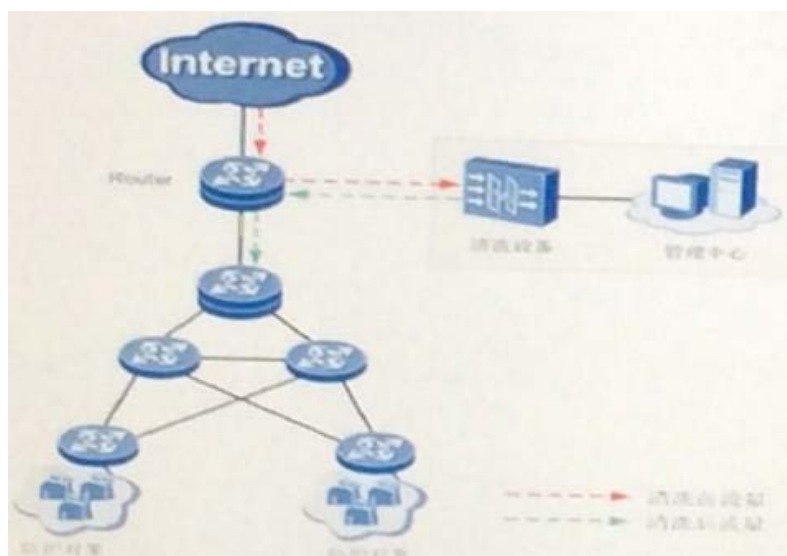
答案：b

142. 某网络将 AntiDdos 清洗设备以旁路方式部署于网络节点处，对牵引到清洗设备的流量进行双向引流清洗。下面组网正确的是：（单选）

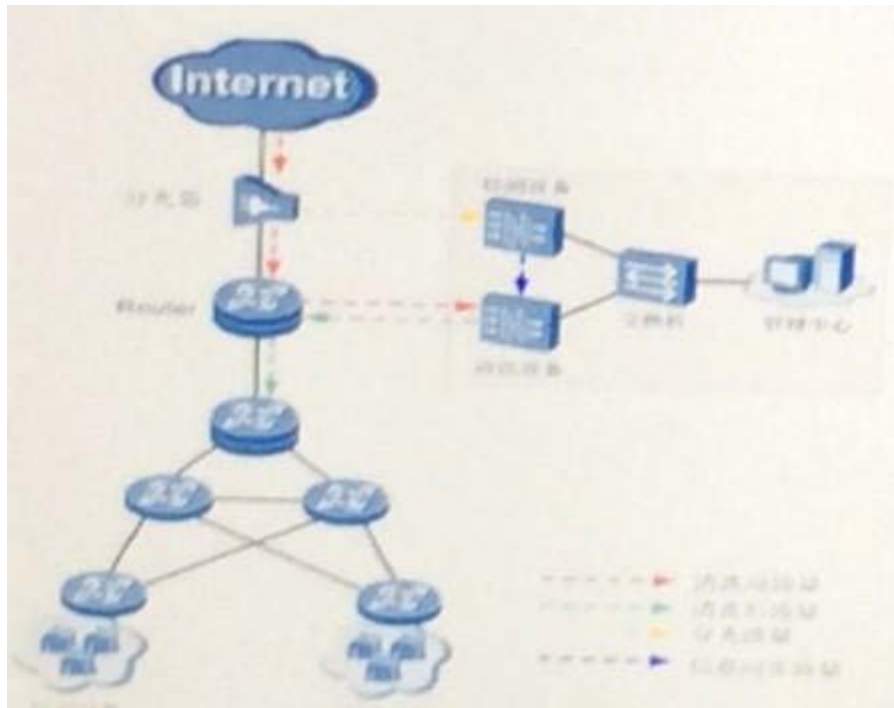
a、



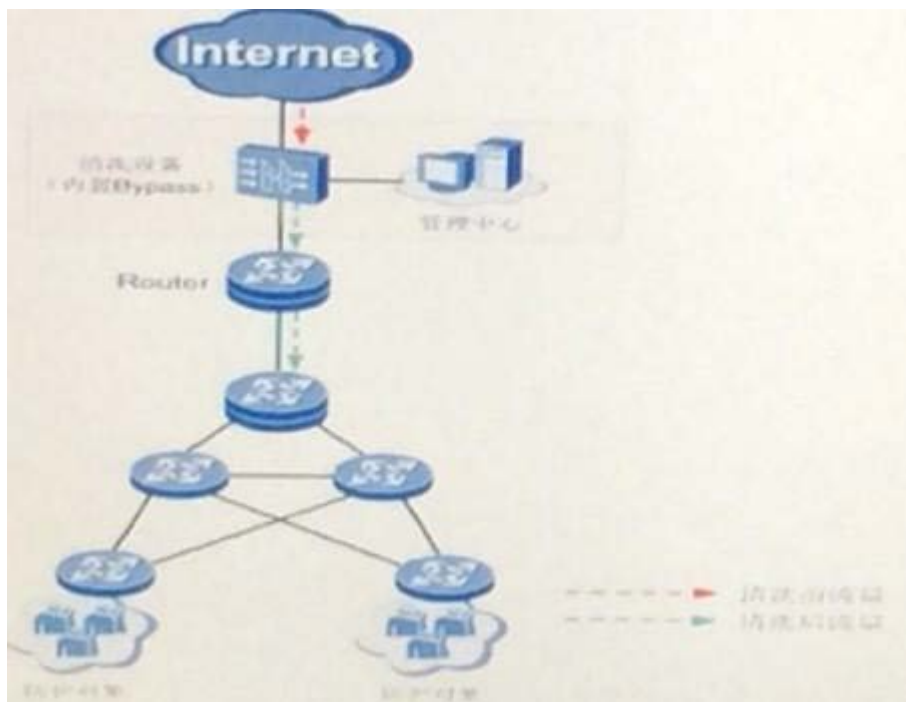
b、



c、



d、



答案：a

143. 如下图所示，在某公司用 USG6000 防火墙作为出口，该公司共有两个出口，运营商 A 和运营商 B 进 行出口负载分担，某工程师部署该防火墙在两个出口同时加入 untrust 域，内网用户则加入了 trust 域，并做了源 NAT 映射。在部署

完之后，发现部分用户上网正常，有部分用户则上网速度很慢，甚至有时上不了网。根据以下信息，请判断如下哪个描述正确？

```

[USG] display firewall session table verbose
http VPN: public --> public
Zone: trust --> untrust TTL: 00:00:10 Left: 00:00:08
Interface: GigabitEthernet0/0/0 NextHop: 41.134.5.49 MAC: F0-DE-F1-69-26-91
<--packets: 9 bytes: 364 -->packets: 9 bytes: 364
10.16.1.20:5246[41.134.5.52:5246] --> 16.8.3.0:80
http VPN: public --> public
Zone: trust --> untrust TTL: 00:10:00 Left: 00:09:59
Interface: GigabitEthernet0/0/1 NextHop: 41.160.30.65 MAC: 00-21-97-cf-22-38
<--packets: 4 bytes: 238 -->packets: 14 bytes: 1640
10.16.1.122:3745[41.134.5.52:3745] --> 2.2.2.2:80
[USG] display ip routing-table
20:56:07 2012/09/20
Route Flags: R - relay, D - download to fib

Routing Tables: Public
Destinations: 5 Routes: 5
Destination/Mask Proto Prio Cost Flags NextHop Interface
0.0.0.0/0 Static 60 0 RD 41.134.5.49 GigabitEthernet0/0/0
0.0.0.0/0 Static 60 0 RD 41.160.30.65 GigabitEthernet0/0/1
10.16.1.1/24 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0

```

- a、可以推断出源 nat 配置是正确的。
- b、该问题是有等价格路由引起的。
- c、该问题与运营商网络稳定性有关。
- d、该问题是用户 pc 导致的。

答案：ab

144.agile controller 的终端安全策略有哪些类型？

- a、检查类策略
- b、加密策略
- c、监控类策略
- d、自定义策略
- e、准入策略

答案：ac

145. 对于已注册的 usb 存储设备，如果管理员限定该设备智能由指定人员使用，那么该设备只能在指定终端上使用，如果管理员没有配置该 usb 存储设备的授权规则，则任何人都不能使用该设备。

- a、true
- b、false

答案：b

### 授权规则管理:

对于已注册的 USB 存储设备，管理员能够限定这些设备只能由指定人员使用（包括指定账号和指定部门的人员），只能在指定终端设备或归属指定设备组的终端设备上使用，或者只能在指定 IP 地址的终端主机上使用，避免其他人员从这些 USB 存储设备中获取重要信息。

前提条件:已注册 USB 存储设备。

背景信息:如果管理员没有配置设备的授权规则，则所有人都能使用该 USB 存储设备。

146. 防火墙 pki 支持的在线申请证书方式是什么？（单选）

- a、http
- b、ldap
- c、Atp
- d、scep
- e、zp

答案: d

147. 802.1x 的认证模式，以下描述正确的有？

- a、802.1x 认证模式分为基于接口和基于 mac 两种。
- b、在同一个接口下，基于端口和基于 mac 两种模式可以同时开启。
- c、从对所有接入用户认证的要求来看，基于 mac 模式比基于端口模式更安全。
- d、从对所有接入用户认证的要求来看，基于端口模式比基于 mac 模式更安全。

答案: ac

148. 关于 udp flood 和 tcp flood 攻击防范说法正确的是:

- a、udp 协议是无连接的，因此无法通过探测实现。
- b、防范 udp flood，通过分析某个主机发送 udp 报文的规律和特征，这个规律

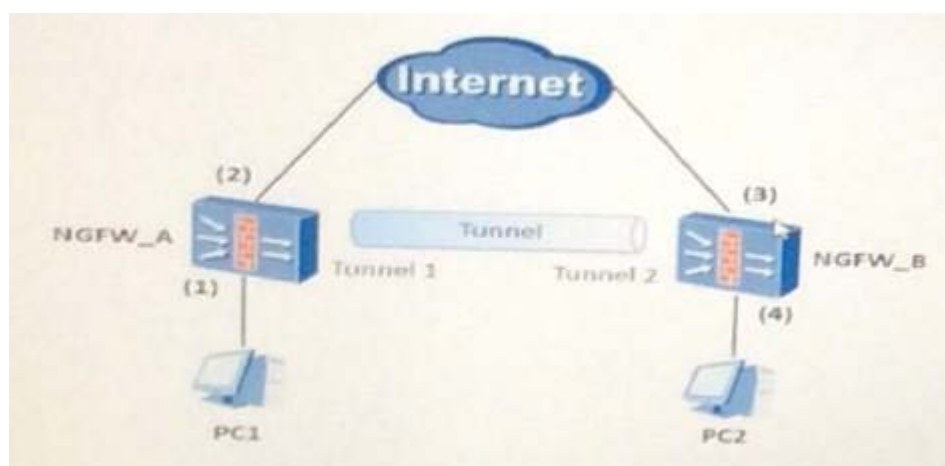
和特征被称为指纹学习。

c、udp 报文的指纹学习功能通过学习报文数据端全部字段。

d、udp 和 tcp 协议可以通过代理技术实现。

答案：ab

148. 如图所示组网，USG\_A 与 USG\_B 之间建立 GRE 隧道，接口 1、4 位于 trust 域，接口 2、3 位于 untrust 域，两个 tunnel 口位于 dmz 域，那么需要打开哪些域间的安全策略，pc1 和 pc2 才能正常访问？



a、trust 《—》 dmz

b、untrust 《—》 local

c、local 《—》 trust

d、dmz 《—》 untrust

答案：ab

149. Anti-DDOS 异常流量清洗解决方案中，关于规划部署建议正确的是：

a、通过基线学习周期学习防护对象中各服务类型的流量基线值，并按照学习任务的设置生成学习结果。

b、优先部署防御模式为自动，待运行一段时间后，Anti-DDOS 工作正常再部署防御模式为手动。



- c、建议在流量较大的场景，建议直路部署。
- d、清洗设备之路部署在企业入口处，同时一般清洗设备内置 bypass 卡，增强方案的可靠性。

答案：ad

150. 以下哪些情况不会出发 802.1x 流程的重新认证？（单选）

- a、处于隔离状态，终端用户点击修复操作（完成严重违规的修复）。
- b、处于隔离状态，终端用户手工进行修复，然后点击注销，再点击认证操作。
- c、处于认证后域状态，Agile controller agent 周期检查终端的安全状态需要被隔离。
- d、处于认证后域状态，用户进行业务系统认证。

答案：a

151. 防火墙采用 web 重定向密码认证时，用户不主动进行认证，而是先进行业务访问，有防火墙将页面重定向至“认证页面”，认证成功后自动跳转到用户之前的页面。

- a、true
- b、false

答案：a

152. 某网络 USG 防火墙的 trust 区域连接终端主机，untrust 区域连接安全控制器，如果使安全控制器能够向 usg 下发规则，必须配置下列哪些安全策略？（单选）

- a、Security-policy  
rule name local\_to\_trust  
source-zone local

```
destination-zone trust
action permit
b、Security-policy
rule name untrust_to_local
source-zone untrust
destination-zone local
action permit
c、Security-policy
rule name to_local
source-zone untrust trust
destination-zone local
action permit
d、Security-policy
rule name untrust_to_local
source-zone untrust
destination-zone local
action permit
rule name local_to_trust
source-zone local
destination-zone trust
action permit
```

答案: b

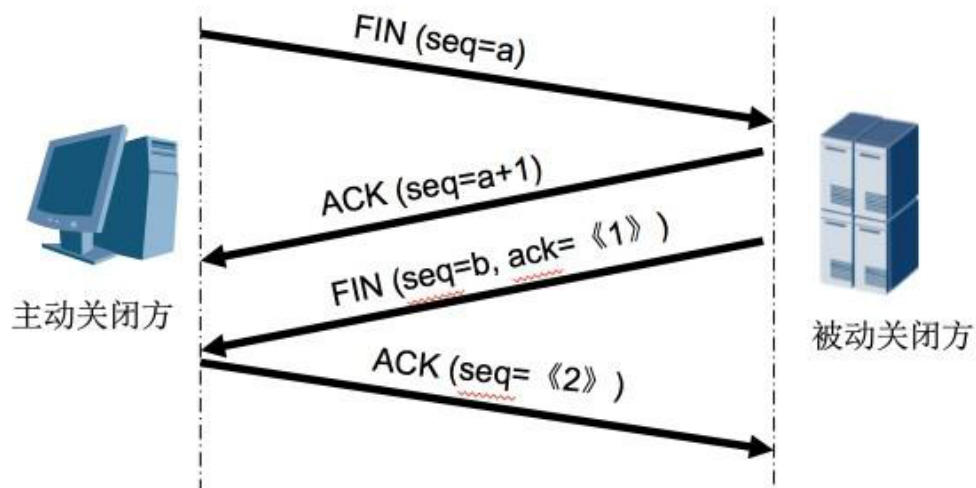
153. 以下哪些攻击利用了主机在收到目的端口为 7 (echo) 和 19 (chargen) 的 udp 报文后, 都会产生回应的机制? (单选)

- a、fraggle 攻击
- b、land 攻击
- c、winnuke 攻击

d、teardrop 攻击

答案：a

154. 如图的 tcp 断开连接 4 次握手中，《1》和《2》应分别是：（单选）



a、a+1 和 b+1

b、a 和 b

c、a+1 和 b

d、a 和 b+1

答案：a

155. 华为下一代防火墙可以对传输的文件进行病毒扫描，以下说法正确的是？

a、NGFW 支持对不同传输方向上的文件进行病毒检测。

b、若命中病毒例外，也命中应用例外，将会执行病毒例外动作。

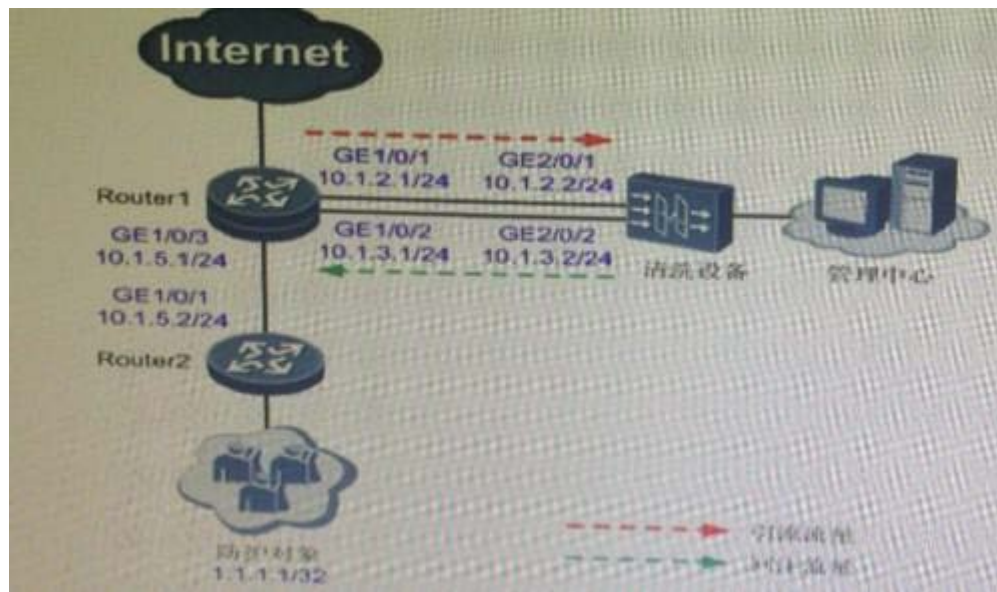
c、NGFW 支持对 HTTP 和 HTTPS 传输的文件进行病毒检测。

d、支持针对断点续传文件的反病毒检测。

答案：ab

156. 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 (单选)



- a、该默认路由用于流量汇注
- 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

答案：a

157. USG 中，规划 UTM 说法正确的是：

- a、推荐定期升级特征库
- b、使用 UTM 个功能前，必须将运行模式配置为 UTM 模式。
- c、UTM 会对所有分片进行重组，如果报文超出缓存范围，将会丢弃报文。
- d、当 USG 无法与安全服务中心连接时，只能通过本地单独升级，无法统一特征库。

答案：ab

158. 相比 802.1x 认证，portal 认证的优点有哪些？

- a、portal 认证不要求安装客户端软件

- b、portal 认证更适合网络的临时访问者。
- c、portal 能够用于哑终端接入场景。
- d、portal 认证兼容 mac 认证。

答案：abd

159. 以下对于双机热备的描述，不正确的是？

- a、开启自动备份后，主机所有会话都将自动备份到备机。
- b、开启快速备份后，主机配置也可以备份到备机。
- c、VGMP 当前主状态，属于改 VGMP 的 VRRP 接口 down 后，该 VGMP 的状态肯定会切换为备状态。
- d、防火墙配置备份方向肯定是从 VGMP 主状态设备备份到备状态设备。

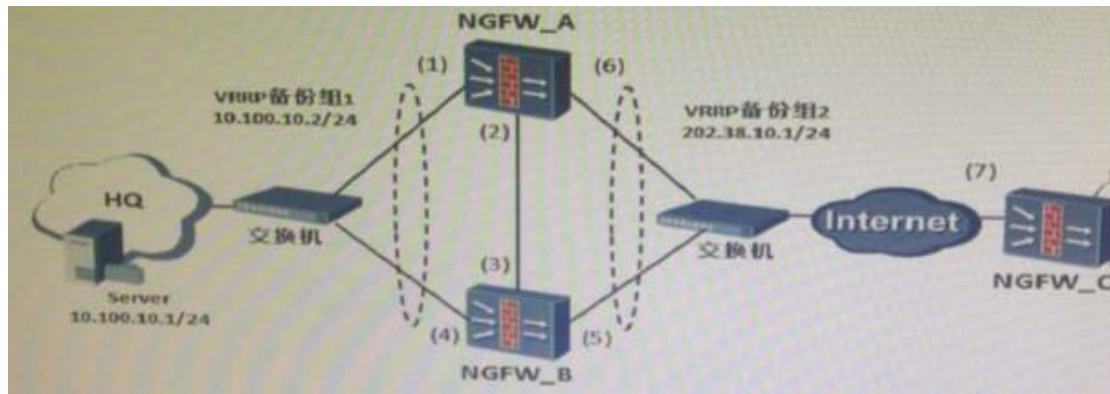
答案：b

160. 某中型企业网内有上百人通过公司防火墙访问互联网，同时公司在防火墙 DMZ 部署了企业门户网站。作为 IT 安全人员应遵循以下哪个标准采购和部署互联网访问审计产品。（单选）

- a、公安部 82 号令
- b、ISO27002
- c、国办发 28 号
- d、NIST800-53

答案：a

161. 对于如图所示组网，建立 ipsec 隧道的一端使用两台设备进行双机热备，当发生主备切换时，以下描述正确的是？



- a、IPSec 隧道不需要重新协商
- b、从 USG\_C 往 HQ 方向的报文会触发重新协商，业务不会影响。
- c、在 USG\_A、USG\_B、USG\_C 上配置 dpd 机制，能够增加 ipsec 双机热备的可靠性。
- d、keepalive 机制相对 dpd 机制，消耗更少的 cpu 资源。

答案：ac

161. 配置 ipsec 安全策略前，需要完成以下哪些任务？

- a、定义被保护的数据流
- b、配置 ipsec 安全提议
- c、配置 ike 安全提议和 ike 对等体
- d、配置 dpd
- e、配置 nat 穿越

答案：abc

162. 通过 tcp 反向源探测和 tcp 代理技术可以防范 sys flood 攻击，比较两种防范技术说法正确的是：

- a、使用 tcp 代理方式可以应用在来回路径不一致的场景。
- b、反向源探测机制和 tcp 代理方式的防范技术必须开启状态检测机制。
- c、syn 报文速率达到告警阈值 alert-rate-number 时，设备才可以对 syn 报文进行源认证检查。

d、syn 报文速率达到告警阈值 alert-rate-number 时，设备才可以对 syn 报文进行 tcp 代理检查。

答案：bd

163. ips 的基本处理流程如下：

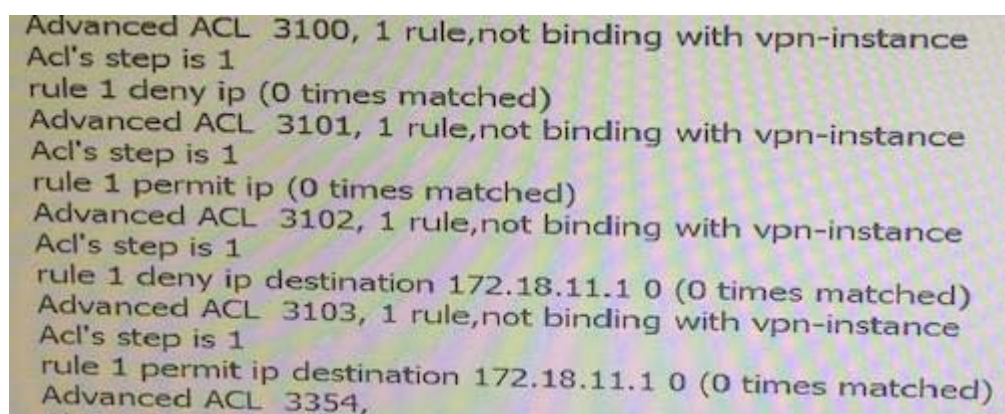
1. 重组应用数据
2. 协议识别
3. 匹配签名
4. 完成检测

以下排列顺序正确的是：（单选）

- a、1-2-3-4      b、2-1-4-3      c、1-2-4-3      d、1-3-2-4

答案：a

164. 在硬件安全接入控制网关采用下一代防火墙的情况下，在“策略》准入控制》SACG 配置》硬件 SACG“，选择”受控域“页签，增加受控域 ERP（172.18.11.1/32）和 DB\_Oracle（172.18.12.32 / 32），然后通过 CLI 查询防火墙配置，获得以下信息： Display acl all



```
Advanced ACL 3100, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 deny ip (0 times matched)
Advanced ACL 3101, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 permit ip (0 times matched)
Advanced ACL 3102, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 deny ip destination 172.18.11.1 0 (0 times matched)
Advanced ACL 3103, 1 rule, not binding with vpn-instance
Acl's step is 1
rule 1 permit ip destination 172.18.11.1 0 (0 times matched)
Advanced ACL 3354,
```

关于以下 acl 配置，下列说法正确的是哪些？

- a、当前受控域为完全下发到硬件安全接入控制网关
- b、可以通过管理员在 agile controller 管理器上进行受控域手工同步把受控域下发到硬件安全接入控制网关。

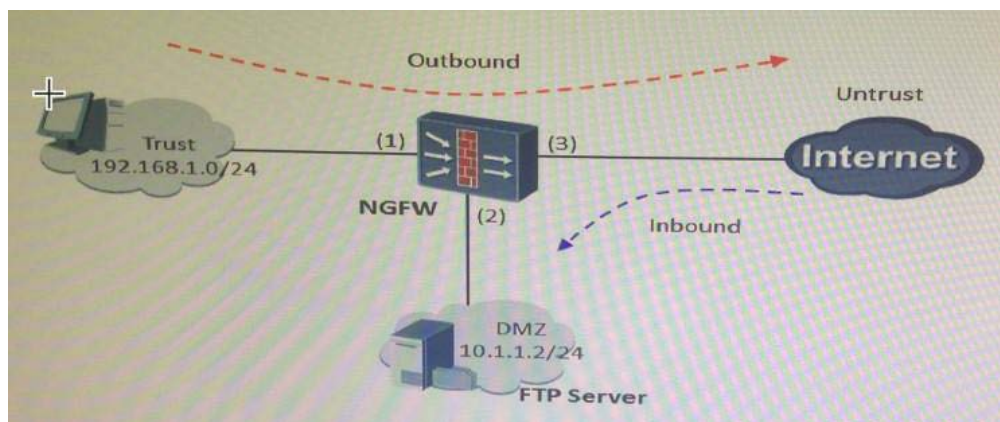


- c、agile controller 管理器会定时检查并下发控制域配置，该问题会自动修复。
- d、只能登录硬件安全接入控制网关，在诊断模式下执行受控域刷新命令 sync role-info, 主动从 agile controller 管理器请求刷新受控域解决。

答案：ad

165. 某企业有如下需求： Trust 区域中内网用户的是 192.168.1.0/24 网段，可以访问 internet。 以下配置正确的是：

```
traffic-policy
profile trust_to_untrust
  bandwidth downstream maximum-bandwidth 400000
  bandwidth downstream guaranteed-bandwidth 50000
  bandwidth ip-car downstream maximum-bandwidth per-ip 2000
rule name trust_to_untrust
  source-zone trust
  destination-zone untrust
  source-address 192.168.1.0 24
  action qos profile trust_to_untrust
#
```



- a、该配置将实现 trust 内网用户主动访问 internet 外网限制总的最大下载带宽为 400M。
- b、该配置将实现 internet 地址主动访问内网网段的进行限速。
- c、该配置将实现从 trust 到 untrust 的方向上的下载流量，最大每 ip 带宽为 2M。
- d、该配置将实现内网 192.168.1.0/24 用户的整体上传带宽为 50M。

答案：ac



166. 关于证书 ocsp 和 crl 技术说法正确的是？

- a、ocsp 可以实时获取证书的吊销状态。
- b、crl 比 ocsp 具有更高的时效性。
- c、ocsp 协议以在线的方式获取某个证书的吊销状态，以此检查对方的证书是否被吊销。
- d、从客户端证书中自动获取的 cdp (CRL Distribution Points) 信息不会存储到配置文件，所以当 USG 重启后，自动获取的 cdp 信息将不被保存。
- e、ocsp 必须经常在客户端下载证书列表，以保证更新。

答案：acd

167. 在使用 utm 功能时，必须先启用防火墙状态检测。

- a、true
- b、false

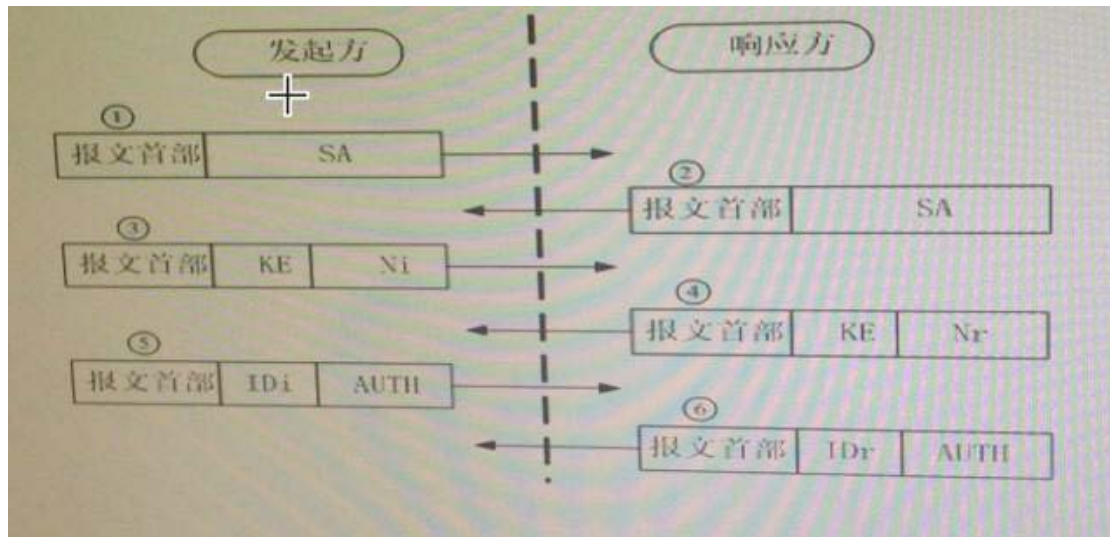
答案：a

168. 华为下一代防火墙可以对传输的文件进行病毒扫描，以下说法正确的是？

- a、NGFW 支持对不同传输方向上的文件进行病毒扫描。
- b、若命中病毒例外，也命中应用例外，将会执行病毒例外动作。
- c、NGFW 支持对 http 和 https 传输的文件。
- d、支持针对断点续传文件的反病毒检测。

答案：ab

169. IKEv1 协商过程如下图所示，关于协商信息内容说法正确的是：（单选）



- a、1、2 交换临时随即值 (Ni、Nr 载荷)
- b、3、4 信息被加密
- c、当使用共享密钥认证时，预共享密钥将直接用于 IKE 消息加密。
- d、5、6 交换身份 ID.

答案: d

170. 关于 udp flood 和 tcp flood 攻击防范说法正确的是:

- a、udp 协议是无连接的，因此无法通过源探测实现。
- b、防范 udp flood，通过分析某个主机发送 udp 报文的规律和特征，这个规律和特征被称为指纹学习。
- c、udp 报文的指纹学习功能通过学习报文数据段全部字段。
- d、udp 和 tcp 协议可以通过代理技术实现。

答案: ab

171. 防火墙双机热备的场景下，ipsec vpn 不支持隧道的实时备份。

- a、true
- b、false

答案: b

172. 主机加固主要包括以下哪些方面？

- a、操作系统加固
- b、数据库加固
- c、账号密码安全
- d、网管系统加固
- e、漏洞扫描

答案：abcd

173. 防火墙 utm 特性包含哪些功能？

- a、ips
- b、av
- c、内容过滤
- d、url 过滤
- e、流量型攻击防范

答案：abcd

174. 下列哪些选项可以作为 portal 推送的条件？

- a、终端 ip 地址范围
- b、终端浏览器类型
- c、终端设备类型
- d、接入 ap 的 ssid
- e、接入 ap 的 mac 地址
- f、接入 ac 的 mac 地址

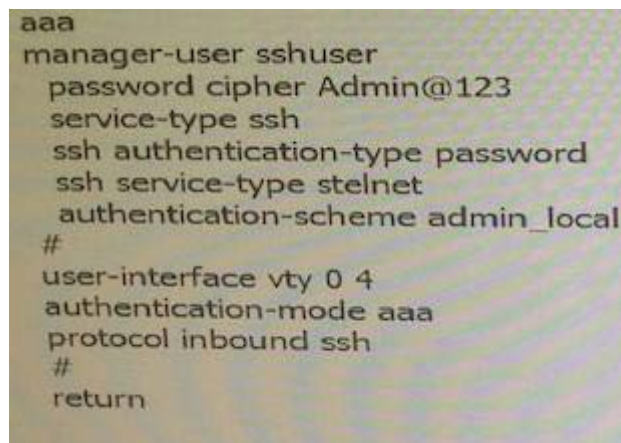
答案：acde

175. radius 和 hwtacacs 协议的主要区别包括：

- a、radius 使用 tcp 协议，网络传输更可靠，hwtacacs 使用 udp 协议。
- b、hwtacacs 对报文主体全部进行加密，radius 只是对认证报文的密码字段进行加密。
- c、radius 认证授权分离，hwtacacs 认证与授权一起处理。
- d、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。

答案：bd

176. 用户无法通过 ssh 登录管理设备，现获取到如下配置信息，请分析可能产生的原因是：



```
aaa
manager-user sshuser
password cipher Admin@123
service-type ssh
ssh authentication-type password
ssh service-type stelnet
authentication-scheme admin_local
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```

- a、管理员未在系统视图下配置 stelnet server enable 命令
- b、为对 ssh user 用户配置 level3
- c、若登录接口非设备管理口，需要在接口下执行 service-manager ssh permit
- d、为配置 aaa 的 domain 及制定其认证方式 local

答案：ac

177. 如果使用手机移动终端（安卓和苹果系统）通过 web 代理访问内网资源，则应该推荐使用以下哪 种方式？

- a、只能使用 web link
- b、只能使用 web 改写
- c、即可以 web link 也可以使用 web 改写

d、这类手机根本无法通过 web 代理访问内网资源

答案：b

需要注意的是，Web link 只适合在用户使用 Windows 操作系统+IE 浏览器的终端上使用。非此场合，只能使用 Web 改写。

178. 随着我国信息化和信息安全保障工作的不断深入推进，加强和规范信息安全服务资质管理已成为信息安全管理的重要基础性工作，以下哪些是中国信息安全认证中心所提供的资质认证？

- a、安全研发服务资质认证
- b、安全部署服务资质认证
- c、风险评估服务资质资质认证
- d、应急处理服务资质认证

答案：cd（还有安全集成服务资质）

179. 防火墙运行 GRE 时，物理口和 tunnel 口都需要加入安全域。

- a、true
- b、flase

答案：a

180. 终端用 agent 进行 802.1x 认证，sc 和 radius 服务器 ip 地址为：

172.18.10.68，认证时总是提示网络 通信失败；查看 radius 认证日志显示 radius 认证成功，并授权为 acl3001，交换机配置如下：

```

dot1x enable
dot1x authentication-method eap
radius-server template lzy
radius-server shared-key simple 123456
radius-server authentication 172.18.10.68 1812
radius-server accounting 172.18.10.68 1813
radius-server authorization 172.18.10.68 shared-key simple 123456
aaa
authentication-scheme default
authentication-scheme auth
authentication-mode radius

```

```

accounting-scheme acco
accounting-mode radius
accounting realtime 3
domain default
authentication-scheme auth
accounting-scheme acco
radius-server lzy
interface GigabitEthernet0/0/14
description connect 222
port hybrid pvid vlan 105
port hybrid untagged vlan 105
dot1x enable
acl number 3001
rule 1 permit ip destination 172.18.100.235 0
rule 2 permit ip destination 172.18.100.237 0
rule 10 deny ip

```

网络通信失败的原因可能是？（单选）

- a、计费配置可能错误
- b、aaa 配置错误
- c、授权规则 acl 配置错误
- d、g0/0/14 接口配置错误

答案：c

181. 用户通过笔记本进行 802.1x 认证，当安全检查失败时只能访问哪些资源？（单选）

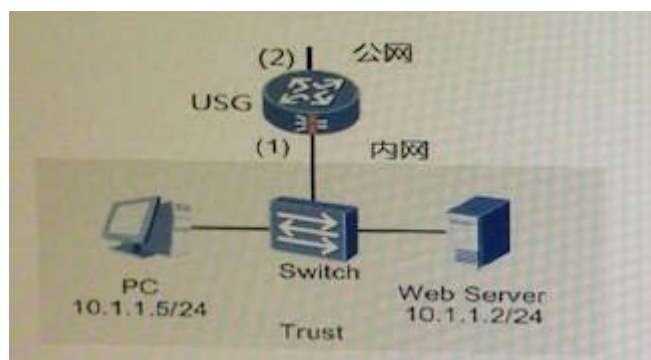


- a、172.19.60.0/24

- b、172.19.50.0/24
- c、172.19.10.0/24
- d、172.19.90.0/24

答案：a

182. 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 地址的描述可能争取的是：



- 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 10.1.1.5.
- b、web 服务器收到的 pc 访问 web 服务的数据包源 ip 地址为接口（1）的 ip 地址。
- c、pc 机收到 web 服务器回应的数据包源 ip 地址为 10.1.1.2。
- d、pc 机收到 web 服务器回应的数据包源 ip 地址为接口（2）的 ip 地址。

答案：bd

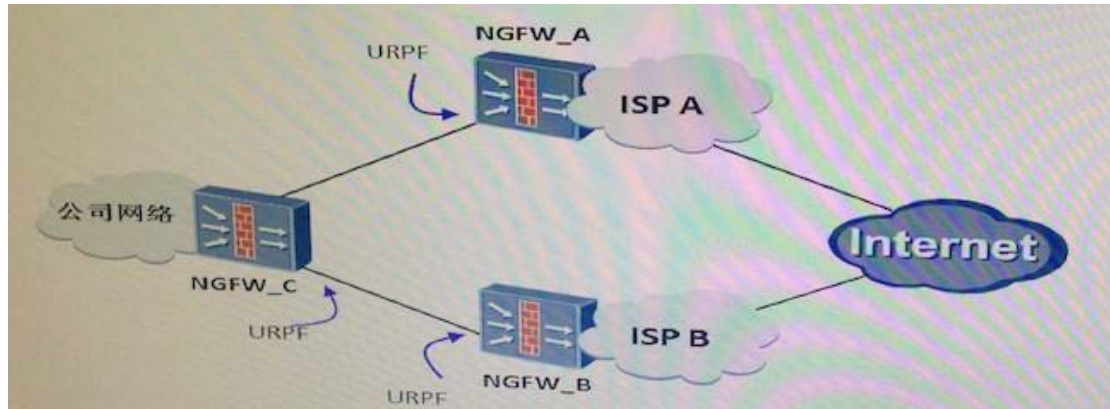
183. 内网网络安全，关于规划部署建议优先考虑项由如下哪些选项？

- a、应用三层架构平面隔离
- b、防火墙和交换机虚拟化实现业务隔离
- c、计算网络和存储网络物理隔离
- d、开启 ddos 功能
- e、开启 nat 功能



答案：ab

184. 某网络期望使用 urpf 技术提高网络安全性, 如下组网场景使用了 urpf 的哪种模式: (单选)



- a、严格模式
- b、松散模式
- c、严格模式或松散模式
- d、根据题干信息, 无法判断相应的模式。

答案：b

185. 入侵防御实现机制包括哪些?

- a、黑名单匹配
- b、协议识别和协议解析
- c、特征匹配
- d、相应处理

答案：bcd

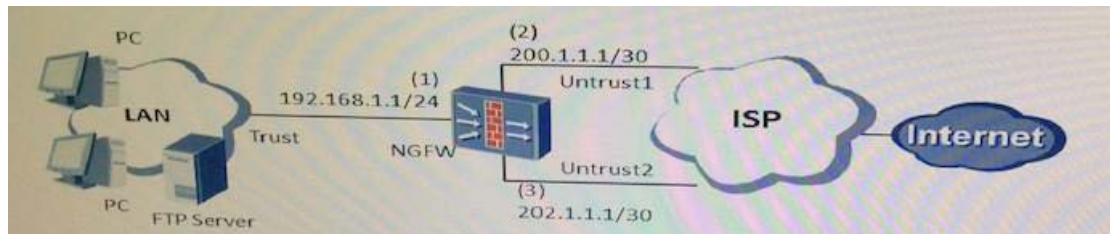
186. ipsec vpn 隧道建立成功, 但是访问对端私网 web 页面的速度慢或访问时断时续, 已经排除 internet 网络质量影响, 以下可能故障有:

- a、报文分片的问题
- b、出口网关的 cpu 占用率过高
- c、网络中间有 nat 设备
- d、包过滤策略没有开启



答案: ab

187. 内网用户可以正常访问 internet, 双链路为主备备份。 对于 internet 用户, 可以通过公网地址访问 ftp 服务器, 对外公布 2 个公网地址, 200.1.1.200 和 202.1.1.200. 以下配置正确的是?



答案: ab

188. 防火墙 utm 特性包含哪些功能?

- a、ips
- b、av
- c、内容过滤
- d、url 过滤
- e、流量型攻击防范

答案: abcd

189. 某网络组网如下: pc——adsl 路由器——usg——lan usg 的关键配置如下:

```
l2tp enable
interface Virtual-Template1
 ppp authentication-mode pap
 ip address 4.1.1.1 255.255.255.0
 remote address pool 1
 l2tp-group 1
 mandatory-lcp
 allow l2tp virtual-template 1
 #
 user-manage user pc1
 password admin@123
 aaa
 domain default
 ip pool 1 4.1.1.1 4.1.1.99
```

假设其他配置完整正确，该配置在实际工作时出现问题和现象是？（单选）

- a、能够拨号成功，也可以访问内网服务器
- b、不能拨号成功
- c、拨号成功会立即断开
- d、能拨号成功，但无法访问内网服务器

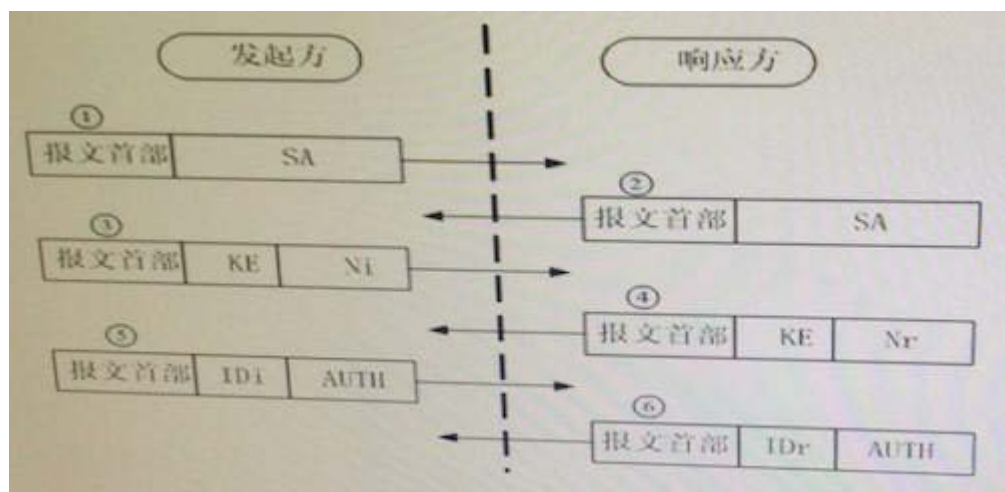
答案：b

190. 在双机热备的场景，关于防火墙主设备和备设备描述错误的是？

- a、当双机热备工作在主备状态下，主用设备的命令提示符显示 HRP\_A, 备用设备的命令提示符显示 HRP\_S.
- b、默认情况下，主备设备的配置会立刻备份到备用设备上。
- c、只有主设备才能进行命令配置，备用设备命令不能进行配置。
- d、配置主设备显示 HRP\_A, 配置从设备显示 HRP\_S, 而且不随优先级变化而变化。

答案：cd

191. 下图为 IKEv1 协商过程，其中 1，2 消息协商了什么消息？

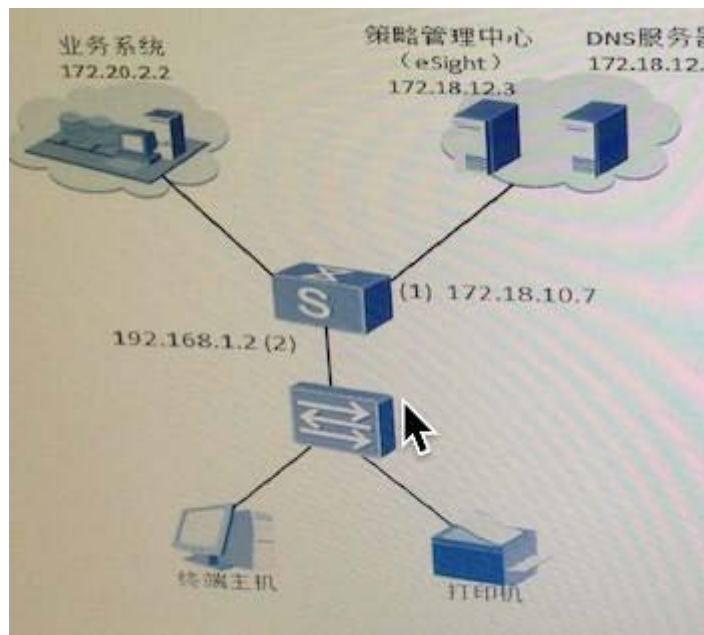


- a、ike 安全提议
- b、交换临时随机数
- c、id 载荷

d、auth 载荷

答案：ab

192. 某网络使用 agile controller 进行 802.1x 认证，其中 s 交换机 g0/0/9 连接了终端主机和打印机，打印机通过 mac 认证，终端主机需要通过 agent 进行即可通过认证，交换机的正确配置是？（单选）



a、

```
[Quidway] dot1x enable
[Quidway] dot1x authentication-method eap
[Quidway] interface GigabitEthernet 0/0/9
[Quidway-GigabitEthernet 0/0/9] port link-type access
[Quidway-GigabitEthernet 0/0/9] port default vlan 105
[Quidway-GigabitEthernet 0/0/9] dot1x enable
[Quidway-GigabitEthernet 0/0/9] dot1x port-method MAC
```

b、

```
[Quidway] dot1x authentication-method eap
[Quidway] interface GigabitEthernet 0/0/9
[Quidway-GigabitEthernet 0/0/9] port link-type access
[Quidway-GigabitEthernet 0/0/9] dot1x port-method MAC
```

c、

```

[Quidway] dot1x enable
[Quidway] dot1x authentication-method eap
[Quidway] interface GigabitEthernet 0/0/9
[Quidway-GigabitEthernet 0/0/9] port link-type trunk

```

d、

```

[Quidway] dot1x authentication-method eap
[Quidway] interface GigabitEthernet 0/0/9
[Quidway-GigabitEthernet 0/0/9] port link-type access
[Quidway-GigabitEthernet 0/0/9] port default vlan 105
[Quidway-GigabitEthernet 0/0/9] dot1x port-method MAC

```

答案：a

小题：

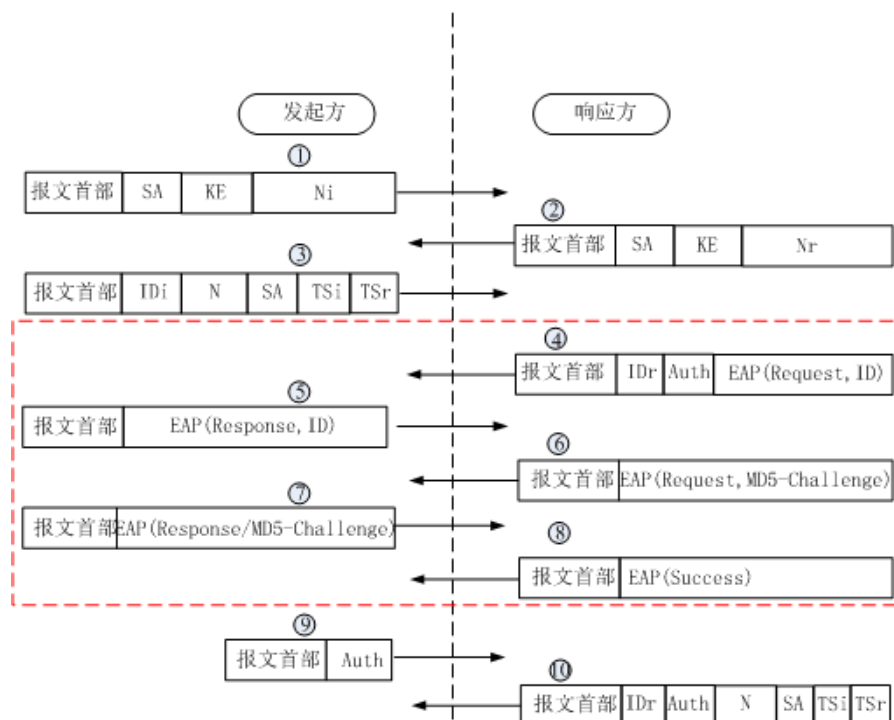
1、L2TP VPN 放开策略：单选

rule permit udp source-port eq 1701

2、在防火墙上 URL 匹配方式包括哪些？

前缀匹配、后缀匹配、关键字匹配

3、如图所示，关于协商信息内容说法正确的是？



- a. 此过程为 IKEv2 的报文协商
- b. ①和②是进行载荷、协商 IKE 安全提议
- c. 红框内是 EAP 的认证协商过程
- d. 红框内是必须配置的协商过程

注释：IKEv2 协商过程（预共享密钥认证+EAP 认证）

1. ①、②：IKE\_SA\_INIT 交换。协商 IKE 安全提议（SA 载荷），交换临时随机数（Ni、Nr 载荷）和 DH 公开值（KE 载荷）。
2. ③：IKE\_SA\_AUTH 交换。发送身份 ID，但省去 AUTH 载荷，表明需要使用 EAP 认证。协商 IPSec 安全提议（SA 载荷），协商待保护的数据流（TS 载荷）。N 载荷用于错误通知。
3. ④、⑤、⑥、⑦、⑧：EAP 消息被封装在 EAP 载荷中进行认证协商。
4. ⑨、⑩：双方继续交换身份 ID（ID 载荷）和 Hash 值（AUTH 载荷），协商待保护数据流、IPSec 安全提议。协商通过后建立 IKE SA 和一对 IPSec SA。

4、给出一个 AAA 的配置，只配置认证(10000)、计费(10003)，单选选择未配置授权部分。

5、给出一段 debug 信息，提示 ipsec\_proposal 的 dh group 错误或 pfs 错误，选择两项。