Modules 3 – 5: Network Security Exam Français

Enterprise Networking, Security, and Automation (Version 7.00) – Examen de la sécurité des réseaux Réponses

1. En règle générale, quelles sont les raisons qui poussent les cybercriminels à attaquer des réseaux, en comparaison d'hacktivistes ou de pirates agissant pour le compte d'un État ?

- La reconnaissance de leurs pairs
- Des raisons politiques
- **gain financier**
- La recherche de la gloire

Explique: Les cybercriminels sont généralement motivés par l'argent. Dans le cas des pirates, c'est davantage le statut qui prime. Quant aux cyberterroristes, ils agissent principalement pour des raisons religieuses ou politiques.

2. Quel type de hacker agit pour des raisons politiques et sociales ?

- cybercriminel
- **Hacktiviste**
- testeur de vulnérabilité
- script kiddie

Explique: Les hackers sont classés en fonction de leurs motivations. Les hacktivistes agissent pour des raisons politiques et sociales.

3. Parmi les propositions suivantes, laquelle décrit le mieux un cheval de Troie ?

- Il s'agit de la forme de programme malveillant la plus facile à détecter.
- Il s'agit d'un logiciel qui entraîne des désagréments pour l'utilisateur, mais pas de problèmes irrécupérables pour l'ordinateur.
- Il s'agit d'un programme malveillant qui ne peut être distribué que sur Internet.
- **Il se présente sous la forme d'un logiciel utile, mais dissimule un code malveillant.**

Explique: Ce qui différencie un cheval de Troie d'un virus ou d'un ver informatique c'est que, sous ses apparences de logiciel utile, il cache en fait du code malveillant. Les chevaux de Troie peuvent causer des désagréments mineurs, mais aussi être à l'origine de problèmes informatiques irrécupérables. Les chevaux de Troie peuvent être distribués via Internet, mais aussi par le biais de clés USB ou d'autres supports. Les chevaux de Troie très ciblés peuvent être particulièrement difficiles à détecter.

4. Un utilisateur reçoit un appel téléphonique d'une personne qui prétend représenter des services informatiques et qui lui demande de confirmer son nom d'utilisateur et son mot de passe à des fins d'audit. Quelle menace cet appel téléphonique représente-t-il pour la sécurité ?

- **Manipulation psychologique**
- Courrier indésirable
- DDoS
- Enregistrement anonyme des frappes

Explique: La manipulation psychologique consiste à gagner la confiance d'un employé et à le persuader de divulguer des informations confidentielles et sensibles, comme ses noms d'utilisateur et mots de passe. Les attaques DDoS, le courrier indésirable et l'enregistrement des frappes sont des exemples de menaces pour la sécurité des logiciels, et non de la manipulation psychologique.

5. Qu'est-ce qu'un balayage ping ?

- **Une technique d'analyse du réseau qui indique les hôtes actifs dans une plage d'adresses IP.**
- Un protocole de type requête/réponse qui identifie des informations relatives à un domaine, y compris les adresses qui lui sont attribuées.
- Une application logicielle qui permet de capturer tous les paquets réseau envoyés sur un LAN.
- Une technique d'analyse qui examine une plage de numéros de port TCP ou UDP sur un hôte afin de détecter les services d'écoute.

Explique: Un balayage ping est un outil utilisé au cours d'une attaque de reconnaissance. Les autres outils qui peuvent être utilisés lors de ce type d'attaque sont le balayage de ports et la demande d'informations Internet. Une attaque de reconnaissance est utilisée pour collecter des informations sur un réseau en particulier, généralement en prévision d'un autre type d'attaque réseau.

6. De quelle façon les zombies sont-ils utilisés dans les attaques contre la sécurité ?

- Il s'agit de segments de code créés de façon malveillante pour remplacer des applications légitimes.
- Ils ciblent des personnes précises pour obtenir les informations d'entreprises ou des informations personnelles.
- **Ce sont des ordinateurs infectés qui effectuent une attaque par déni de service (DDoS).**
- Ils sondent un groupe de machines pour trouver des ports ouverts afin de déterminer quels services sont en fonctionnement.

Explique: Les zombies sont des ordinateurs infectés qui constituent un réseau de zombies. Les zombies sont utilisés pour déployer une attaque par déni de service distribué (DDoS).

7. Quel masque générique correspondra aux réseaux 172.16.0.0 à 172.19.0.0?

- 0.0.3.255
- 0.252.255.255
- **0.3.255.255**
- 0.0.255.255

Explique: Les sous-réseaux 172.16.0.0 à 172.19.0.0 partagent tous les mêmes 14 bits de haut niveau. Un masque générique en binaire qui correspond à 14 bits d'ordre supérieur est 00000000.00000011.11111111111111111. En décimal pointillé, ce masque générique est 0.3.255.255.

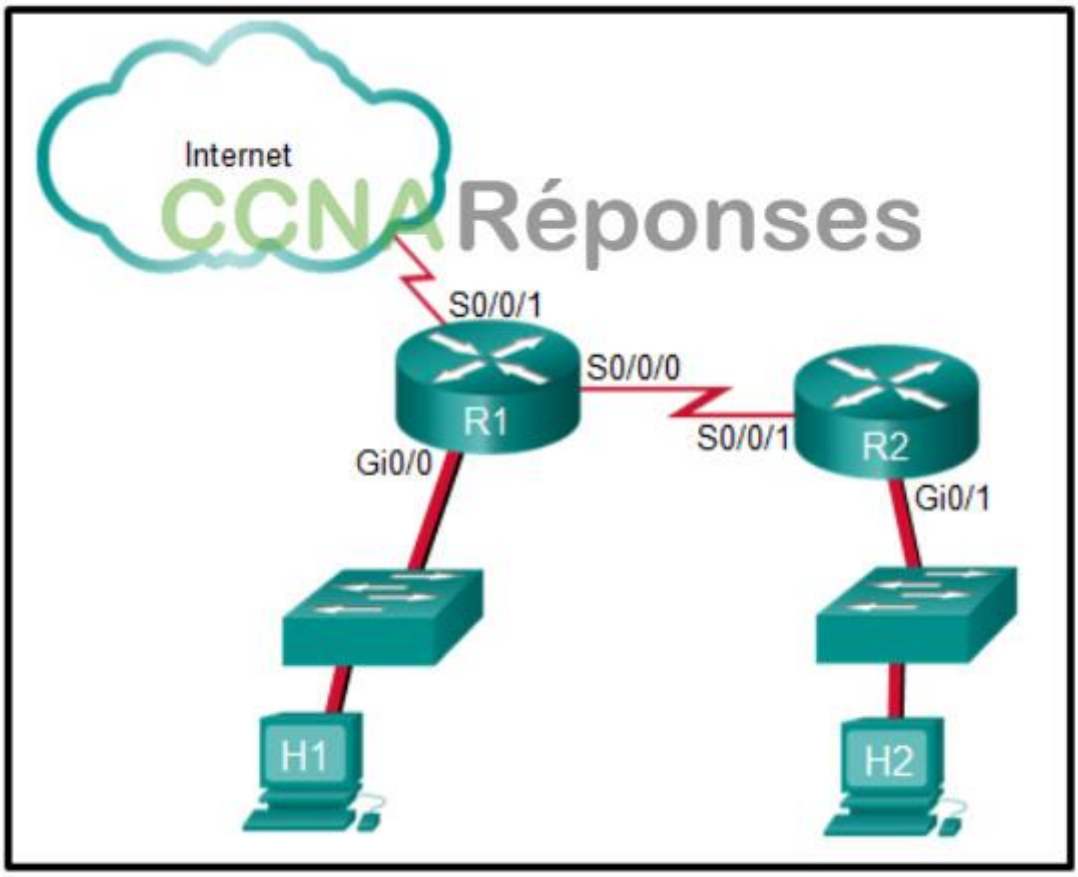
8. Quels filtres de paquet un administrateur réseau peut-il utiliser sur une liste de contrôle d'accès étendue IPv4 ? (Choisissez deux réponses.)

- Adresse MAC de destination

- Adresse Hello TCP source
- **Type de message ICMP**
- **Numéro de port UDP de destination**
- Type d'ordinateur

Explique: Les listes de contrôle d'accès étendues filtrent généralement les adresses source et de destination IPv4 et les numéros de port TCP ou UDP. Un filtrage supplémentaire peut être fourni pour les types de protocoles.

9. Examinez l'illustration. L'étudiant sur l'ordinateur H1 continue à lancer une requête ping étendue avec des paquets étendus à l'étudiant sur l'ordinateur H2. L'administrateur réseau de l'établissement scolaire souhaite mettre un terme à ce comportement, tout en continuant à autoriser les deux étudiants à accéder aux devoirs informatiques basés sur le Web. Quelle est la meilleure méthode que l'administrateur réseau doit suivre pour ce faire ?



- **Appliquer une liste de contrôle d'accès étendue entrante sur R1 Gi0/0.**
- Appliquer une liste de contrôle d'accès étendue sortante sur R1 S0/0/1.
- Appliquer une liste de contrôle d'accès standard sortante sur R2 S0/0/1.
- Appliquer une liste de contrôle d'accès étendue entrante sur R2 Gi0/1.
- Appliquer une liste de contrôle d'accès standard entrante sur R1 Gi0/0.

Explique: Cette liste d'accès doit être une liste de contrôle d'accès étendue pour filtrer les adresses d'hôte source et de destination spécifiques. Généralement, le meilleur emplacement pour une liste de contrôle d'accès étendue est le plus proche de la source, qui est H1. Le trafic remonte H1 et accède au commutateur, puis sort du commutateur dans l'interface R1 Gi0/0. Cette interface Gi0/0 serait le meilleur

emplacement pour ce type de liste de contrôle d'accès étendue. La liste de contrôle d'accès serait appliquée à l'interface d'entrée car les paquets de H1 entreraient dans le routeur R1.

10. Quel type d'ACL offre une grande flexibilité et un meilleur contrôle sur l'accès au réseau?

- flexible
- Numérotée standard
- Standard nommée
- **étendu**

Explique: Les deux types de listes de contrôle d'accès sont les listes standard et les listes étendues. Les deux types peuvent être nommés ou numérotés, mais les ACL étendues offrent une grande flexibilité.

11. Examinez l'illustration. Un administrateur réseau configure une liste de contrôle d'accès IPv4 standard. Que se passe-t-il après l'exécution de la commande no access-list 10 ?

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 10 permit host 192.168.25.16
R1(config)# access-list 10 deny 192.168.25.0 0.0.0.255
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip access-group 10 in
R1(config-if)# end
R1#

R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no access-list 10
R1(config)# end
R1#
```


- La liste de contrôle d'accès 10 sera désactivée et supprimée après le redémarrage de R1.
- La liste de contrôle d'accès 10 est désactivée sur Fa0/1.
- La liste de contrôle d'accès 10 est supprimée de la configuration en cours et de l'interface Fa0/1.
- **La liste de contrôle d'accès 10 est supprimée de la configuration en cours.**

Explique: La commande R1(config)# no access-list < access-list number > supprime immédiatement la liste de contrôle d'accès de la configuration en cours. Toutefois, pour désactiver une liste de contrôle d'accès sur une interface, la commande R1(config-if)# no ip access-group doit être saisie.

12. Reportez-vous à l'illustration. Un administrateur réseau a configuré l'ACL 9 comme indiqué. Les utilisateurs sur le réseau 172.31.1.0 /24 ne peuvent pas transférer le trafic via le routeur CiscoVille. Quelle est la cause la plus probable

de la défaillance de la circulation ?

```
CiscoVille#
CiscoVille# configure terminal
CiscoVille(config)# access-list 9 permit 172.29.0.0 0.0.0.255
CiscoVille(config)# access-list 9 permit 172.30.0.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 172.31.0.0 0.0.255.255
CiscoVille(config)# access-list 9 permit 172.31.1.0 0.0.0.255
CiscoVille(config)# access-list 9 deny 192.168.1.0 0.0.0.255
CiscoVille(config)# access-list 9 permit any
CiscoVille(config)# interface fastethernet0/1
CiscoVille(config-if)# ip access-group 9 in
CiscoVille(config-if)# end
```


- L'instruction permit spécifie un masque générique incorrect.
- Le numéro de port du trafic n'a pas été identifié avec le mot-clé eq .
- **La séquence des ACEs est incorrecte.**
- Le mot-clé établi n'est pas spécifié.

Explique: Lors de la vérification d'une liste ACL, les instructions sont toujours répertoriées dans un ordre séquentiel. Même s'il existe un permis explicite pour le trafic provenant du réseau 172.31.1.0 /24, il est refusé en raison de l'ACE précédemment implémenté de CiscoVille (config) # access-list 9 deny 172.31.0.0 0.255.255 . La séquence des ACEs doit être modifiée pour autoriser le trafic spécifique provenant du réseau 172.31.1.0 /24, puis refuser 172.31.0.0 /16.

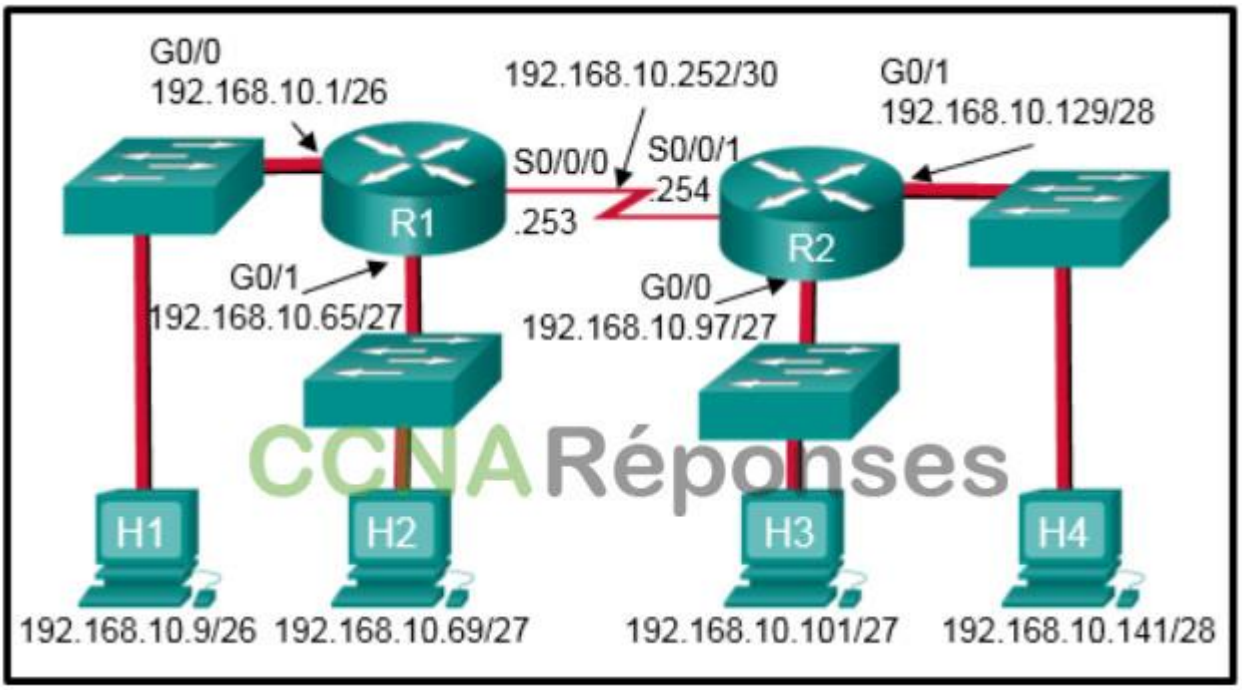
13. Un administrateur réseau doit configurer une ACL standard afin que seule la station de travail de l'administrateur avec l'adresse IP 192.168.15.23 puisse accéder au terminal virtuel du routeur principal. Quelles sont les deux commandes de configuration qui peuvent accomplir la tâche? Citez-en deux.

- **Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0**
- Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255
- Router1 (config)# access-list 10 permit 192.168.15.23 255.255.255.255
- **Router1 (config)# access-list 10 permit host 192.168.15.23**
- Router1 (config)# access-list 10 permit 192.168.15.23 255.255.255.0

Explique: Pour autoriser ou refuser une adresse IP spécifique, il est possible d'utiliser soit le masque générique 0.0.0.0 (utilisé après l'adresse IP), soit le mot clé hôte du masque générique (utilisé avant l'adresse IP).

14. Reportez-vous à l'illustration. Quelle commande est utilisée dans une liste de contrôle d'accès standard pour autoriser uniquement les périphériques sur le réseau qui sont connectés à l'interface G0/0 de R2 à accéder aux réseaux

connectés à R1 ?



- **access-list 1 permit 192.168.10.96 0.0.0.31**
- access-list 1 permit 192.168.10.0 0.0.0.255
- access-list 1 permit 192.168.10.0 0.0.0.63
- access-list 1 permit 192.168.10.128 0.0.0.63

Explique: Les listes d'accès standard filtrent uniquement l'adresse IP source. Dans la conception, les paquets proviennent du réseau 192.168.10.96/27 (le réseau G0/0 de R2). La liste ACL correcte est access-list 1 permit 192.168.10.96 0.0.0.31 .

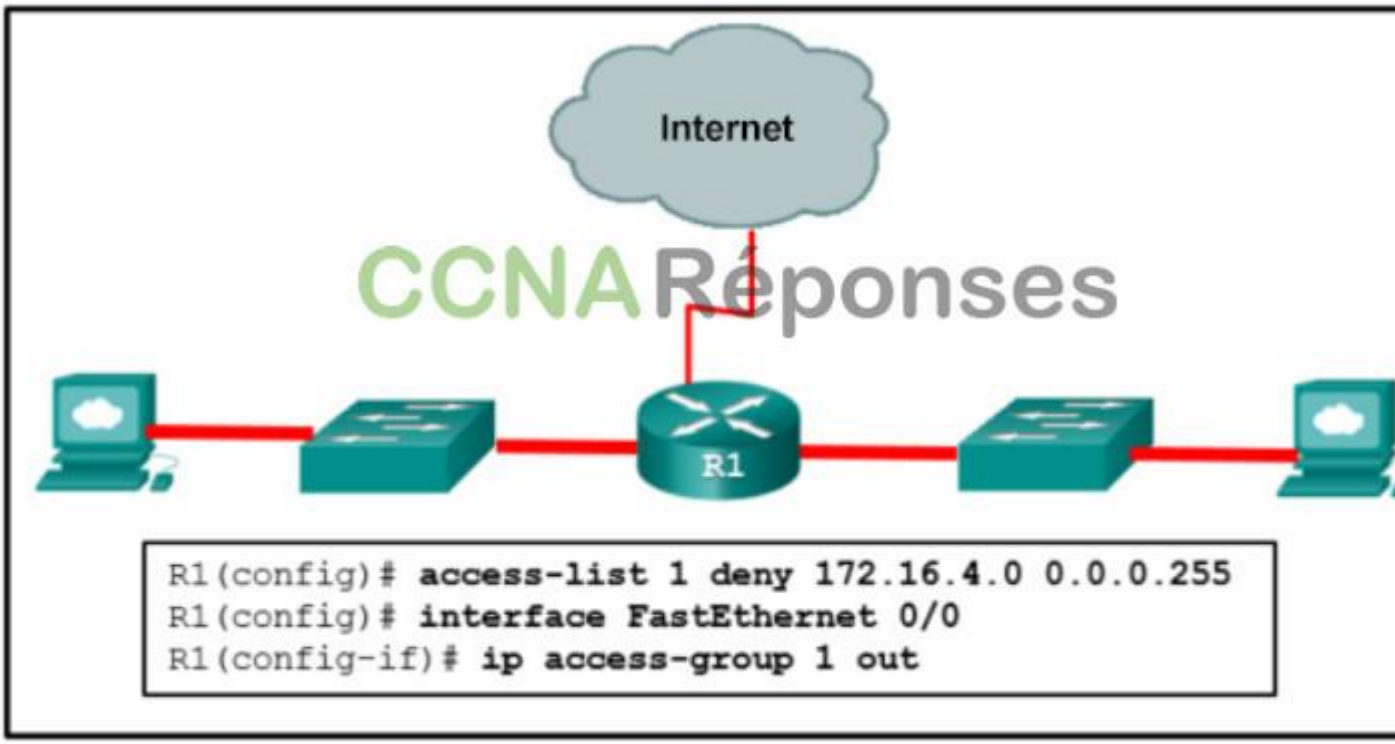
15. Un administrateur réseau établit une liste de contrôle d'accès standard qui interdira tout trafic venant du réseau 172.16.0.0/16 mais autorisera tous les autres trafics. Quelles sont les deux commandes à utiliser ? (Choisissez deux réponses.)

- Router(config)# access-list 95 host 172.16.0.0
- Router(config)# access-list 95 deny any
- **Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255**
- Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0
- **Router(config)# access-list 95 permit any**
- Router(config)# access-list 95 172.16.0.0 255.255.255.255

Explique: Pour refuser l'accès au trafic depuis le réseau 172.16.0.0/16, on utilise la commande access-list 95 deny 172.16.0.0 0.0.255.255 . Pour autoriser tout le reste du trafic, on ajoute la commande access-list 95 permit any .

16. Reportez-vous à l'illustration. Une liste de contrôle d'accès a été configurée sur R1 afin de refuser l'entrée du trafic venant du sous-réseau 172.16.4.0/24 dans le sous-réseau 172.16.3.0/24. Tout autre trafic entrant dans le sous-réseau 172.16.3.0/24 est autorisé. Cette liste de contrôle d'accès standard est ensuite appliquée en sortie sur l'interface Fa0/0. Quelles conclusions pouvez-vous tirer

de cette configuration ?



- La liste de contrôle d'accès devrait être appliquée comme interface de sortie sur toutes les interfaces de R1.
- Une liste de contrôle d'accès étendue doit être utilisée dans cette situation.
- Seul le trafic venant du sous-réseau 172.16.4.0/24 est bloqué, et tout autre trafic est autorisé.
- **Tous les trafics seront bloqués, pas seulement le trafic venant du sous-réseau 172.16.4.0/24.**
- La liste de contrôle d'accès doit être appliquée à l'interface FastEthernet 0/0 de R1 en tant qu'interface d'entrée pour répondre aux exigences.

Explique: À cause de l'instruction deny implicite à la fin de toutes les listes ACL, la commande access-list 1 permit any doit être incluse afin d'assurer que seul le trafic du sous-réseau 172.16.4.0/24 est bloqué et que les autres trafics sont autorisés.

17. Reportez-vous à l'illustration. Un administrateur réseau souhaite ajouter une entrée ACE à la liste de contrôle d'accès TRAFFIC-CONTROL pour refuser le trafic IP du sous-réseau 172.23.16.0/20. Quelle entrée ACE répond à cette exigence ?

- 15 deny 172.23.16.0 0.0.15.255
- 30 deny 172.23.16.0 0.0.15.255
- 5 deny 172.23.16.0 0.0.255.255

- **5 deny 172.23.16.0 0.0.15.255**

Explique: L'adresse IPv4 source est le seul critère de filtrage spécifié pour une liste d'accès standard. Le masque de caractère générique est écrit pour identifier les parties de l'adresse qui doivent correspondre, avec un bit 0, et les parties de l'adresse qui doivent être ignorées, avec un bit 1. Le routeur analyse les entrées ACE en partant du plus bas numéro de séquence vers le plus élevé. Si vous devez ajouter une entrée ACE à une liste d'accès existante, vous devez indiquer le numéro de séquence de sorte que l'entrée ACE soit correctement placée au cours du processus d'évaluation de la liste ACL.

18. Quel est l'effet de la commande Router1(config-ext-nacl)# permit tcp 172.16.4.0 0.0.0.255 any eq www lors de son implémentation en entrée sur l'interface f0/0 ?

- Tout le trafic en provenance du réseau 172.16.4.0/24 est autorisé partout, sur tout port.
- La commande est refusée par le routeur car elle est incomplète.
- **Le trafic en provenance du réseau 172.16.4.0/24 est autorisé sur l'ensemble des destinations de port 80 TCP.**
- Tout le trafic TCP est autorisé et tout autre trafic est refusé.

19. Examinez l'illustration. Quelles conclusions pouvez-vous tirer de ces informations ?

```
R1# show access-list MyACL
Extended IP access list MyACL
10 permit tcp host 10.35.80.22 host 10.23.77.101 eq telnet
20 permit tcp host 10.35.80.25 host 10.23.77.101 eq 16100 (149407 matches)
30 permit tcp host 10.35.80.25 host 10.23.77.101 eq 17600 (80592 matches)
40 permit tcp host 10.35.80.27 host 10.23.77.101 eq 10701 (26008 matches)
```


- **Le routeur n'a reçu aucun paquet Telnet provenant de 10.35.80.22 et destiné à 10.23.77.101.**
- La liste de contrôle d'accès surveille uniquement le trafic destiné à 10.23.77.101 et provenant de trois hôtes spécifiques.
- La liste de contrôle d'accès est dépourvue d'une entrée deny ip any any.
- Comme il n'existe aucune correspondance pour la ligne 10, la liste de contrôle d'accès ne fonctionne pas.

Explique: L'entrée 10 de la liste de contrôle d'accès dans MyACL correspond à tous les paquets Telnet entre l'hôte 10.35.80.22 et l'adresse 10.23.77.101. Aucune correspondance n'apparaît dans cette instruction ACE, comme le prouve l'absence d'une instruction ACE « (xxx correspondances) ». L'instruction ACE « deny ip any any » n'est pas requise, parce que chaque liste de contrôle d'accès contient une instruction ACE de refus implicite. Lorsque qu'une liste de contrôle d'accès n'a aucune correspondance, cela signifie seulement qu'aucun trafic ne correspond aux conditions existant pour cette ligne donnée. La liste de contrôle d'accès surveille le trafic correspondant à trois hôtes spécifiques à destination de périphériques de destination très spécifiques. Tout autre trafic n'est pas autorisé par l'instruction implicite ACE « deny ip any any ».

20. À quoi change l'invite CLI après avoir entré la commande ip access-list standard aaa à partir du mode de configuration global?

- **Router(config-std-nacl)#**
- Router(config)#
- Router(config-router)#
- Router(config-line)#
- Router(config-if)#

21. Reportez-vous à l'illustration. Une nouvelle politique de réseau exige qu'une ACL refuse à tous les utilisateurs l'accès FTP et Telnet à un serveur de fichiers Corp. L'adresse du serveur de fichiers est 172.16.1.15 et tous les utilisateurs se voient attribuer des adresses dans le réseau 172.18.200.0/24. Après la mise en œuvre de l'ACL, personne dans le réseau de Corp ne peut accéder à aucun des serveurs. Quel est le problème?

```
Corp# show running-config

interface GigabitEthernet0/1
description Server Farm
ip address 172.16.1.1 255.255.255.0
ip access-group FileServerAccess out
!
<output omitted>
!
ip access-list extended FileServerAccess
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq ftp
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq ftp-data
deny tcp 172.18.200.0 0.0.0.255 host 172.16.1.15 eq telnet
!
```


- Les listes ACL nommées nécessitent l'utilisation de numéros de port.
- La liste de contrôle d'accès est appliquée à une mauvaise interface et dans la mauvaise direction.
- **L'ACL refuse implicitement l'accès à tous les serveurs.**
- Les listes ACL entrantes doivent être routées avant qu'elles ne soient traitées.

Explique: Les ACL nommées et numérotées ont un ACE de refus implicite à la fin de la liste. L'instruction de refus implicite bloque l'ensemble du trafic.

22. Considérez la liste d'accès suivante.

```
access-list 100 permit ip host 192.168.10.1 any

access-list 100 deny icmp 192.168.10.0 0.0.255 any echo

access-list 100 permit ip any any
```

Deux actions sont prises si le liste d'accès est placé entrant sur un routeur port Gigabit Ethernet qui a l'adresse IP 192.168.10.254 attribué? (Choisissez deux réponses.)

- **Une session Telnet ou SSH est autorisée à partir de n'importe quel périphérique sur le 192.168.10.0 dans le routeur avec cette liste d'accès attribuée.**
- Seules les connexions de couche 3 peuvent être effectuées à partir du routeur vers n'importe quel autre périphérique réseau.
- Seul le périphérique réseau attribué à l'adresse IP 192.168.10.1 est autorisé à accéder au routeur.
- **Les périphériques du réseau 192.168.10.0/24 peuvent effectuer un ping sur les périphériques du réseau 192.168.11.0.**
- Les périphériques du réseau 192.168.10.0/24 ne sont pas autorisés à répondre à des requêtes ping.

Explique: Le premier ACE permet au périphérique 192.168.10.1 d'effectuer des transactions TCP/IP avec n'importe quelle autre destination. Le second ACE empêche les périphériques du réseau 192.168.10.0/24 d'exécuter des commandes ping vers n'importe quel autre emplacement. Tout le reste est autorisé par le troisième ACE. Par conséquent, une session Telnet/SSH ou une réponse ping est autorisée à partir d'un périphérique sur le réseau 192.168.10.0/24.

23. Lors de quelle attaque TCP le cybercriminel tente-t-il de submerger un hôte cible au moyen de connexions TCP semi-ouvertes ?

- Attaque par réinitialisation
- Attaque par piratage de sessions
- **Attaque par inondation SYN**
- Attaque par analyse de ports

Explique: Lors d'une attaque par inondation SYN TCP, le hacker envoie à l'hôte cible un flot continu de requêtes de session SYN TCP avec une adresse IP source usurpée. L'hôte cible répond avec un paquet TCP-SYN-ACK à chacune des requêtes de session SYN et attend un TCP ACK qui n'arrivera jamais. Finalement, la cible est submergée par des connexions TCP semi-ouvertes.

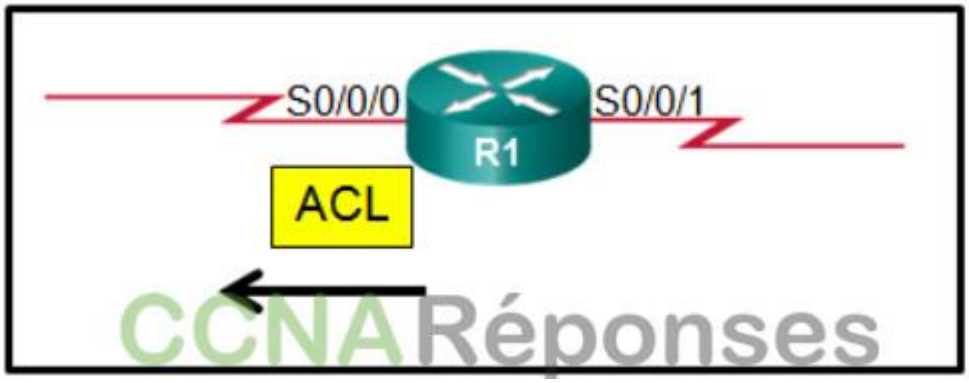
24. Quel protocole est attaqué lorsqu'un cybercriminel fournit une passerelle non valide afin de lancer une attaque de l'homme du milieu ?

- HTTP ou HTTPS
- **DHCP**
- ICMP
- DNS

Explique: Un cybercriminel peut configurer un serveur DHCP pirate qui fournit un ou plusieurs des éléments suivants :
Une passerelle par défaut incorrecte utilisée pour lancer une attaque de l'homme du milieu et permettre au hacker d'intercepter des données
Un serveur DNS incorrect en raison duquel l'utilisateur est redirigé vers un site web malveillant.
Une adresse IP de passerelle par défaut non valide qui provoque une attaque par déni de service sur le client DHCP

25. Reportez-vous à l'illustration. Un administrateur a configuré une liste ACL standard sur R1 et l'a appliqué à l'interface série 0/0/0 dans le sens sortant. Qu'arrive-t-il au trafic quittant l'interface série 0/0/0 qui ne correspond pas aux

instructions ACL configurés ?

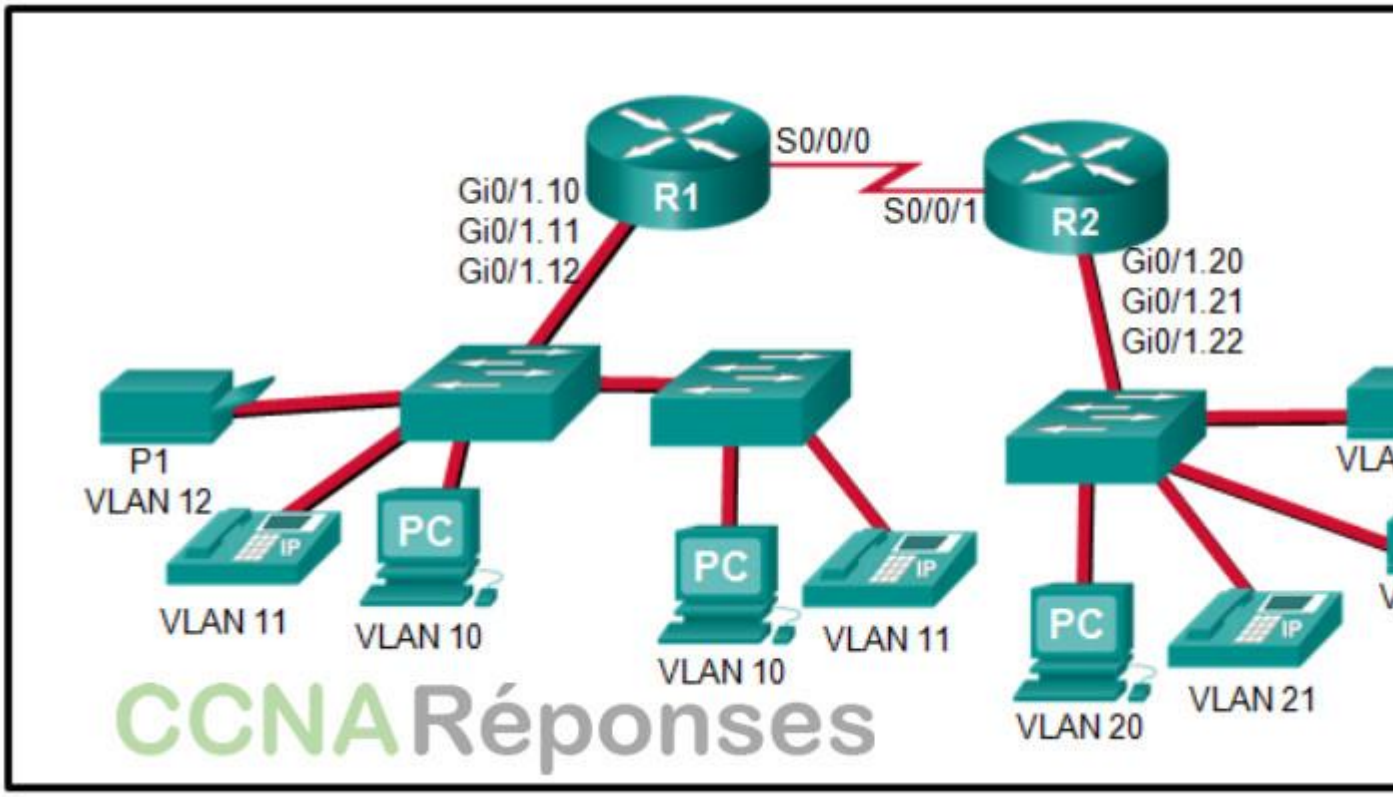


- L'action résultante est déterminée par l'adresse IP de destination.
- L'action résultante est déterminée par l'adresse IP de destination et le numéro de port.
- **le trafic est abandonné.**
- L'adresse IP source est vérifiée et, si une correspondance n'est pas trouvée, le trafic est acheminé vers l'interface série 0/0/1.

Explique: Le refus implicite est appliqué à tout trafic qui ne correspond pas à l'une des instructions d'une liste ACL, ce qui signifie que le trafic est supprimé.

26. Examinez l'illustration. Les interfaces Gigabit sur les deux routeurs ont été configurées avec les numéros de sous-interface correspondant aux numéros des VLAN qui leur sont connectés. Les PC sur le VLAN 10 doivent pouvoir imprimer sur l'imprimante P1 du VLAN 12. Les PC sur le VLAN 20 doivent pouvoir imprimer sur les imprimantes du VLAN 22. Dans quelle interface, et dans quelle direction, devez-vous placer une liste de contrôle d'accès standard permettant l'impression sur P1 à partir du VLAN de données 10, mais empêchant les PC du VLAN 20 d'utiliser l'imprimante P1 ? (Choisissez deux

réponses.)



- entrante
- R2 Gi0/1.20
- R2 S0/0/1
- **R1 Gi0/1.12**
- **sortante**
- R1 S0/0/0

Explique: Une liste de contrôle d'accès standard est généralement placée aussi près que possible du réseau de destination car les expressions de contrôle d'accès dans une liste de contrôle d'accès standard n'incluent pas les informations sur le réseau de destination.
La destination dans cet exemple est l'imprimante VLAN 12 qui a pour passerelle la sous-interface Gigabit 0/1/.12 du routeur R1. Un exemple de liste de contrôle d'accès standard qui permet uniquement l'impression à partir du VLAN données 10 (192.168.10.0/24) et d'aucun autre VLAN serait comme suit :
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny any
R1(config)# interface gigabitethernet 0/1.12
R1(config-if)# ip access-group 1 out

27. Quelle affirmation décrit une caractéristique des listes de contrôle d'accès IPv4 standard ?

- Elles sont configurées en mode de configuration d'interface.
- Elles peuvent être configurées de manière à filtrer le trafic en fonction des adresses IP source et des ports source.
- **Elles filtrent le trafic en fonction des adresses IP source uniquement.**
- Elles peuvent être créées avec un numéro, mais pas avec un nom.

Explique: Une liste de contrôle d'accès IPv4 standard peut filtrer le trafic en fonction des adresses IP source uniquement. Contrairement à une liste de contrôle d'accès étendue, elle ne peut pas filtrer le trafic en fonction des ports de couche 4. Cependant, les listes de contrôle d'accès standard et étendues peuvent toutes deux être identifiées par un numéro ou un nom, et toutes deux sont configurées en mode de configuration globale.

28. Quelle est la meilleure pratique lors de la configuration des ACL sur des lignes vty?

- Supprimer le mot de passe vty car l'ACL limite l'accès aux utilisateurs approuvés.
- Utiliser uniquement des listes d'accès étendues.
- Appliquer la commande ip access-group entrante.
- **Placer des restrictions identiques sur toutes les lignes vty.**

29. Reportez-vous à l'illustration. Un administrateur a d'abord configuré une liste ACL étendue comme indiqué par la sortie de la commande show access-lists . L'administrateur a ensuite modifié cette liste d'accès en exécutant les commandes ci-dessous.

```
Router# show access-lists
Extended IP access list 101
    10 deny tcp any any
    20 permit udp any any
    30 permit icmp any any
```

```
Router(config)# ip access-list extended 101

Router(config-ext-nacl)# no 20

Router(config-ext-nacl)# 5 permit tcp any any eq 22

Router(config-ext-nacl)# 20 deny udp any any
```

Quelles deux conclusions peut-on tirer de cette nouvelle configuration? (Choisissez deux.)

- **Les paquets SSH seront autorisés.**
- Tous les paquets TCP et UDP seront refusés.
- Les paquets Telnet seront autorisés.
- Les paquets TFTP seront autorisés.
- **Les paquets ping seront autorisés.**

Explique: Après la modification, la configuration finale est la suivante:
Router# show access-lists
Extended IP access list 101
5 permit tcp any any eq ssh
10 deny tcp any any
20 deny udp any any
30 permit icmp any any
Ainsi, seuls les paquets SSH et ICMP seront autorisés.

30. Quel ensemble d'entrées de contrôle d'accès permettrait à tous les utilisateurs du réseau 192.168.10.0/24 d'accéder à un serveur Web situé à l'adresse 172.17.80.1, sans toutefois les autoriser à utiliser le protocole Telnet ?

access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

access-list 103 deny tcp host 192.168.10.0 any eq 23
access-list 103 permit tcp host 192.168.10.1 eq 80

access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet

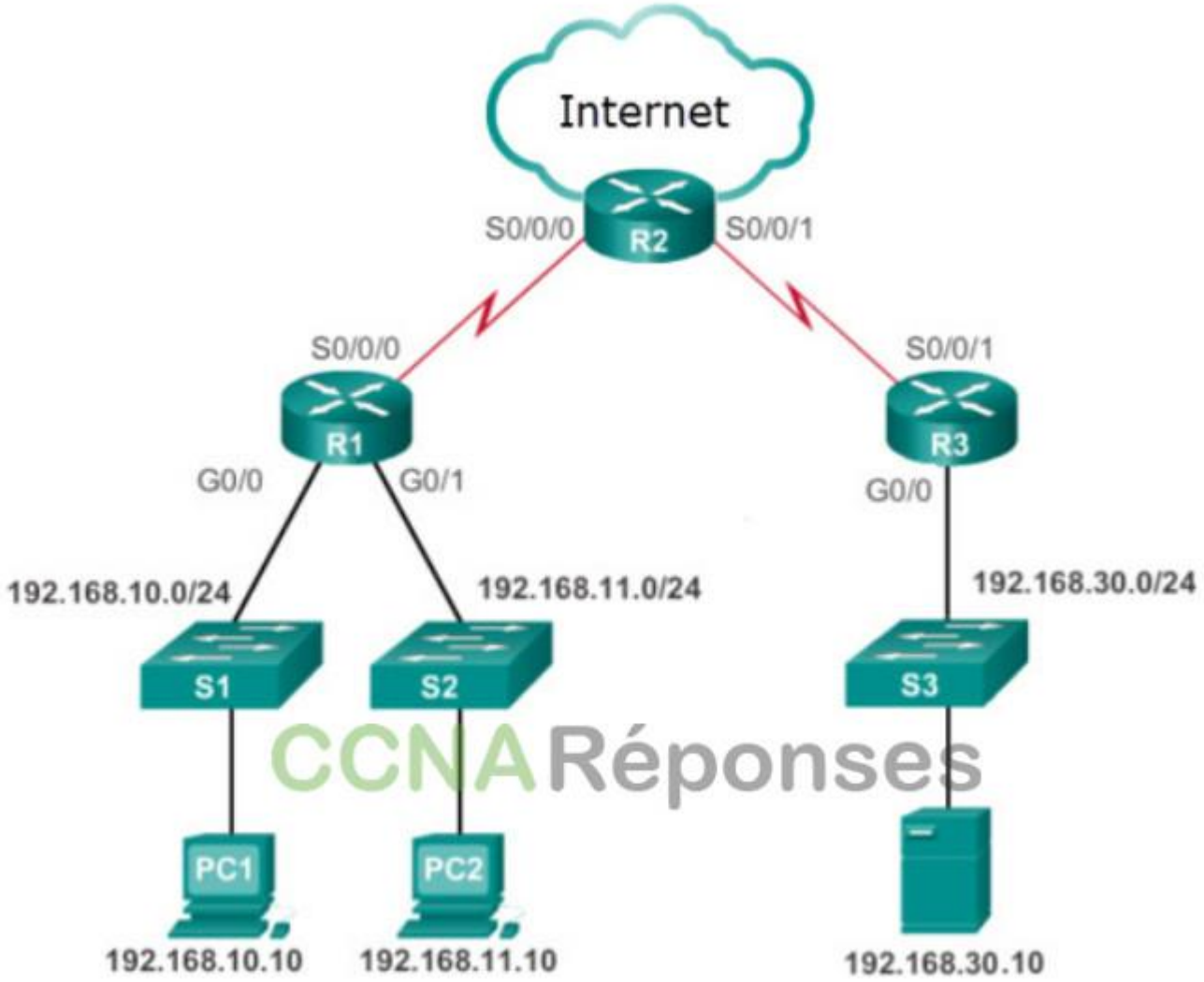
Explique: Pour qu'une liste de contrôle d'accès étendue respecte ces conditions, les éléments suivants doivent être inclus dans les entrées de contrôle d'accès :
numéro d'identification compris entre 100 et 199 ou 2000 et 2699
paramètre d'autorisation ou de refus
protocole
adresse source et caractère générique
adresse de destination et caractère générique
numéro de port ou nom

31. Quel est le terme utilisé pour décrire la garantie qu'il ne s'agit pas d'un faux message et qu'il provient réellement du propriétaire. ?

- des risques
- **L'authentification de l'origine**
- exploit
- atténuation

32. Reportez-vous à l'illustration. Le réseau 192.168.30.0/24 contient tous les serveurs de l'entreprise. La stratégie exige que le trafic des serveurs vers les deux réseaux 192.168.10.0 et 192.168.11.0 soit limité aux réponses pour les demandes d'origine. Quel est le meilleur type et placement ACL à utiliser dans cette situation

?



- ACL étendues entrantes sur R1 G0/0 et G0/1
- ACL étendue entrante sur R3 S0/0/1
- **ACL entrante étendue sur R3 G0/0**
- ACL entrante standard sur les lignes R1 vty

Explique: Les ACL standard autorisent ou refusent les paquets selon l'adresse IPv4 source uniquement. Comme tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situés le plus près possible de la destination.

Les ACL étendues autorisent ou refusent les paquets selon l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination et plus encore. Le filtrage des ACL étendus étant très spécifique, les ACL étendus doivent être situés le plus près possible de la source du trafic à filtrer. Un trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure de réseau.

33. Un technicien est chargé d'utiliser les ACLs pour sécuriser un routeur. Quand le technicien utiliserait-il l'option ou la commande de configuration access-class 20 in ?

- pour supprimer une liste ACL configurée

- **pour sécuriser l'accès administratif au routeur**
- pour appliquer une liste ACL standard à une interface
- pour supprimer une liste ACL d'une interface

34. Quelle affirmation caractérise avec précision l'évolution des menaces à la sécurité du réseau?

- Les premiers utilisateurs d'Internet se livraient souvent à des activités susceptibles de nuire à d'autres utilisateurs.
- Les architectes Internet ont prévu la sécurité du réseau dès le début.
- Les menaces sont devenues moins sophistiquées tandis que les connaissances techniques nécessaires à un attaquant ont augmenté.
- **Les menaces internes peuvent causer des dommages encore plus importants que les menaces externes.**

Explique: Les menaces internes peuvent être intentionnelles ou accidentelles et causent des dommages plus importants que les menaces externes car l'utilisateur interne a un accès direct au réseau interne de l'entreprise et aux données de l'entreprise.

35. Par quel type d'attaque un cybercriminel tente-t-il d'empêcher les utilisateurs légitimes d'accéder à des services réseau ?

- MITM
- **DoS**
- Piratage de session
- usurpation d'adresse

Explique: L'objectif d'un hacker qui lance une attaque par déni de service ou DoS est d'empêcher les utilisateurs légitimes d'accéder à des services réseau.

36. Dans quel type d'attaque des informations falsifiées sont-elles utilisées pour rediriger les utilisateurs vers des sites Internet malveillants ?

- **Empoisonnement du cache DNS**
- Empoisonnement du cache ARP
- Génération de domaine
- Amplification et réflexion DNS

Explique: Dans le cadre d'une attaque par empoisonnement du cache DNS, des informations falsifiées sont utilisées pour rediriger les utilisateurs vers des sites Internet malveillants à partir de sites légitimes.

37. Quelle exigence de communications sécurisées est assurée par la mise en œuvre d'algorithmes de génération de hachage MD5 ou SHA?

- non répudiation
- **Intégrité**
- Confidentialité
- Authentification

Explique: L'intégrité est garantie par la mise en œuvre de l'un des algorithmes de génération de hachage MD5 ou SHA. De nombreux réseaux modernes garantissent l'authentification avec des protocoles, par exemple le code HMAC. La confidentialité des données est garantie par des algorithmes de cryptage symétriques comme le DES, le 3DES et l'AES. La confidentialité des données peut également être garantie par l'utilisation d'algorithmes asymétriques comme le RSA et le PKI.

38. Quels sont les mots clés que vous pouvez utiliser dans une liste de contrôle d'accès pour remplacer un masque générique, ou un couple d'adresse et de masque générique? (Choisissez deux réponses.)

- **any**
- **host**
- some
- most
- gt
- all

Explique: Le mot-clé host est utilisé lors de l'utilisation d'une adresse IP de périphérique spécifique dans une liste ACL. Par exemple, la commande deny host 192.168.5.5 est la même que la commande deny 192.168.5.5 0.0.0.0 . Le mot-clé any est utilisé pour autoriser n'importe quel masque qui répond aux critères. Par exemple, la commande permit any est la même que la commande permit 0.0.0.0 255.255.255.255 .

39. Quelle est la méthode la plus rapide pour supprimer une entrée ACE unique d'une liste de contrôle d'accès nommée ?

- Utiliser la commande no access-list pour supprimer l'ensemble de la liste de contrôle d'accès, puis la recréer sans une entrée ACE.
- **Utiliser le mot clé no et le numéro de séquence de l'entrée ACE à supprimer.**
- Créer une nouvelle liste de contrôle d'accès avec un numéro différent et appliquer la nouvelle liste de contrôle d'accès à l'interface du routeur.
- Copier la liste de contrôle d'accès dans un éditeur de texte, supprimer l'entrée ACE, puis copier à nouveau la liste de contrôle d'accès sur le routeur.

Explique: Les entrées ACE d'une liste ACL nommée peuvent être supprimées en utilisant la commande no suivie du numéro de séquence.

40. Quel ACE autorisera un paquet provenant de n'importe quel réseau et destiné à un serveur Web à 192.168.1.1?

- access-list 101 permit tcp host 192.168.1.1 any eq 80
- access-list 101 permit tcp host 192.168.1.1 eq 80 any
- **access-list 101 permit tcp any host 192.168.1.1 eq 80**
- access-list 101 permit tcp any eq 80 host 192.168.1.1

41. Consultez la figure. La liste de contrôle d'accès nommée « Gestionnaires » existe déjà dans le routeur. Que se passera-t-il lorsque l'administrateur réseau émettra les commandes indiquées dans la figure ?

```
Router(config)# ip access-list extended Managers
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq telnet
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq www
Router(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq ftp
```

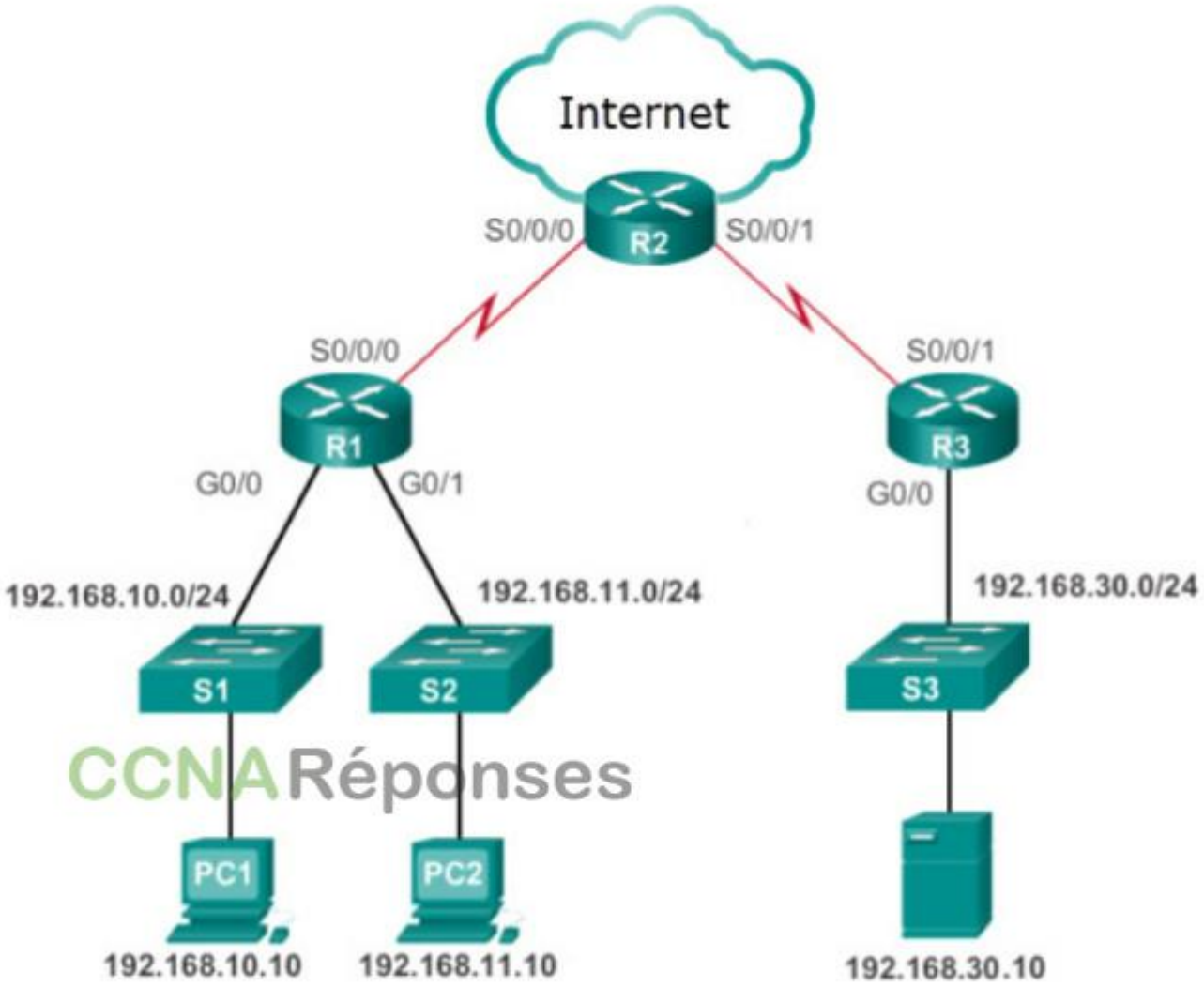

- **Les commandes seront ajoutées à la fin de la liste de contrôle d'accès Gestionnaires existante.**

- Les nouvelles commandes seront ajoutées au début de la liste de contrôle d'accès Gestionnaires existante.
- Les commandes remplaceront la liste de contrôle d'accès Gestionnaires existante.
- L'administrateur réseau recevra un message d'erreur stipulant que la liste de contrôle d'accès existe déjà.

42. Quel est le terme utilisé pour décrire les criminels contraires à l'éthique qui compromettent la sécurité de l'ordinateur et du réseau pour un gain personnel ou pour des raisons malveillantes?

- testeur de vulnérabilité
- hacktivistes
- script kiddies (hackers néophytes)
- **pirates au chapeau noir**

43. Reportez-vous à l'illustration. La société a fourni des téléphones IP aux employés sur le réseau 192.168.10.0/24 et le trafic vocal aura besoin de priorité sur le trafic de données. Quel est le meilleur type et placement ACL à utiliser dans cette situation?



- **ACL entrante étendue sur R3 G0/0**
- ACL entrante étendue sur R3 G0/0
- ACL entrante standard sur R1 G0/1

- ACL entrante standard sur les lignes R1 vty

Explique: Les ACL standard autorisent ou refusent les paquets selon l'adresse IPv4 source uniquement. Comme tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situés le plus près possible de la destination.

Les ACL étendues autorisent ou refusent les paquets selon l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination et plus encore. Le filtrage des ACL étendus étant très spécifique, les ACL étendus doivent être situés le plus près possible de la source du trafic à filtrer. Un trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure de réseau.

44. Un technicien est chargé d'utiliser les ACL pour sécuriser un routeur. Quand le technicien utiliserait-il l'option ou la commande de configuration no ip access-list 101 ?

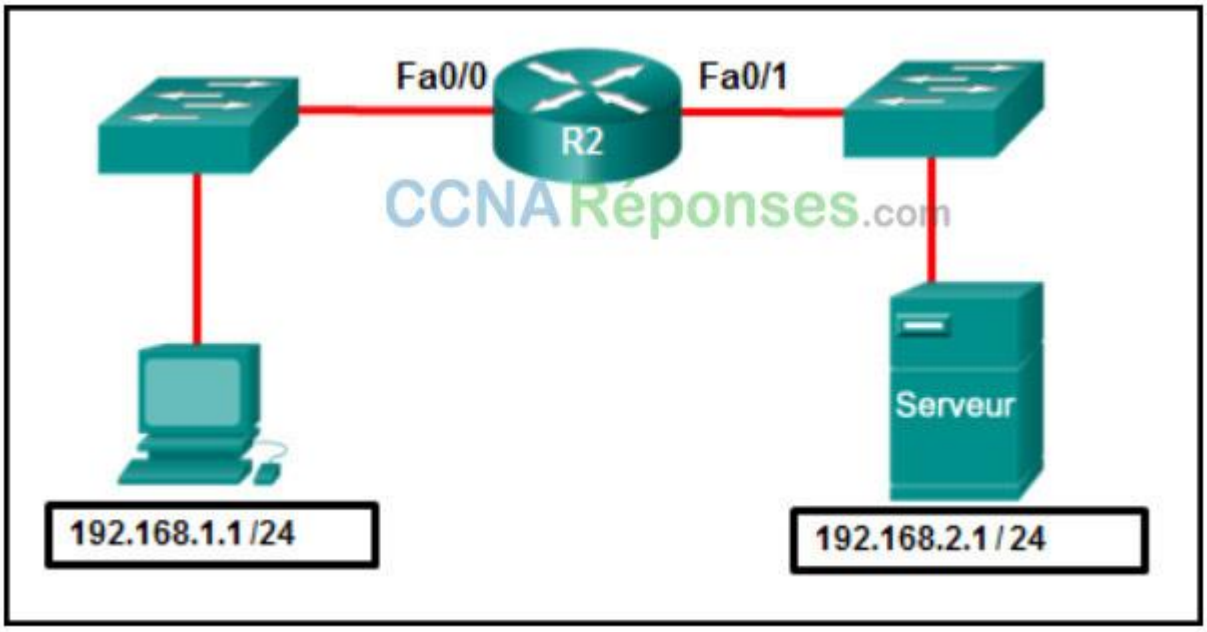
- pour appliquer une liste ACL à toutes les interfaces de routeur
- pour sécuriser l'accès administratif au routeur
- **pour supprimer une liste ACL configurée**
- pour supprimer toutes les ACL du routeur

45. Quelle affirmation décrit la différence entre le fonctionnement d'une liste de contrôle d'accès entrante et le fonctionnement d'une liste de contrôle d'accès sortante ?

- Sur une interface réseau, il est possible de configurer plusieurs listes de contrôle d'accès entrantes, mais une liste de contrôle d'accès sortante uniquement.
- **Les listes de contrôle d'accès entrantes sont traitées avant que les paquets soient acheminés, alors que les listes de contrôle d'accès sortantes sont traitées une fois le routage terminé.**
- Contrairement aux listes de contrôle d'accès sortantes, les listes de contrôle d'accès entrantes peuvent être utilisées pour filtrer les paquets selon plusieurs critères.
- Les listes de contrôle d'accès entrantes peuvent être utilisées indifféremment sur les routeurs et les commutateurs, tandis que les listes de contrôle d'accès sortantes peuvent être utilisées uniquement sur les routeurs.

Explique: Avec une liste de contrôle d'accès entrante, les paquets qui arrivent sont traités avant d'être acheminés. Avec une liste de contrôle d'accès sortante, les paquets sont d'abord acheminés vers l'interface de sortie avant d'être traités. De ce fait, le traitement des éléments entrants est plus efficace du point de vue du routeur. La structure, les méthodes de filtrage et les limites (sur une interface, une seule liste de contrôle d'accès entrante et une seule liste de contrôle d'accès sortante peuvent être configurées) sont identiques pour les deux types de liste.

46. Reportez-vous à l'illustration. Un administrateur ne souhaite autoriser l'accès au serveur 192.168.2.1 /24 qu'à l'hôte 192.168.1.1 /24. Quelles sont les trois commandes utilisant les bonnes pratiques relatives au placement des ACL qui permettront de réaliser cette action ? (Choisissez trois propositions.)



- R2(config)# access-list 101 permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
- R2(config)# access-list 101 permit ip any any
- R2(config)# interface fastethernet 0/1
- **R2(config)# access-list 101 permit ip host 192.168.1.1 host 192.168.2.1**
- R2(config-if)# ip access-group 101 out
- **R2(config)# interface fastethernet 0/0**
- **R2(config-if)# ip access-group 101 in**

Explique: Une ACL étendue est placée aussi près que possible de la source du trafic. Dans ce cas, elle est placée en direction entrante sur l'interface fa0/0 de R2 pour le trafic qui entre dans le routeur en provenance de l'hôte dont l'adresse IP est 192.168.1.1 et qui se dirige vers le serveur dont l'adresse IP est 192.168.2.1.

47. Quel est le terme utilisé pour décrire les pirates attaquant du chapeau gris qui protestent publiquement des organisations ou des gouvernements en publiant des articles, des vidéos, des fuites d'informations sensibles et en effectuant des attaques réseau?

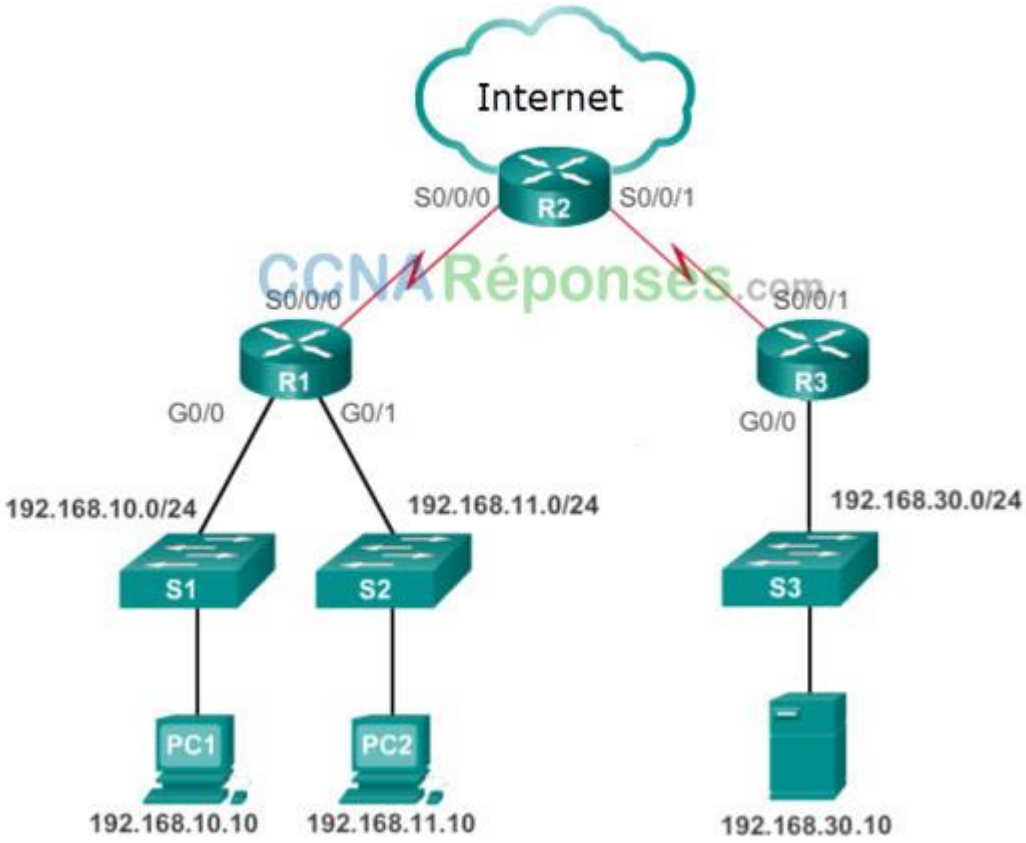
- Pirates au chapeau blanc
- Pirates au chapeau gris
- Pirates Parrainés par l'État
- **hacktivistes**

48. Quelle attaque implique des acteurs de menace se positionnant entre une source et une destination dans le but de surveiller, capturer et contrôler la communication de manière transparente?

- attaque par déni de service (DoS)
- Attaque par inondation SYN
- **attaque d'homme-au-milieu**
- Attaque ICMP

Explique: L'attaque de l'homme-au-milieu est une attaque liée à l'IP courante où les acteurs de menace se positionnent entre une source et une destination pour surveiller, capturer et contrôler la communication de manière transparente.

49. Reportez-vous à l'illustration. De nombreux employés perdent du temps à accéder aux médias sociaux sur leurs ordinateurs de travail. La société veut arrêter cet accès. Quel est le meilleur type et placement ACL à utiliser dans cette situation?



- ACL sortante standard sur l'interface WAN R2 vers Internet
- **ACL étendues entrantes sur R1 G0/0 et G0/1**
- ACL sortante standard sur R2 S0/0/0
- ACL étendue sortante sur l'interface WAN R2 vers l'internet

Explique: Les ACL standard autorisent ou refusent les paquets selon l'adresse IPv4 source uniquement. Comme tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situés le plus près possible de la destination.

Les ACL étendues autorisent ou refusent les paquets selon l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination et plus encore. Le filtrage des ACL étendus étant très spécifique, les ACL étendus doivent être situés le plus près possible de la source du trafic à filtrer. Un trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure de réseau.

50. Quel est le terme utilisé pour décrire un danger potentiel pour les actifs, les données ou les fonctionnalités réseau d'une entreprise?

- **menace**
- exploit
- vulnérabilité

- Algorithmes de chiffrement asymétrique

51. Un technicien est chargé d'utiliser les ACLs pour sécuriser un routeur. Quand le technicien utiliserait-il l'option ou la commande de configuration ip access-group 101 ?

- pour sécuriser l'accès administratif au routeur
- pour créer une entrée dans une liste ACL numérotée
- pour appliquer une liste ACL à toutes les interfaces de routeur
- **pour appliquer une ACL étendue à une interface**

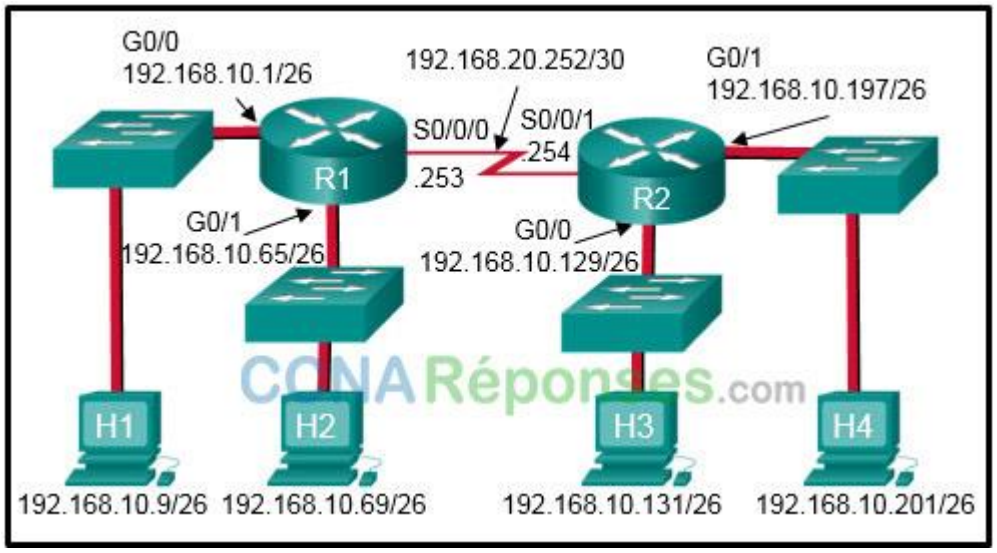
52. Reportez-vous à l'illustration. Un administrateur réseau configure une liste ACL sur le routeur. Quelle affirmation décrit le résultat de la configuration ?

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-list 120 permit tcp host 192.168.25.18 host 172.16.45.16 eq 22
Router(config)# line vty 0 4
Router(config-line)# password admin-in
Router(config-line)# login local
Router(config-line)# access-class 120 in
Router(config-line)# end
Router#
```


- Une connexion Telnet est autorisée à partir d'un poste de travail avec IP 172.16.45.16 vers un périphérique avec IP 192.168.25.18.
- **Une connexion SSH est autorisée à partir d'un poste de travail avec IP 192.168.25.18 vers un périphérique avec IP 172.16.45.16.**
- Une connexion Telnet est autorisée à partir d'un poste de travail avec IP 192.168.25.18 à un périphérique avec IP 172.16.45.16.
- Une connexion SSH est autorisée à partir d'un poste de travail avec IP 172.16.45.16 vers un périphérique avec IP 192.168.25.18.

Explique: Dans une liste ACL étendue, la première adresse est l'adresse IP source et la seconde est l'adresse IP de destination. Le port TCP numéro 22 est un numéro de port bien connu réservé aux connexions SSH. Les connexions Telnet utilisent le port TCP numéro 23.

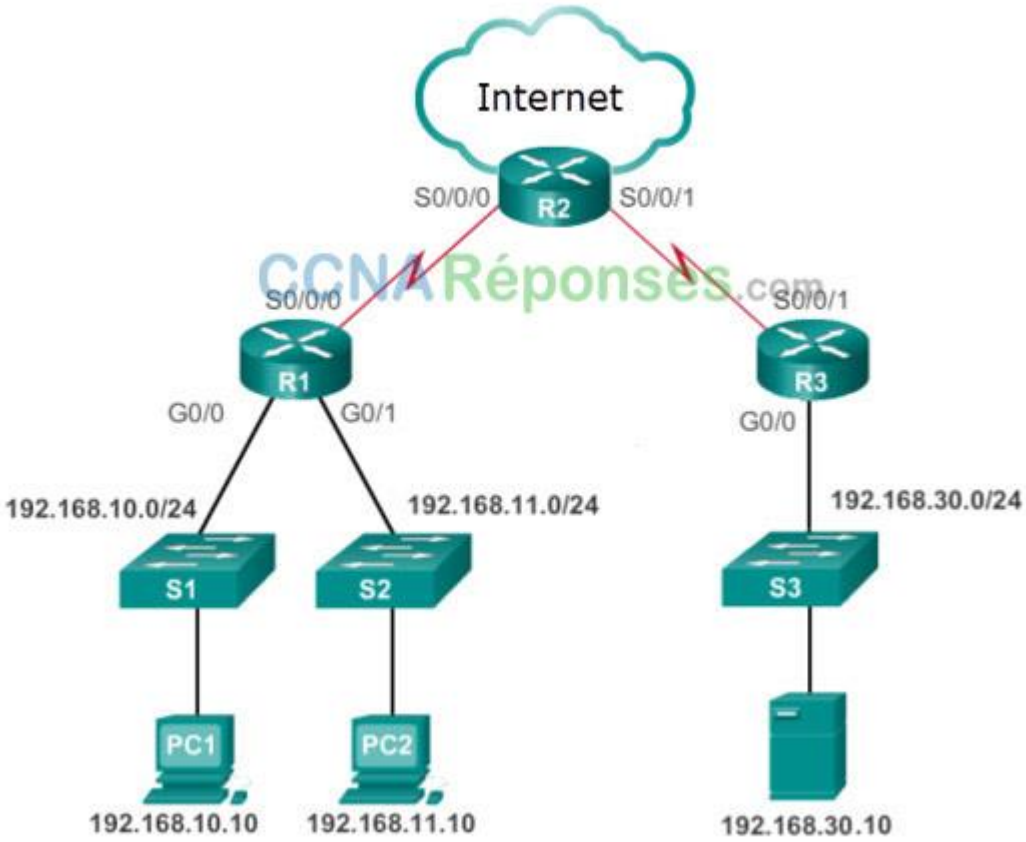
53. Reportez-vous à l'illustration. Quelles deux ACL permettraient uniquement aux deux réseaux LAN connectés à R1 d'accéder au réseau qui se connecte à l'interface R2 G0/1 ? (Choisissez deux réponses.)



- access-list 3 permit 192.168.10.128 0.0.0.63
- **access-list 1 permit 192.168.10.0 0.0.0.127**
- **access-list 5 permit 192.168.10.0 0.0.0.63**
  access-list 5 permit 192.168.10.64 0.0.0.63
- access-list 4 permit 192.168.10.0 0.0.0.255
- access-list 2 permit host 192.168.10.9
  access-list 2 permit host 192.168.10.69

Explique: La commande **permit 192.168.10.0 0.0.127** ignore les positions de bits 1 à 7, ce qui signifie que les adresses 192.168.10.0 à 192.168.10.127 sont autorisées. Les deux ACE du **permis 192.168.10.0 0.0.63** et du **permis 192.168.10.64 0.0.63** permettent la même plage d'adresses par le biais du routeur.

54. Reportez-vous à l'illustration. L'administrateur réseau a une adresse IP 192.168.11.10 et a besoin d'un accès pour gérer R1. Quel est le meilleur type et placement ACL à utiliser dans cette situation?



- ACL sortante standard sur R2 S0/0/0
- ACL entrante standard sur l'interface WAN R2 se connectant à l'internet
- **ACL entrante standard sur les lignes R1 vty**
- ACL étendue entrante sur R2 S0/0/0

Explique: Les ACL standard autorisent ou refusent les paquets selon l'adresse IPv4 source uniquement. Comme tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situés le plus près possible de la destination.

Les ACL étendues autorisent ou refusent les paquets selon l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination et plus encore. Le filtrage des ACL étendus étant très spécifique, les ACL étendus doivent être situés le plus près possible de la source du trafic à filtrer. Un trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure de réseau.

55. Si un algorithme asymétrique utilise une clé publique pour chiffrer les données, quel outil est utilisé pour la déchiffrer ?

- **Une clé privée**
- DH
- Un certificat numérique
- Une autre clé publique

Explique: Lorsqu'un algorithme asymétrique est utilisé, les clés privées et publiques sont utilisées pour le cryptage. L'une de ces deux clés peut être utilisée pour le cryptage, mais la clé appariée complémentaire doit être utilisée pour le décryptage.

Par exemple, si une clé publique est utilisée pour le cryptage, alors la clé privée doit être utilisée pour le décryptage.

56. Un technicien est chargé d'utiliser les listes ACL pour sécuriser un routeur. Quand le technicien utiliserait-il l'option ou la commande de configuration ip access-group 101 ?

- **pour appliquer une ACL étendue à une interface**
- pour sécuriser l'accès administratif au routeur
- pour afficher tout le trafic restreint
- pour sécuriser le trafic de gestion dans le routeur