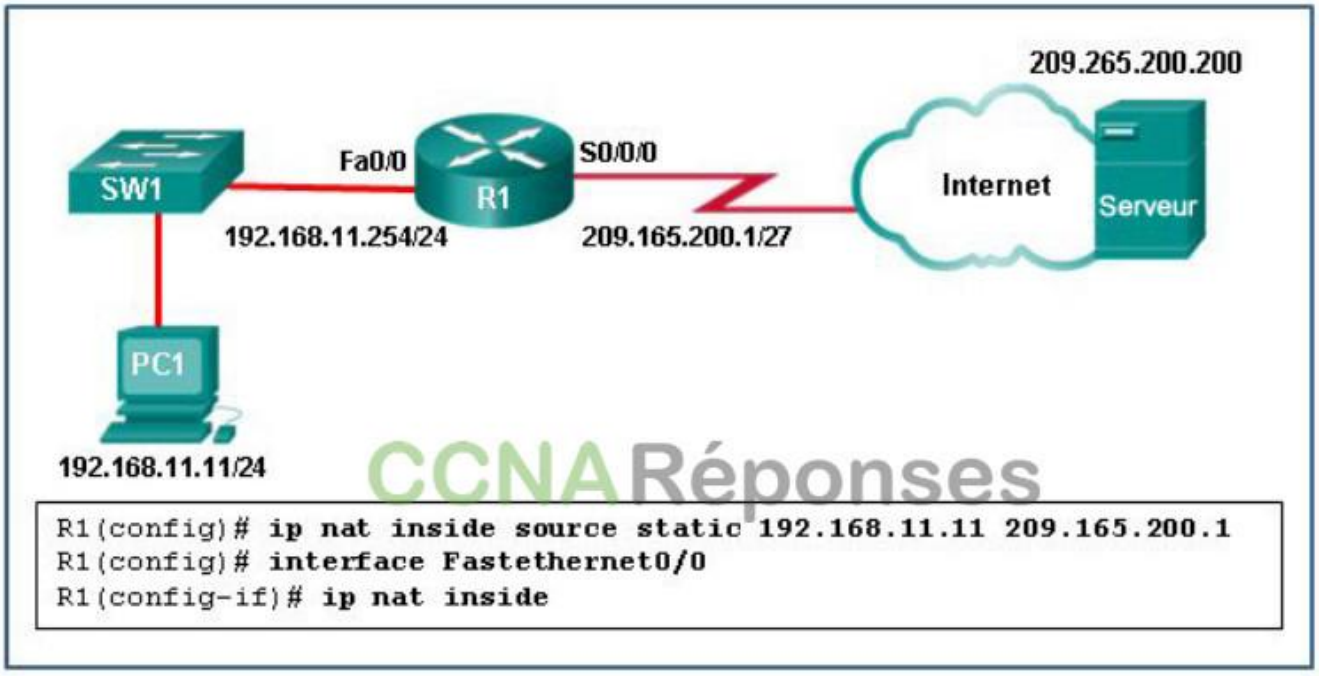
Modules 6 – 8: WAN Concepts Exam Français

Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN Réponses

1. Examinez l'illustration. Que faut-il faire pour terminer la configuration de la NAT statique sur R1 ?

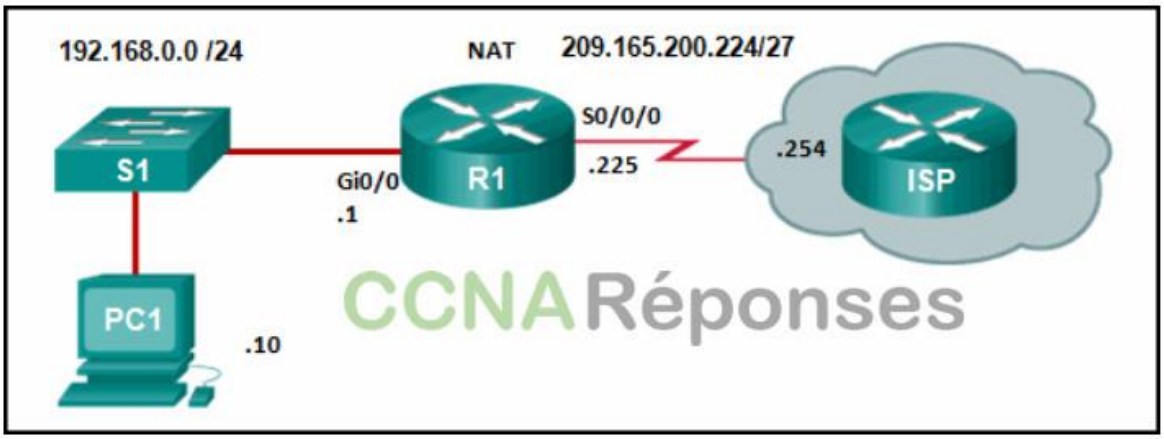


Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 1

- R1 doit être configuré avec la commande ip nat inside source static 209.165.200.200 192.168.11.11 .
- R1 doit être configuré avec la commande ip nat inside source static 209.165.200.1 192.168.11.11 .
- **L'interface S0/0/0 doit être configurée avec la commande ip nat outside .**
- L'interface Fa0/0 doit être configurée avec la commande no ip nat inside .

Explique: Pour que les traductions NAT fonctionnent correctement, des interfaces à la fois interne et externe doivent être configurées pour la traduction NAT sur le routeur.

2. Reportez-vous à l'illustration. Du point de vue de R1, le routeur NAT, quelle adresse est l'adresse globale interne?

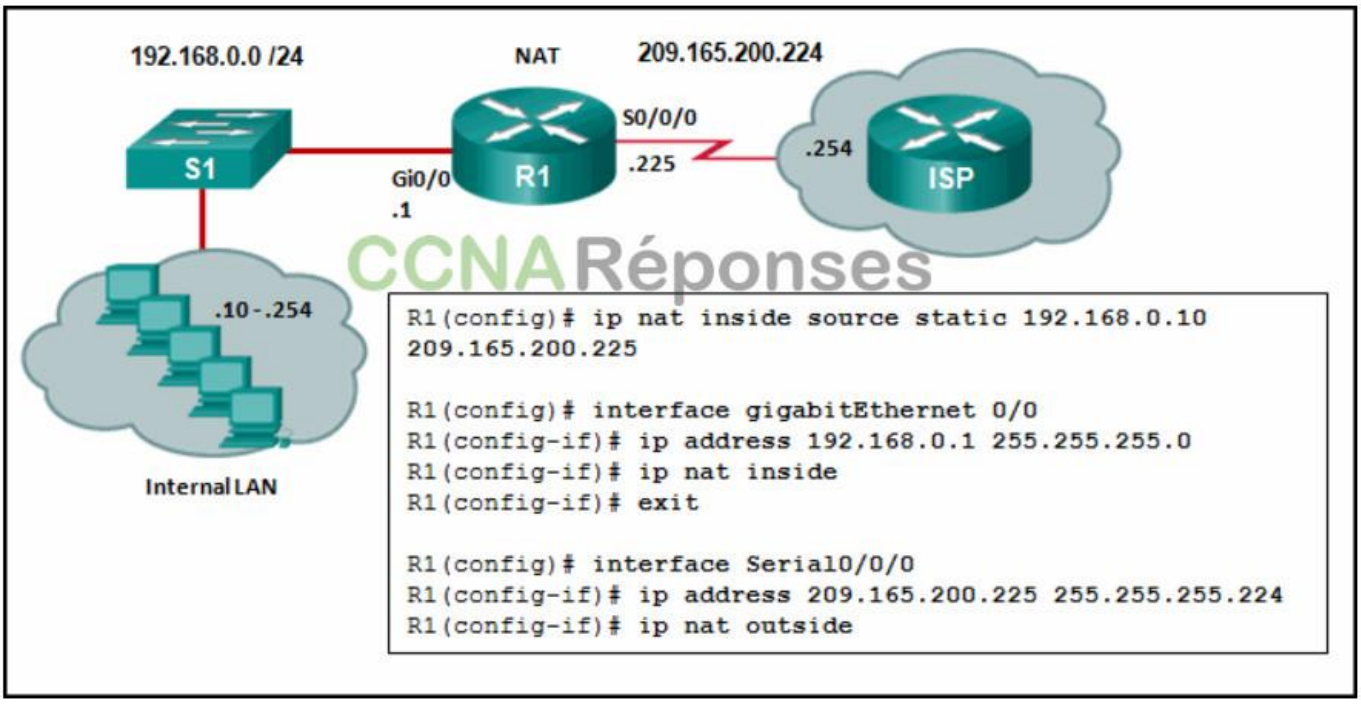


Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 2

- 192.168.0.10
- 209.165.200.254
- **209.165.200.225**
- 192.168.0.1

Explique: Il existe quatre types d'adresses dans la terminologie NAT.
Inside local address
Inside global address
Outside local address
Outside global address
L'adresse globale interne de PC1 est l'adresse que le FAI voit comme l'adresse source des paquets, qui est dans cet exemple l'adresse IP de la série interface de R1, 209.165.200.224.

3. Reportez-vous à l'illustration. Compte tenu des commandes comme indiqué, combien d'hôtes sur le réseau local interne hors R1 peuvent avoir des traductions NAT simultanées sur R1?



- **1**
- 244
- 255
- 10

Explique: La configuration NAT sur R1 est NAT statique qui traduit une seule adresse IP interne, 192.168.0.10 en une seule adresse IP publique, 209.165.200.255. Si d'autres hôtes ont besoin de traduction, un pool NAT d'adresse globale interne ou de surcharge doit être configuré.

4. Associez les étapes aux actions utilisées lorsqu'un hôte interne dont l'adresse IP est 192.168.10.10 tente d'envoyer un paquet à un serveur externe dont l'adresse IP est 209.165.200.254 via un routeur R1 exécutant la NAT dynamique. (Les options ne doivent pas être toutes utilisées.)

Explique: La traduction d'adresses IP de 209.65.200.254 à 192.168.10.10 a lieu lorsque la réponse revient du serveur.

5. Quel inconvénient l'utilisation de la traduction PAT des deux côtés de la transmission présente-t-elle ?

- La sécurité de la communication en pâtit.
- L'adressage IPv4 d'hôte est complexe.
- **La traçabilité IPv4 de bout en bout est perdue.**
- La flexibilité des connexions à Internet est réduite.

Explique: Avec l'utilisation de la NAT, particulièrement de la PAT, la traçabilité de bout en bout est perdue. En effet, l'adresse IP d'hôte dans les paquets est convertie pendant une transmission lorsqu'elle sort du réseau et lorsqu'elle entre dans le réseau. L'utilisation de la NAT/PAT, la flexibilité des connexions à Internet et la sécurité sont réellement améliorées. L'adressage IPv4 d'hôte est assuré par le protocole DHCP, il n'est pas lié à la traduction NAT/PAT.

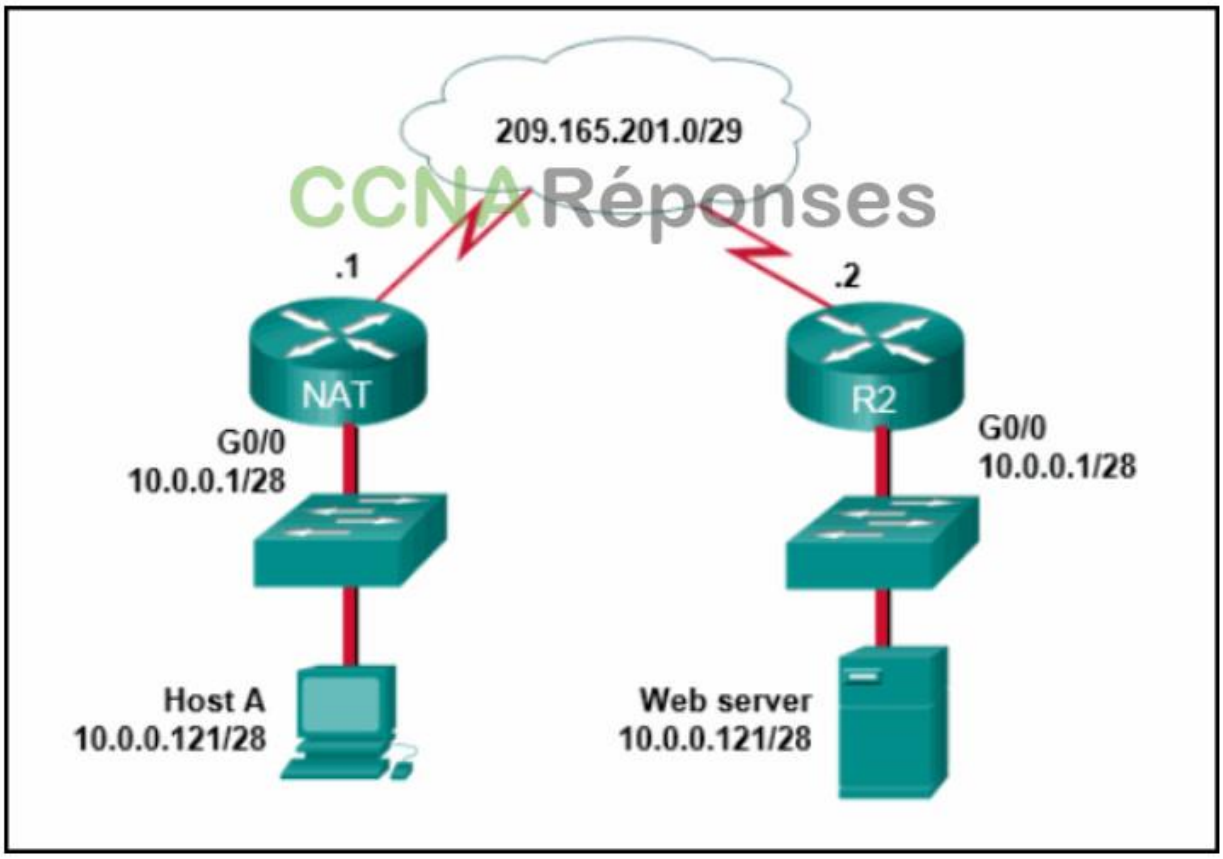
6. Reportez-vous à l'illustration. Sur la base de la sortie affichée, quel type de NAT a été implémenté?

```
R1# show ip nat translations
Pro Inside global         Inside local   Outside local      Outside global
tcp 209.165.200.225:1405 10.6.15.2:1405 209.165.202.141:80 209.165.202.141:80
tcp 209.165.200.225:1406 10.6.15.1:1406 198.51.100.3:80    198.51.100.3:80
```

- NAT statique avec une entrée
- NAT dynamique avec un pool de deux adresses IP publiques
- **PAT à l'aide d'une interface externe**
- NAT statique avec un pool NAT

Explique: La sortie montre qu'il y a deux adresses globales internes qui sont les identique mais qui ont des numéros de port différents. Le seul numéro de port de temps est affiché lorsque PAT est utilisé. Le même résultat serait indicatif de PAT qui utilise un pool d'adresses. PAT avec un pool d'adresses est approprié lorsque l'entreprise a besoin de plus de 4000 traductions simultanées.

7. Reportez-vous à l'illustration. Du point de vue des utilisateurs derrière le routeur NAT, quel type d'adresse NAT est 209.165.201.1?



Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 11

- **Globale interne**
- Locale externe
- Locale interne
- Globale externe

Explique: Du point de vue des utilisateurs derrière la NAT, les adresses globales internes sont utilisées par des utilisateurs externes pour atteindre des hôtes internes. Les adresses locales internes sont celles attribuées à des hôtes internes. Les adresses globales externes sont les adresses des destinations sur le réseau externe. Les adresses locales externes sont les adresses privées réelles des hôtes de destination derrière d'autres périphériques NAT.

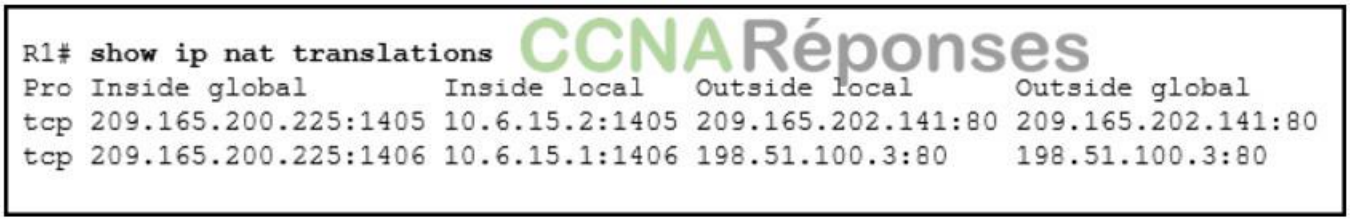
8. Quel est l'objectif du mot clé overload dans la commande iip nat inside source list 1 pool NAT_POOL overload ?

- Il permet à une liste d'hôtes internes de communiquer avec un groupe spécifique d'hôtes externes.
- **Il permet à de nombreux hôtes internes de partager une ou quelques adresses globales internes.**
- Il permet aux hôtes internes d'utiliser un pool d'adresses globales internes.
- Il permet aux hôtes externes d'établir des sessions avec des hôtes internes.

Explique: La NAT dynamique utilise un pool d'adresses globales internes qui sont attribuées aux sessions sortantes. Si dans le pool le nombre d'hôtes internes est supérieur aux adresses publiques, l'administrateur peut activer la traduction d'adresse de port en ajoutant le mot clé overload . Grâce à la traduction d'adresse de port, plusieurs hôtes internes peuvent partager une adresse globale interne unique,

car le périphérique NAT suit les sessions individuelles par numéro de port de la couche 4.

9. Reportez-vous à l'illustration. Quelle adresse source est utilisée par le routeur R1 pour les paquets transmis sur Internet ?

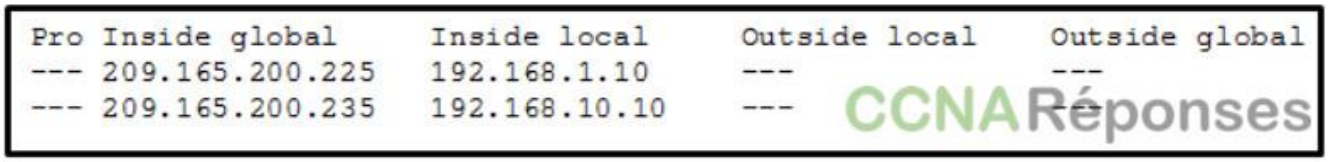


Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 14

- 198.51.100.3
- **209.165.200.225**
- 209.165.202.141
- 10.6.15.2

Explique: L'adresse source des paquets transmis par le routeur sur Internet sera l'adresse globale interne 209.165.200.225. Il s'agit de l'adresse en laquelle les adresses internes du réseau 10.6.15.0 seront traduites par la NAT.

10. Examinez l'illustration. D'après le résultat présenté dans cette illustration, quels énoncés sont exacts ? (Choisissez deux réponses.)



Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 17

- **L'hôte dont l'adresse est 209.165.200.235 répond aux requêtes en utilisant l'adresse source 192.168.10.10.**
- L'hôte dont l'adresse est 209.165.200.235 répond aux requêtes en utilisant l'adresse source 209.165.200.235.
- **Ce résultat est celui de la commande show ip nat translations .**
- Le trafic dont l'adresse de destination est celle d'un serveur Web public provient de l'adresse IP 192.168.1.10.
- Ce résultat est celui de la commande show ip nat statistics .

Explique: Le résultat affiché dans la présentation est le résultat de la commande show ip nat translations . Des entrées NAT statiques sont toujours présentes dans la table NAT, tandis que les entrées dynamiques expireront par la suite.

11. Quelles sont les deux technologies catégorisées comme infrastructures WAN privées ? (Choisissez deux propositions.)

- DSL
- **MetroE**
- Câble
- **Frame Relay**

- VPN

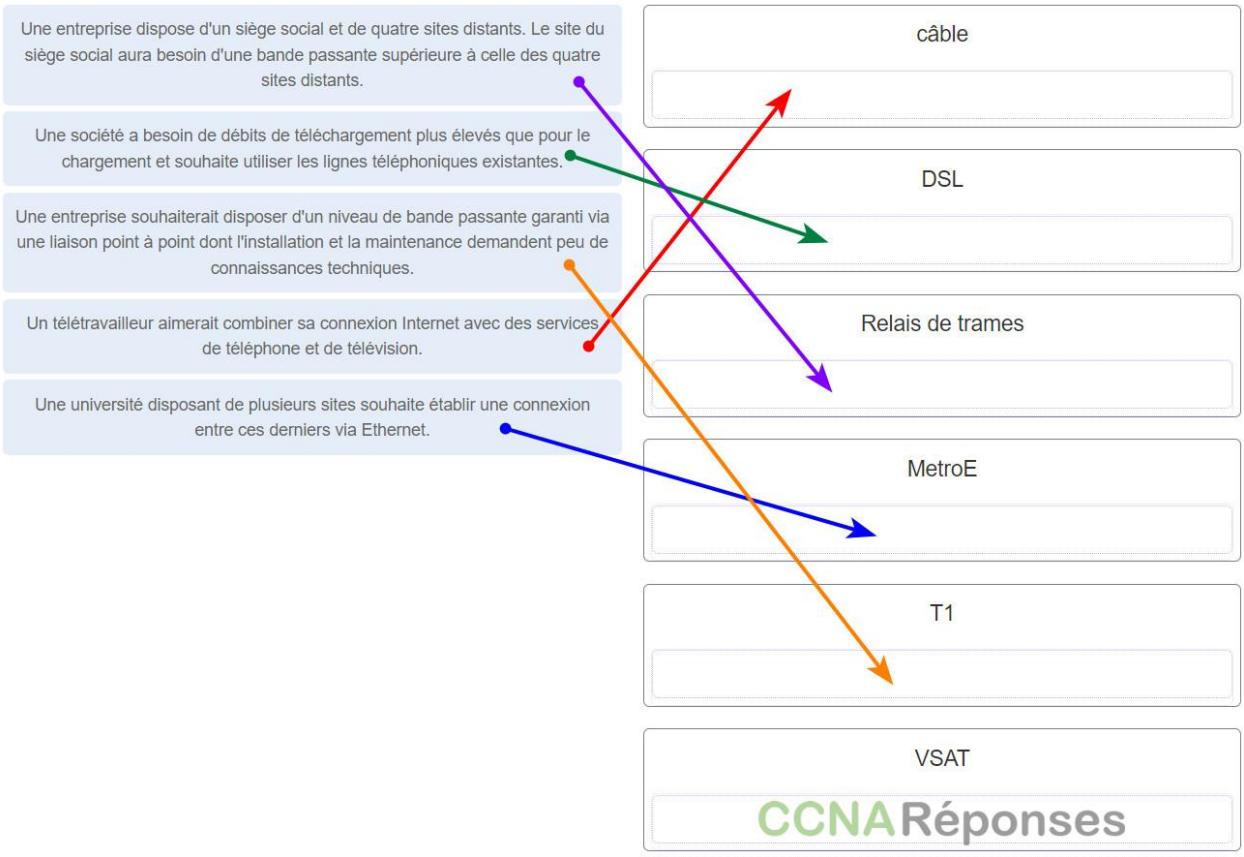
Explique: Les technologies WAN privées comprennent les lignes louées, les connexions commutées, le RNIS, le relais de trames, l'ATM, le WAN Ethernet (par exemple MetroE), MPLS et VSAT.

12. Quel scénario de réseau nécessite l'utilisation d'un WAN ?

- Les employés doivent accéder aux pages Web hébergées sur les serveurs Web de l'entreprise dans la DMZ au sein de leur bâtiment.
- **Lors de leurs déplacements, les employés doivent se connecter au serveur de messagerie de l'entreprise par l'intermédiaire d'un VPN.**
- Les stations de travail des employés doivent obtenir des adresses IP attribuées dynamiquement.
- Les employés de la filiale ont besoin de partager des fichiers avec le siège social qui se trouve dans un autre bâtiment, et ce, sur le même réseau de campus.

Explique: Lorsque des employés en déplacement doivent se connecter à un serveur de messagerie de l'entreprise par le biais d'une connexion WAN, le VPN crée un tunnel sécurisé entre l'ordinateur portable de l'employé et le réseau de l'entreprise par l'intermédiaire de la connexion WAN. L'obtention d'adresses IP dynamiques à l'aide du protocole DHCP est une fonction de la communication LAN. Le partage de fichiers entre des bâtiments distincts sur un campus d'entreprise est obtenu grâce à l'infrastructure LAN. Une DMZ est un réseau protégé au sein de l'infrastructure LAN de l'entreprise.

13. Reliez le scénario à la solution WAN adaptée. (Les options ne sont pas toutes utilisées.)



14. Dans quel cas une entreprise déciderait-elle de mettre en œuvre un WAN d'entreprise ?

- **Lorsque ses employés sont répartis sur plusieurs filiales**
- Lorsque l'entreprise décide de sécuriser son LAN d'entreprise
- Lorsque le nombre d'employés dépasse la capacité du LAN
- Lorsqu'il est prévu que le réseau englobe plusieurs bâtiments

Explique: Les WAN couvrent une plus grande zone géographique que les LAN. En conséquence, si des employés sont répartis entre plusieurs sites, la mise en œuvre de technologies WAN serait nécessaire pour connecter ces sites. Les clients auront accès aux services internet d'entreprise par l'intermédiaire d'un WAN public implémenté par un fournisseur de services et non par l'entreprise elle-même. Si le nombre d'employés augmente, la taille du LAN doit également croître. Un WAN n'est pas requis, à moins que les employés ne soient localisés dans des sites distants. La sécurité du LAN n'est pas liée à la décision d'implémenter un WAN.

15. Quel algorithme est utilisé avec IPsec pour assurer la confidentialité des données?

- Diffie-Hellman
- **AES**
- SHA
- RSA
- MD5

Explique: Le cadre de travail IPsec utilise divers protocoles et algorithmes pour assurer la confidentialité des données, l'intégrité des données , l'authentification et l'échange de clés sécurisé. MD5 et SHA sont deux algorithmes populaires utilisés pour garantir que les données ne sont pas interceptées et modifiées (intégrité des données). AES est un protocole de cryptage et assure la confidentialité des données. DH (Diffie-Hellman) est un algorithme utilisé pour l'échange de clés. RSA est un algorithme utilisé pour l'authentification.

16. Quelle solution VPN permet d'utiliser un navigateur Web pour établir un tunnel VPN d'accès distant sécurisé vers l'ASA?

- **SSL sans client**
- site à site à l'aide d'une clé prépartagée
- site à site à l'aide d'une ACL
- SSL basé sur le client

Explique: Lorsqu'un navigateur Web est utilisé pour accéder en toute sécurité au réseau d'entreprise, le navigateur doit utiliser une version sécurisée de HTTP pour fournir le cryptage SSL. Il n'est pas nécessaire d'installer un client VPN sur l'hôte distant, donc une connexion SSL sans client est utilisée.

17. Quelle fonction de sécurité IPsec garantit que les données reçues via un VPN n'ont pas été modifiées en transit?

- confidentialité
- authentification
- **intégrité**
- échange sécurisé de clés

Explique: L'intégrité est une fonction d'IPsec et garantit que les données arrivent inchangées à la destination grâce à l'utilisation d'un algorithme de hachage. La confidentialité est une fonction d'IPsec et utilise le chiffrement pour protéger les transferts de données avec une clé. L'authentification est une fonction d'IPsec et fournit un accès spécifique aux utilisateurs et aux périphériques avec des facteurs d'authentification valides. L'échange de clés sécurisé est une fonction d'IPsec et permet à deux pairs de maintenir la confidentialité de leur clé privée tout en partageant leur clé publique.

18. Quelles sont les deux technologies qui fournissent des solutions VPN gérées par l'entreprise? (Choisissez deux.)

- Couche 2 MPLS VPN
- relayage de trames (Frame Relay)
- **Réseau privé virtuel site à site (VPN)**
- Couche 3 MPLS VPN
- **VPN d'accès à distance**

Explique: Les VPN peuvent être gérés et déployés selon deux types:
VPN d'entreprise – Les VPN gérés par l'entreprise sont une solution courante pour sécuriser le trafic d'entreprise sur Internet. Les VPN de site à site et d'accès distant sont des exemples de VPN gérés par l'entreprise.
VPN des fournisseurs de services – Les VPN gérés par le fournisseur de services sont créés et gérés sur le réseau du fournisseur. Les couches MPLS de couche 2 et de couche 3 sont des exemples de VPN gérés par un fournisseur de services. Les autres solutions WAN héritées incluent le Frame Relay et les VPN ATM.

19. Quels sont les deux types de VPN qui sont des exemples de VPN d'accès à distance gérés par l'entreprise? (Choisissez deux.)

- **VPN IPsec basé sur le client**
- VPN IPsec
- **VPN SSL sans client**
- VPN GRE sur IPsec
- VPN d'interface de tunnel virtuel IPsec

Explique: Les VPN gérés par l'entreprise peuvent être déployés dans deux configurations:
VPN d'accès à distance – Ce VPN est créé dynamiquement lorsque cela est nécessaire pour établir une connexion sécurisée entre un client et un serveur VPN. Les VPN d'accès à distance incluent les VPN IPsec basés sur le client et les VPN SSL sans client.
VPN de site à site – Ce VPN est créé lorsque les périphériques d'interconnexion sont préconfigurés avec des informations pour établir un tunnel sécurisé. Le trafic VPN est chiffré uniquement entre les périphériques d'interconnexion, et les hôtes internes ne savent pas qu'un VPN est utilisé. Les VPN de site à site incluent IPsec, GRE sur IPsec, Cisco Multipoint dynamique (DMVPN) et IPsec Interface de tunnel virtuel (VTI) VPN.

20. Parmi les affirmations suivantes, laquelle s'applique à un VPN site à site ?

- Il oblige les hôtes à utiliser un logiciel client VPN pour encapsuler le trafic.

- Il nécessite le placement d'un serveur VPN à la périphérie du réseau de l'entreprise.
- **Il nécessite une passerelle VPN à chaque extrémité du tunnel pour chiffrer et déchiffrer le trafic.**
- Il nécessite une architecture client/serveur.

Explique: Les VPN site à site sont statiques et sont utilisés pour connecter des réseaux entiers. Les hôtes n'ont pas connaissance du VPN et ils envoient le trafic TCP/IP vers des passerelles VPN. La passerelle VPN est responsable de l'encapsulation du trafic et de son acheminement par le tunnel VPN vers une passerelle homologue située à l'autre extrémité et qui décapsule le trafic.

21. Quelle est la fonction de l'algorithme Diffie-Hellman dans le cadre de travail IPsec?

- **permet aux pairs d'échanger des clés partagées**
- fournit une authentification
- garantit l'intégrité des messages
- fournit un cryptage des données puissant

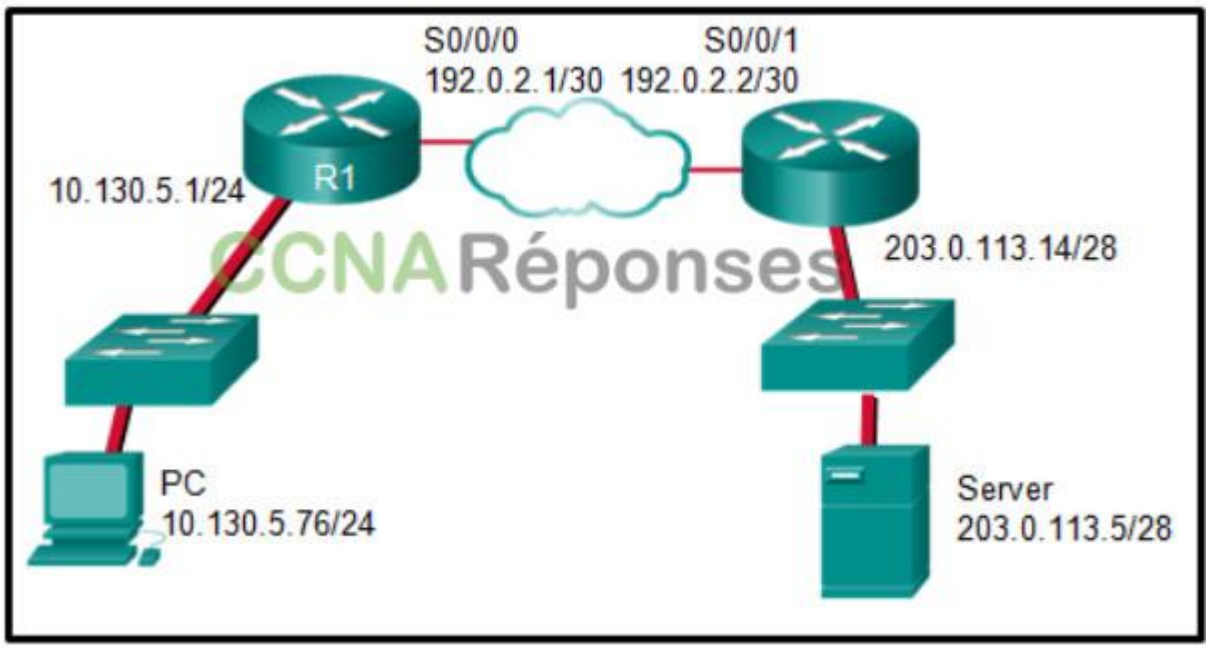
Explique: Le cadre IPsec utilise divers protocoles et algorithmes pour fournir la confidentialité des données, l'intégrité des données, l'authentification et l'échange de clés sécurisé. DH (Diffie-Hellman) est un algorithme utilisé pour l'échange de clés. DH est une méthode d'échange de clés publiques qui permet à deux pairs IPsec d'établir une clé secrète partagée sur un canal non sécurisé.

22. Qu'est-ce que la surcharge NAT utilise pour suivre plusieurs hôtes internes qui utilisent une adresse globale interne?

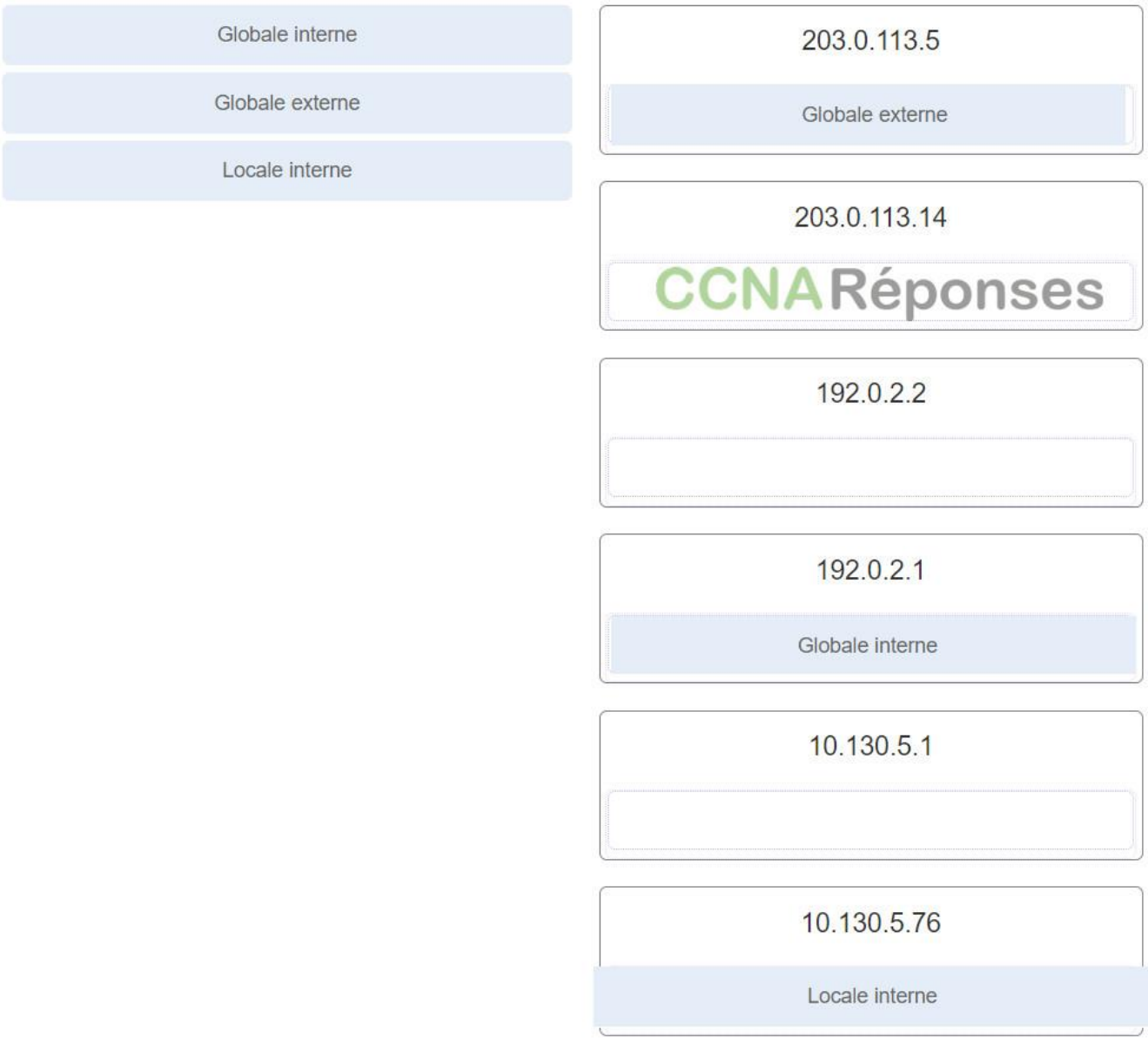
- Les numéros de système autonome
- Adresses MAC
- **Numéros de port**
- Adresses IP

Explique: La surcharge NAT, également connue sous le nom de Port Address Translation (PAT), utilise des numéros de port pour différencier plusieurs hôtes internes.

23. Reportez-vous à l'illustration. Le PC envoie un paquet au serveur sur le réseau distant. Le routeur R1 effectue une surcharge NAT. Du point de vue du PC, faire correspondre le type d'adresse NAT avec l'adresse IP correcte. (les options ne doivent pas être toutes utilisées.)



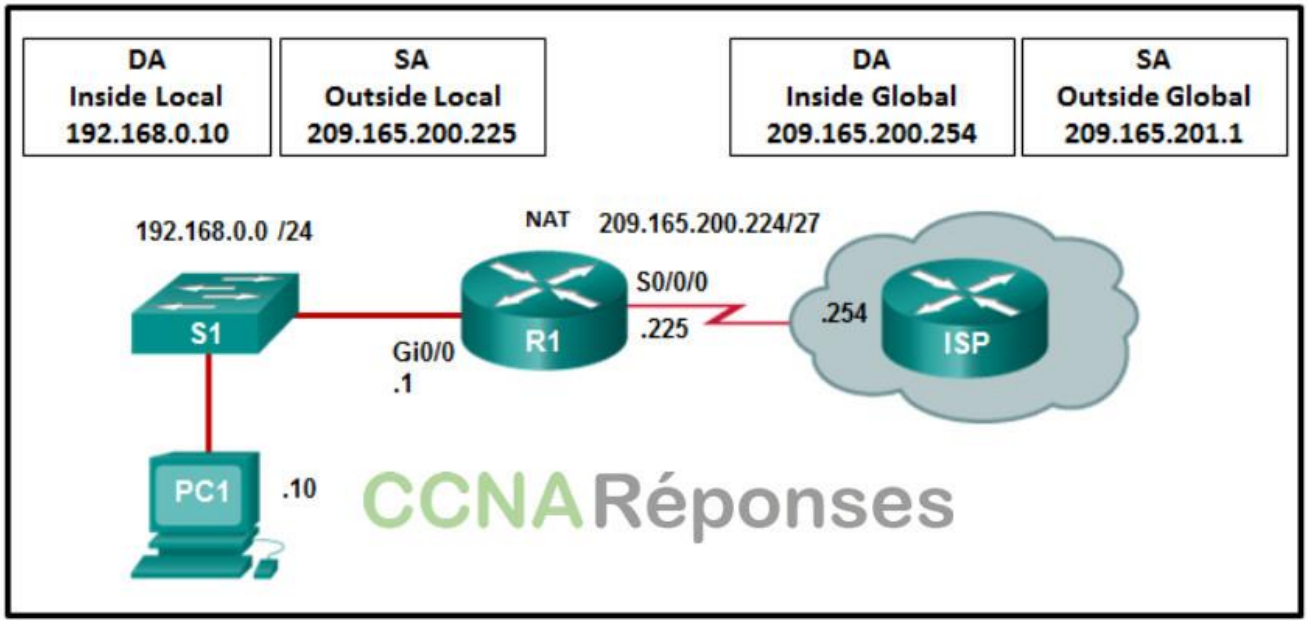
Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 38



Explique: L'adresse locale interne est l'adresse IP privée de la source ou du PC dans cette instance. L'adresse globale interne est l'adresse traduite de la source ou l'adresse telle qu'elle est vue par le périphérique externe. Puisque le PC utilise l'adresse externe du routeur R1, l'adresse globale interne est 192.0.2.1. L'adressage externe est simplement l'adresse du serveur ou 203.0.113.5.

24. Reportez-vous à l'illustration. R1 est configuré pour NAT statique. Quelle

adresse IP les hôtes Internet utiliseront-ils pour atteindre PC1 ?



- 192.168.0.10
- 192.168.0.1
- **209.165.200.225**
- 209.165.201.1

Explique: Dans NAT statique, une seule adresse locale interne, dans ce cas 192.168.0.10, sera mappée à une seule adresse globale interne, dans ce cas 209.165.200.225. Les hôtes Internet enverront des paquets à PC1 et utiliseront comme adresse de destination l'adresse globale interne 209.165.200.225.

25. Reportez-vous à l'illustration. Un administrateur réseau affiche la sortie de la commande show ip nat translations . Quelle instruction décrit correctement la traduction NAT qui se produit sur le routeur RT2?

```
RT2# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.0.10.5       YES manual up                    up

FastEthernet0/1        192.0.2.254     YES manual up                    up

Serial0/0/0            10.0.10.1       YES manual up                    up

Serial0/0/1            unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down

RT2# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.0.2.254:13  192.168.2.20:13    203.0.113.20:13    203.0.113.20:13
---  192.0.2.88      192.168.254.253    ---                ---
tcp  192.0.2.88:80   192.168.254.253:80 203.0.113.20:1025  203.0.113.20:1025

RT2#
```

- **Le trafic provenant d'une adresse IPv4 source de 192.168.254.253 est traduit en 192.0.2.88 au moyen d'un NAT statique.**
- Le trafic provenant d'une adresse publique IPv4 source qui provient du trafic sur Internet pourrait atteindre des adresses IPv4 internes privées.
- Le trafic provenant d'une adresse IPv4 source de 192.168.2.20 est traduit par le routeur RT2 pour atteindre une adresse IPv4 de destination 192.0.2.254.
- Le trafic provenant d'une adresse IPv4 source de 192.0.2.88 est traduit par le routeur RT2 pour atteindre une adresse IPv4 de destination 192.168.254.253.

Explique: Comme aucune adresse externe locale ou externe n'est référencée, le trafic provenant d'une adresse IPv4 source de 192.168.254.253 est traduit en 192.0.2.88 à l'aide d'un NAT statique. Dans la sortie de la commande show ip nat translations , l'adresse IP locale interne de 192.168.2.20 est traduite en une adresse IP externe de 192.0.2.254 afin que le trafic puisse traverser le réseau public. Un périphérique IPv4 public peut se connecter au périphérique IPv4 privé 192.168.254.253 en ciblant l'adresse IPv4 de destination 192.0.2.88.

26. Citez deux services d'infrastructure WAN qui sont des exemples de connexions privées. (Choisissez deux réponses.)

- DSL
- **Frame Relay**
- Câble
- Technologie sans fil
- **T1/E1**

Explique: Les WAN privés peuvent utiliser les technologies suivantes : T1/E1, T3/E3, RTPC, RNIS, Metro Ethernet, MPLS, Frame Relay, ATM ou VSAT.

27. Quelles sont les deux déclarations concernant la relation entre les LAN et les WAN? (Choisissez deux réponses.)

- **Les réseaux WAN sont généralement gérés par plusieurs fournisseurs de services Internet, mais les réseaux locaux sont généralement gérés par des organisations ou des particuliers.**
- **Les réseaux WAN connectent les réseaux locaux à une vitesse plus lente que les réseaux locaux connectent leurs périphériques internes.**
- Les réseaux locaux et les réseaux étendues connectent les périphériques terminaux.
- Les réseaux locaux connectent plusieurs réseaux WAN ensemble.
- Les réseaux WAN doivent être publics, mais les réseaux locaux peuvent être détenus par des entités publiques ou privées.

Explique: Bien que les LAN et les WAN puissent utiliser les mêmes supports de réseau et les mêmes appareils intermédiaires, ils servent des domaines et des objectifs très différents. Le cadre administrative et géographique d'un réseau étendu est plus grande que celle d'un réseau local. Les vitesses de bande passante sont plus lentes sur les WAN en raison de leur complexité accrue. Internet est un réseau de réseaux qui peuvent fonctionner sous gestion publique ou privée.

28. Quelle déclaration décrit une caractéristique importante d'un VPN de site à site??

- Cela nécessite l'utilisation d'un client VPN sur le PC du hôte.

- Une fois la connexion initiale établie, elle peut modifier dynamiquement les informations de connexion.
- Il est idéalement adapté à une utilisation par des travailleurs mobiles.
- Il est généralement mis en œuvre sur les réseaux par modem commutés et câblés.
- **Il doit être configuré statiquement.**

Explique: Un VPN de site à site est créé entre les périphériques du réseau de deux réseaux distincts. Le VPN est statique et reste établi. Les hôtes internes des deux réseaux n'ont aucune connaissance du VPN.

29. Comment fonctionne le tunneling sur un VPN ?

- Tous les paquets entre deux hôtes sont attribués à un seul support physique pour garantir la confidentialité des paquets.
- **De nouveaux en-têtes d'un ou de plusieurs protocoles VPN encapsulent les paquets d'origine.**
- Un circuit dédié est établi entre les périphériques source et de destination pendant la durée de la connexion.
- Les paquets sont déguisés pour ressembler à d'autres types de trafic afin qu'ils soient ignorés par les pirates éventuels.

Explique: Dans un VPN, les paquets sont encapsulés avec les en-têtes d'un ou de plusieurs protocoles VPN avant d'être envoyés sur le réseau tiers. Cette opération porte le nom de « tunneling ». Ces en-têtes externes peuvent être utilisés pour acheminer les paquets, authentifier la source et empêcher les utilisateurs non autorisés de lire le contenu des paquets.

30. Quelle déclaration décrit un VPN?

- Les VPN utilisent des connexions physiques dédiées pour transférer des données entre des utilisateurs distants.
- Les VPN utilisent des connexions logiques pour créer des réseaux publics via Internet.
- **Les VPN utilisent des connexions virtuelles pour créer un réseau privé via un réseau public.**
- Les VPN utilisent un logiciel de virtualisation de source ouverte pour créer le tunnel via Internet.

Explique: Un VPN est un réseau privé créé sur un réseau public. Au lieu d'utiliser des connexions physiques dédiées, un VPN utilise des connexions virtuelles acheminées via un réseau public entre deux périphériques réseau.

31. Ouvrez le fichier d'activité Packet Tracer.Effectuez les tâches décrites dans les instructions relatives à l'activité, puis répondez à la question.
Quel problème empêche PC-A de communiquer avec Internet?

- La liste d'accès utilisée dans le processus NAT fait référence au mauvais sous-réseau.
- La route statique ne doit pas faire référence à l'interface, mais plutôt à l'adresse extérieure.
- Ce routeur doit être configuré pour utiliser le NAT statique au lieu de PAT.
- **Les interfaces NAT ne sont pas correctement attribuées.**
- La commande ip nat inside source fait référence à la mauvaise interface.

Explique: La sortie de show ip nat statistics montre que l'interface interne est FastEtherNet0/0 mais qu'aucune interface n'a été désignée comme interface externe. Cela peut être corrigé en ajoutant la commande ip nat outside à l' interface Serial0/0/0.

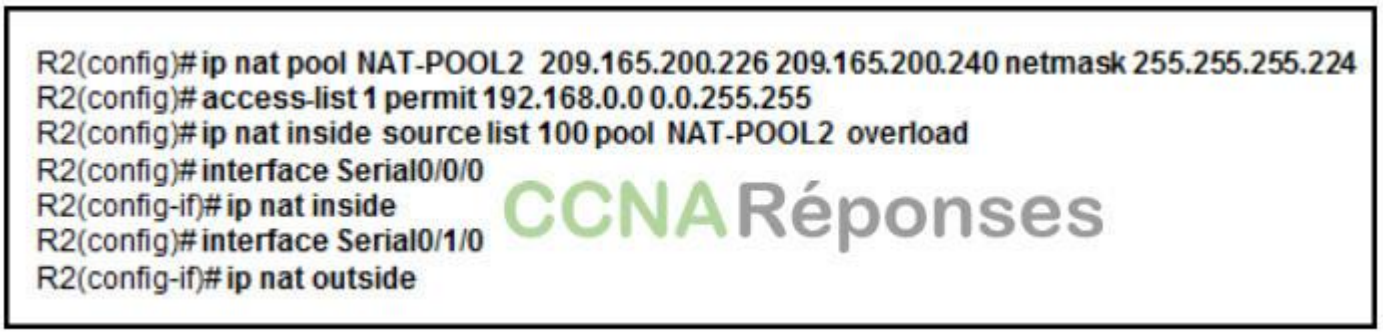
32. Quel type d'adresse est 64.100.190.189?

- **public**
- privé

33. Quel type de VPN a à la fois des implémentations de couche 2 et de couche 3?

- VPN multipoint dynamique
- **VPN MPLS**
- VPN SSL
- GRE sur IPsec

34. xaminez l'illustration. Un administrateur réseau a configuré R2 pour la traduction d'adresses de port (PAT). Pourquoi la configuration est-elle incorrecte ?

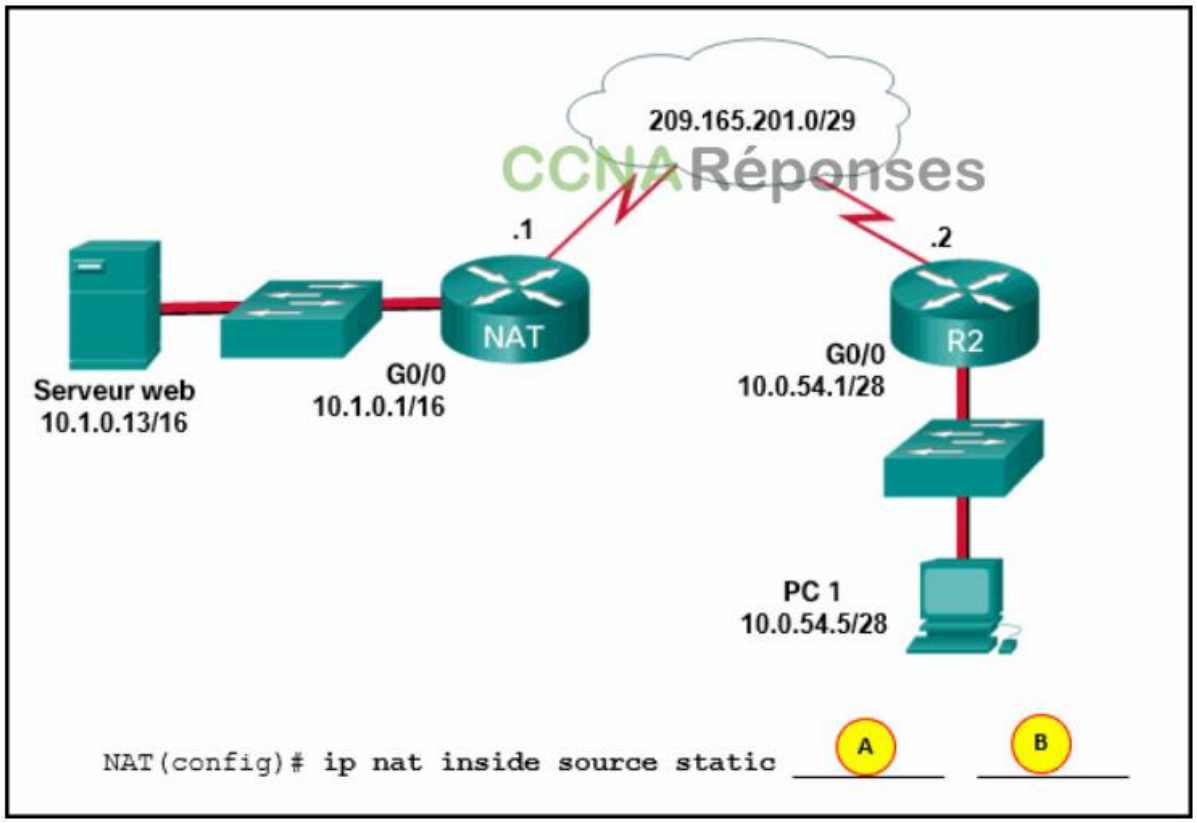


Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN

- Il manque l'entrée NAT statique.
- La liste de contrôle d'accès ne définit pas la liste des adresses à traduire.
- Le mot clé overload n'aurait pas dû être appliqué.
- **NAT-POOL2 n'est pas lié à la liste de contrôle d'accès adéquate.**

Explique: Sur l'illustration, NAT-POOL 2 est relié à la liste de contrôle d'accès 100, mais il doit être associé à la liste de contrôle d'accès ACL 1. Cela entraîne l'échec de PAT. 100, mais il doit être associé à la liste de contrôle d'accès ACL 1. Cela entraîne l'échec de PAT.

35. Reportez-vous à l'illustration. La fonction NAT statique est configurée pour autoriser PC 1 à accéder au serveur Web sur le réseau interne. Quelles adresses doivent remplacer les points A et B pour terminer la configuration de la NAT statique ? (Choisissez deux réponses.)



Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 12

- **A = 10.1.0.13**
- A = 209.165.201.2
- **B = 209.165.201.1**
- B = 209.165.201.7
- B = 10.0.254.5

Explique: La NAT statique est un mappage un-à-un entre une adresse locale interne et une adresse globale interne. Grâce à la NAT, les périphériques externes peuvent démarrer des connexions aux périphériques internes en utilisant les adresses globales internes. Les périphériques NAT traduisent l'adresse globale interne à l'adresse locale interne de l'hôte cible.

36. Quelles sont les deux adresses spécifiées dans une configuration NAT statique?

- Globale interne et locale externe
- Globale externe et locale externe
- **Locale interne et globale interne**
- Locale interne et globale externe

Explique: La configuration NAT statique spécifie une adresse locale interne unique et une adresse globale interne unique.

37. Examinez l'illustration. La configuration NAT appliquée au routeur est la suivante :

```
ERtr(config)# access-list 1 permit 10.0.0.0 0.255.255.255
```

```
ERtr(config)# ip nat pool corp 209.165.201.6 209.165.201.30
netmask 255.255.255.224

ERtr(config)# ip nat inside source list 1 pool corp overload

ERtr(config)# ip nat inside source static 10.10.10.55
209.165.201.4

ERtr(config)# interface gigabitethernet 0/0

ERtr(config-if)# ip nat inside

ERtr(config-if)# interface serial 0/0/0

ERtr(config-if)# ip nat outside
```

```
ERtr# show ip nat statistics
Total translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  GigabitEthernet0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool corp refCount 0
 pool NAT-POOL1: netmask 255.255.255.224
            start 209.165.201.6 end 209.165.201.30
            type generic, total addresses 25, allocated 0 (0%), misses 0
```


Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 16

D'après la configuration et le résultat affichés, que peut-on dire de l'état de la NAT au sein de l'organisation ?

- La NAT fonctionne.
- La NAT statique fonctionne, mais pas la NAT dynamique.
- **Les informations fournies sont insuffisantes pour déterminer si la NAT statique et la NAT dynamique fonctionnent.**
- La NAT dynamique fonctionne, mais pas la NAT statique.

Explique: Il n'y a pas suffisamment d'informations fournies. Cela peut s'expliquer par le fait que le routeur n'est pas encore relié au réseau, que les interfaces n'ont pas encore été associées à des adresses IP ou que la commande a été transmise au milieu de la nuit. Le résultat correspondant à la configuration donnée, aucune erreur typographique n'a été commise lorsque les commandes NAT ont été saisies.

38. Une entreprise envisage de changer sa connexion WAN pour son réseau local. Quelles sont les deux options représentatives d'une architecture WAN privée ? (Choisissez deux propositions.)

- **WAN Ethernet**

- Wi-Fi municipal
- **ligne louée**
- ligne d’abonné numérique
- câble

Explique: Une entreprise peut se connecter au WAN de deux façons basiques : Infrastructure WAN privée telle que lignes point à point louées dédiées, RTPC, RNIS, WAN Ethernet, ATM ou relais de trames.
Infrastructure WAN publique telle que ligne d’abonné numérique (DSL), câble, accès satellite, Wi-Fi municipal, WiMax, ou sans-fil cellulaire notamment 3G/4G

39. Mettez en correspondance chaque composant d’une connexion WAN et sa description. (Les options ne sont pas toutes utilisées.)

Enterprise Networking, Security, and Automation (Version 7.00) – Examen des concepts WAN 20

40. Quelle est la fonction de l’algorithme HMAC (Code d’authentification de message haché) dans la configuration d’un VPN IPsec?

- protège les clés IPsec pendant la négociation de session
- **garantit l’intégrité des messages**
- crée un canal sécurisé pour la négociation des clés
- authentifie les pairs IPsec

Explique: Le cadre de travail de IPsec utilise divers protocoles et algorithmes pour assurer la confidentialité des données, l’intégrité des données, l’authentification et l’échange de clés sécurisé. Le code d’authentification de message haché (HMAC) est un algorithme d’intégrité des données qui utilise une valeur de hachage pour garantir l’intégrité d’un message.

41. Quels sont les deux algorithmes de hachage utilisés avec IPsec AH pour garantir l'authenticité? (Choisissez deux.)

- **SHA**
- RSA
- AES
- **MD5**
- DH

Explique: Le cadre de travail IPsec utilise divers protocoles et algorithmes pour fournir la confidentialité des données, l'intégrité des données, l'authentification et l'échange de clés sécurisé. MD5 et SHA sont deux algorithmes populaires utilisés pour garantir que les données ne sont pas interceptées et modifiées (intégrité et authenticité des données).

42. Quels deux algorithmes peuvent faire partie d'une politique IPsec pour fournir le chiffrement et le hachage pour protéger le trafic intéressant?? (Choisissez deux.)

- DH
- **SHA**
- RSA
- PSK
- **AES**

Explique: Le cadre IPsec utilise divers protocoles et algorithmes pour fournir la confidentialité des données, l'intégrité des données, l'authentification et l'échange de clés sécurisé. Deux algorithmes qui peuvent être utilisés dans une politique IPsec pour protéger le trafic intéressant sont AES, qui est un protocole de chiffrement, et SHA, qui est un algorithme de hachage.

43. Quel protocole crée une connexion virtuelle de point à point vers un trafic de tunnel non chiffré entre les routeurs Cisco et provenant de différents types de protocole ?

- IPsec
- **GRE**
- OSPF
- Protocole IKE

Explique: L'Encapsulation générique du routage (GRE) est un protocole de mise en tunnel développé par Cisco. Ce protocole encapsule un trafic multiprotocole entre des routeurs Cisco à distance. Le GRE ne crypte pas les données. Le protocole OSPF est un protocole de routage libre. IPsec est une suite de protocoles qui permet l'échange d'informations pouvant être cryptées et vérifiées. Internet Key Exchange (IKE) est une norme de gestion de clés utilisée avec IPsec.

44. Quel type d'adresse est 198.133.219.148?

- privé
- **public**

45. Quel type de VPN implique un protocole de tunnel non sécurisé encapsulé par IPSec?

- VPN multipoint dynamique

- Interface de tunnel virtuel IPSec
- VPN SSL
- **GRE sur IPsec**

46. Quel type d'adresse est 192.168.7.126?

- public
- **privé**

47. Quels deux terminaux peuvent être de l'autre côté d'un VPN de site à site ASA configuré à l'aide d'ASDM? (Choisissez deux.)

- Commutateur de Frame Relay
- Commutateur DSL
- Commutateur multicouche
- **Routeur ISR**
- **un autre ASA**

Explique: ASDM prend en charge la création d'un VPN de site à site ASA entre deux ASA ou entre un ASA et un routeur ISR.

48. Quel type de VPN prend en charge plusieurs sites en appliquant des configurations aux interfaces virtuelles plutôt qu'aux interfaces physiques?

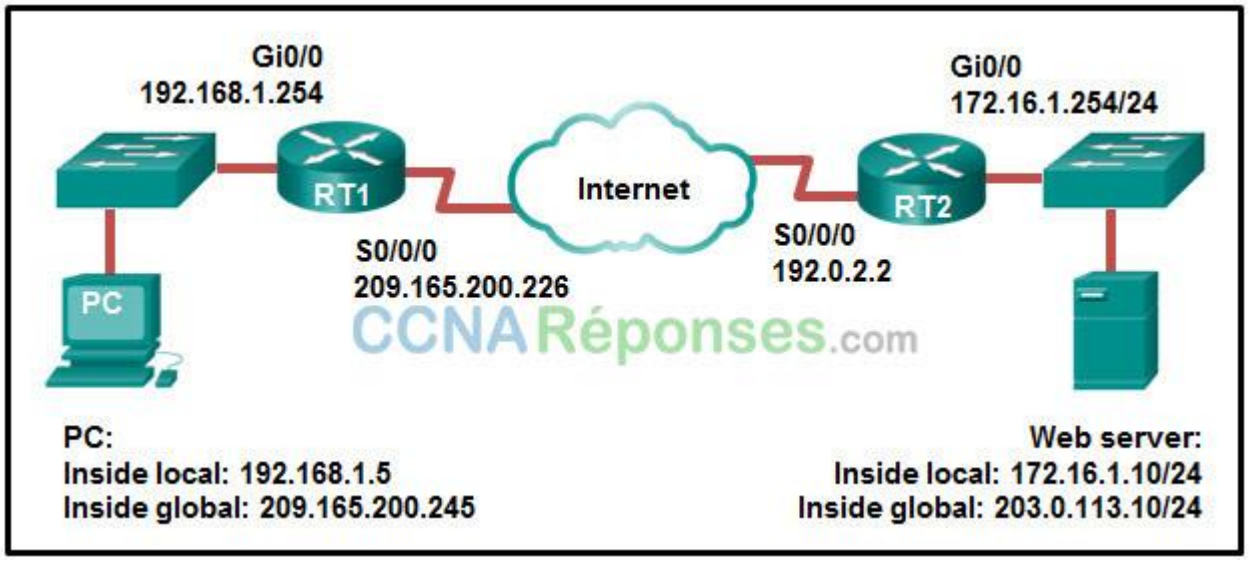
- VPN multipoint dynamique
- VPN MPLS
- **Interface de tunnel virtuel IPSec**
- GRE sur IPsec

49. En termes de NAT, quel type d'adresse désigne l'adresse IPv4 globalement routable d'un hôte de destination sur l'internet ?

- Locale externe
- Globale interne
- **Globale externe**
- Locale interne

Explique: Du point de vue d'un périphérique NAT, les utilisateurs externes se servent d'adresses globales internes pour accéder aux hôtes internes. Les adresses locales internes sont celles attribuées à des hôtes internes. Les adresses globales externes sont les adresses des destinations sur le réseau externe. Les adresses locales externes sont les adresses privées réelles des hôtes de destination derrière d'autres périphériques NAT.

50. Reportez-vous à l'illustration. La NAT est configurée sur RT1 et RT2. Le PC envoie une requête au serveur Web. Quelle adresse IPv4 est l'adresse IP source du paquet entre RT2 et le serveur Web?



- **209.165.200.245**
- 203.0.113.10
- 192.168.1.5
- 172.16.1.10
- 172.16.1.254
- 192.0.2.2

Explique: Étant donné que le paquet est entre RT2 et le serveur Web, l'adresse IP source est l'adresse globale interne du PC, 209.165.200.245.

51. Examinez l'illustration. Un administrateur réseau vient de configurer la traduction d'adresses et vérifie la configuration. Que peut-il vérifier ? (Choisissez trois réponses.)

```
R1# show ip nat statistics
Total translations: 6 (2 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/2/1
Inside Interfaces: Serial0/2/0 , FastEthernet0/0.10 , FastEthernet0/0.11 ,
FastEthernet0/0.12
Hits: 3  Misses: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool NAT refCount 4
 pool NAT: netmask 255.255.255.248
       start 209.165.200.228 end 209.165.200.230
       type generic, total addresses 3 , allocated 1 (33%), misses 0
```


- **Que la traduction d'adresses fonctionne.**
- **Qu'une liste de contrôle d'accès standard numérotée 1 est utilisée dans le cadre du processus de configuration.**
- Que les hôtes utilisent trois adresses du pool NAT.
- Que le nom du pool NAT est refCount.
- **Que deux types de NAT sont activés.**
- Qu'un port du routeur ne participe pas à la traduction d'adresses.

Explique: Les commandes **show ip nat statistics** , **show ip nat translations** et **debug ip nat** sont utiles pour déterminer si la NAT fonctionne et pour résoudre les problèmes associés à la NAT. La NAT fonctionne, comme indiqué par le décompte de succès et d'échecs. Comme il y a quatre échecs, un problème peut être présent. La liste de contrôle d'accès standard numéro 1 est utilisée et le pool de traduction est nommé NAT comme en atteste la dernière ligne de sortie. La NAT statique et la surcharge NAT sont utilisées comme indiqué dans la ligne des traductions totales.

52. Quelle situation décrit les transmissions de données via une connexion WAN?

- Un directeur envoie un courriel à tous les employés du département ayant des bureaux situés dans plusieurs bâtiments.
- **Un employé partage un fichier de base de données avec un collègue qui se trouve dans une filiale de l'autre côté de la ville.**
- Un administrateur réseau du bureau accède à distance à un serveur Web situé dans le centre de données à la périphérie du campus.
- Un employé imprime un fichier via une imprimante en réseau située dans un autre bâtiment.

Explique: Lorsque deux bureaux d'une ville communiquent, il est probable que les transmissions de données se font sur un type quelconque de connexion WAN. Les communications de données au sein d'un campus se font généralement sur des connexions LAN.

53. Quel type d'adresse est 192.168.7.98?

- **privé**
- public

54. Quel type d'adresse est 10.131.48.7?

- public
- **privé**

55. Quel type de VPN se connecte à l'aide de la fonctionnalité TLS (Transport Layer Security)?

- Interface de tunnel virtuel IPSec
- **VPN SSL**
- VPN MPLS
- VPN multipoint dynamique

56. Quel type d'adresse est 10.100.126.126?

- **privé**
- public