Quiz VPN

Note : /20

Correction :

1. Quel est le protocole de VPN qui est peu compatible avec le NAT ?

- PPTP
- IPSEC
- SSL
- AES

Explication

IPSEC est un protocole de couche 3 où le NAT intervient, contrairement au PPTP (couche 2) et au SSL (couche Transport/session)

---

2. IPSEC permet de :

- Chiffrer HTTP
- Chiffrer Ethernet
- Chiffrer IP
- Chiffrer FTP

Explication

IPSEC encapsule les paquet IP et les chiffre, c'est donc bien IP qui est chiffré

3. SSL/TLS permet de :

- Chiffrer HTTP
- Chiffrer IP
- Chiffrer Ethernet

Explication

SSL/TLS agissent au niveau du chiffrement des applications IP et pas sur les couches inférieures

4. Un système de VPN doit pouvoir mettre en œuvre :
(3 réponses)

- L'authentification d'utilisateur
- La gestion d'adresses publiques
- Le chiffrement des données
- La gestion de clés
- La translation d'adresses

Explication

La translation d'adresse est effectué par le NAT et la gestion des adresses publiques par le FAI

5. Sélectionner les protocoles VPN
(3 réponses)

- L2TP
- PPTP
- RADIUS
- IPSEC
- AES

6. TLS est un protocole propriétaire contrairement à SSL

- VRAI
- FAUX

Explication

SSL appartient à Netscape alors que TLS est normé et libre d'utilisation

7. Un VPN est vu comme une connexion point à point

- VRAI
- FAUX

Explication

Les points d'accès entre routeurs VPN sont considérés comme des connexions point à point (de 1 vers 1)

8. Quelles affirmations sont vraies à propos du VPN ?
(2 réponses)

- Un tunnel sécurisé est créé entre deux sites distants
- Les paquets qui circulent sur Internet sont chiffrés
- Il est obligatoire d'utiliser un firewall
- Il faut absolument activer la fonctionnalité NAT

9. Quelle serait la bonne définition d'un tunnel VPN établi entre un PC de télétravailleur utilisant un logiciel client VPN et le routeur VPN l'entreprise ?

- VPN site à site
- Lan to Lan VPN
- VPN Modulaire
- VPN d'accès distant

10. Lequel de ces protocoles est un VPN de niveau 2 ?

- PPTP
- SSL
- IPSEC

11. Un service qui vous permet d'accéder au Web en toute sécurité et en toute confidentialité en acheminant votre connexion via un serveur et en masquant vos actions en ligne.

- SSL
- TLS
- Firewall
- IDS

Explication

Grâce au protocole HTTPS qui s'appuie sur SSL/TLS

12. Quels sont les protocoles de tunneling utilisés par les VPN ?

- Blowfish et Twofish
- HTTP et FTP
- IPsec et L2TP
- AES et MD5

13. ESP fournit :

- Authentification
- Chiffrement
- Intégrité
- Tout ce qui est au dessus

Explication

Le mode ESP sur IPsec permet d'authentifier, de chiffrer et de gérer l'intégrité

14. AH ne fournit pas :

- Authentification
- Chiffrement
- Intégrité

Explication

Le mode AH dans IPsec se contente de gérer l'intégrité et l'authentification mais pas le chiffrement

15. A quoi sert IKE dans IPsec ?

- Authentification
- Chiffrement
- Echange de clés
- Protection d'en tête

Explication

Internet Key Exchange comme son nom l'indique est chargé de négocier la connexion. IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées. Ce protocole permet deux types d'authentifications, PSK (clé partagée) ou à l'aide de certificats

16. Quel mode IPsec ne modifie pas l'en-tête IP ?

- SSH
- Tunnel
- Transport
- NAT

Explication

Le mode transport ne chiffre que les données contrairement au mode tunnel qui lui chiffre la totalité du paquet et créé un nouvel en-tête

17. Si l'on veut vérifier les paquets sans les chiffrer on utilisera IPsec en mode :

- AH
- IKE
- ESP

18. Dans un VPN site à site :

- Le client doit lancer un logiciel VPN
- Seuls les routeurs construisent le tunnel
- C'est le FAI qui doit gérer le VPN

19. Peut-on utiliser une connexion HTTPS dans un VPN IPsec ?

- OUI
- NON

Explication

Un VPN s'occupe du réseau alors qu'https s'occupe de l'application. Il n'y aucune incompatibilité de ce fait

20. Lequel de ces protocoles chiffre FTP grâce à SSL/TLS ?

- FTPS
- SFTP
- HTTPS
- Ce sont des normes de câbles ça ?

Explication

FTPS s'appuie sur SSL/TLS alors que SFTP s'appuie sur SSH