Nom : _____ Date : _____ Note : _____

VPN d'accès à distance

Sécurisation des terminaux des employés à distance, authentification multifacteur et configuration des tunnels IPsec.

VPN D'ACCÈS À DISTANCE : PRÉSENTATION

APPRENANT
STATUT D'ÉTUDIANT
Parcours Défenseur du réseau

SÉCURISÉ
ÉTAT DE LA CONNEXION
Protéger les paquets de données

ACTIF
PROTECTION CONTRE LES FUITES
Protection contre les fuites DNS et IPv6

Bienvenue ! Ce dossier d'activités vous guide à travers les réseaux VPN d'accès à distance. Vous étudierez les tunnels client-à-site, les connexions multifacteurs, les contrôles de posture des terminaux, les plafonds de bande passante et l'audit de sécurité via syslog.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez les configurations VPN et de sécurité réseau.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com des meilleurs VPN

URL: https://www.vpn.com/fr/vpn/meilleur-vpn-entreprise/acces-distant/

Votre parcours d'apprentissage : VPN d'accès à distance

- Sécuriser les terminaux des employés à distance qui accèdent aux nœuds du réseau local.
- Configurez des politiques d'authentification multifacteur pour les connexions à distance.
- Mettre en place des configurations IPsec et OpenVPN client-à-site.
- Auditer les journaux de connexion à distance pour détecter les violations du contrôle d'accès.
- Mettre en place des contrôles de conformité des appareils avant d'accorder l'accès au réseau.
- Optimiser le débit des serveurs pour éviter l'engorgement de la bande passante en télétravail.

VPN D'ACCÈS À DISTANCE : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances aux contrôles de conformité des appareils et aux connexions multifacteurs. Terminez par l'activité bonus Réflexion rapide.

TUNNELS CLIENT À SITE ET CONFORMITÉ DES TERMINAUX (INTRODUCTION)

Les VPN d'accès à distance établissent des tunnels sécurisés client-à-site pour les employés hors site. Sécuriser ces connexions exige d'imposer des connexions avec authentification multifacteur (MFA), d'effectuer des contrôles de conformité des terminaux et d'auditer les journaux via des collecteurs syslog centralisés.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quelle norme d'authentification les portails VPN d'accès à distance doivent-ils imposer ?

- A) Multifacteur
- B) Facteur unique
- C) Non chiffré
- D) Invité local

2. Quel protocole est la norme pour sécuriser les connexions client-site du télétravail ?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. Quelle vérification permet de valider qu'un ordinateur portable distant est sain avant sa connexion ?

- A) Vérification de la posture
- B) Test de vitesse
- C) Test de ping
- D) Quantité de mémoire

4. Où sont stockés les journaux de connexion des télétravailleurs pour les audits de sécurité ?

- A) Serveur Syslog
- B) Clé de registre
- C) Mémoire du client
- D) Navigateur web

5. Quel problème survient lorsque le nombre de télétravailleurs dépasse la capacité de bande passante de la passerelle ?

- A) Étranglement de la bande passante
- B) Fuite DNS
- C) Passage de la négociation (handshake)
- D) Exposition de l'IP

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. L'authentification multifacteur ajoute un jeton de validation secondaire pour sécuriser les connexions à distance.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. Les contrôles de conformité autorisent les appareils distants dont le pare-feu est désactivé à accéder aux serveurs privés.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. Les journaux des VPN d'accès à distance sont essentiels pour retracer les intrusions non autorisées dans le réseau de l'entreprise.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. OpenVPN et IPsec sont des protocoles anciens qui ne chiffrent pas les données des clients distants.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. L'engorgement de la bande passante de la passerelle se produit lorsque le trafic distant dépasse la capacité de la carte réseau.

- ◯ Vrai
- ◯ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Pour protéger les portails d'entreprise, les connexions à distance doivent exiger une authentification _____ .

2. Les clients distants chiffrent les données utiles du tunnel au moyen de protocoles standard tels que _____ .

3. Les appareils doivent réussir un contrôle de _____ **sécurité avant d'obtenir un accès au réseau.**

4. Des journaux d'accès vérifiables sont transmis en continu à un serveur _____ **central.**

5. Un trafic intense pendant les heures de bureau peut saturer la _____ **de la passerelle.**

6. Sous Windows et macOS, des pilotes d'adaptateur virtuel gèrent la _____ **client-à-site.**

BANQUE DE MOTS DE VOCABULAIRE

BANDE PASSANTE CHIFFREMENT MULTIFACTEUR OPENVPN PARE-FEU
POSTURE SYSLOG TUNNELISATION

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions clés

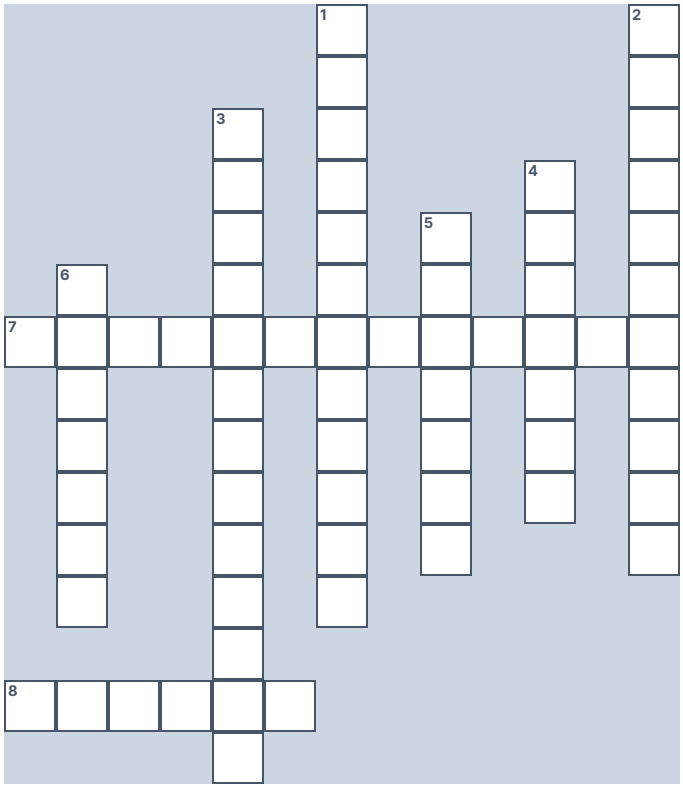
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. MULTIFACTEUR	A	Encapsulation des données dans un chemin sécurisé.
☐	2. OPENVPN	B	Collecteur central des journaux de sécurité.
☐	3. CONFORMITÉ	C	Limite de capacité de données du réseau.
☐	4. SYSLOG	D	Protocole client-à-site standard.
☐	5. BANDE PASSANTE	E	Validation de l'état de santé d'un appareil distant.
☐	6. CHIFFREMENT	F	Règles du système de filtrage du trafic.
☐	7. TUNNELISATION	G	Brouillage cryptographique des paquets.
☐	8. PARE-FEU	H	Sécurité de connexion exigeant des jetons supplémentaires.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

7. Limite de capacité de données du réseau (13)

8. Collecteur central des journaux de sécurité (6)

VERTICALEMENT

1. Sécurité de connexion exigeant des jetons supplémentaires (12)

2. Brouillage cryptographique des paquets (11)

3. Encapsulation des données dans un chemin sécurisé (13)

4. Protocole client-à-site standard (7)

5. Validation de l'état de santé des appareils distants (7)

6. Règles d'un système de filtrage du trafic (7)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

7 horizontal: Limite de capacité de données du réseau (13 lettres):

8 horizontal: Collecteur central des journaux de sécurité (6 lettres):

VERTICALEMENT

1 vertical: Sécurité de connexion exigeant des jetons supplémentaires (12 lettres):

2 vertical: Brouillage cryptographique des paquets (11 lettres):

3 vertical: Encapsulation des données dans un chemin sécurisé (13 lettres):

4 vertical: Protocole client-à-site standard (7 lettres):

5 vertical: Validation de l'état de santé des appareils distants (7 lettres):

6 vertical: Règles d'un système de filtrage du trafic (7 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

N R J M L T O H Q Q H Z A O V
O T N E M E R F F I H C G U B
I Y R Y B H L Z O P E N V P N
T G J O P P N W C M Z Y G Y O
A W U K O V P S B N V T M G V
S D Y U S K R Y B X Z Y M R Q
I X I P T D A S D J Q V W W L
L J H T U H G L B E I K T S V
E R Z E R H E O S C A L Q C Z
N M K V E R U G P A R E F E U
N B A N D E P A S S A N T E A
U S W J M M H H N H R F K T L
T R M U L T I F A C T E U R W
H B U F Y O Y W S H T X A P U
N N Z O I Q T I P V U O U U K

LISTE DE MOTS DE VOCABULAIRE

MULTIFACTEUR OPENVPN POSTURE SYSLOG BANDEPASSANTE
CHIFFREMENT TUNNELISATION PAREFEU

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. MULTIFACTEUR
B. OPENVPN
C. POSTURE
D. SYSLOG
E. BANDEPASSANTE
F. CHIFFREMENT
G. TUNNELISATION
H. PAREFEU

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Collecteur central des journaux de sécurité.
2. Règles d'un système de filtrage du trafic.
3. Encapsulation des données dans un chemin sécurisé.
4. Brouillage cryptographique des paquets.
5. Protocole client-à-site standard.
6. Limite de capacité de données du réseau.
7. Validation de l'état de santé des appareils distants.
8. Sécurité de connexion exigeant des jetons supplémentaires.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions clés de cette fiche. Écrivez vos réponses dans les champs prévus.

1. TFCIUAEMULRT
2. PSERUTO
3. ABSASTENAEPND
4. LOANSENIITTUN
5. VNNEOPP
6. OLSSGY
7. MFCHETENIRF
8. AEUPEFR

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Idées reçues sur les VPN			
2	Mots qui décrivent le Zero Trust			
3	Logiciels de bureautique que vous connaissez			
4	Règles pour un télétravail sûr			
5	Choses que votre fournisseur d'accès à Internet peut voir			
6	Services VPN que vous connaissez			
7	Endroits d'où travaillent les employés			
8	Outils qu'une entreprise utilise chaque jour			
9	Rôles dans un service informatique			
10	Appareils qu'un employé peut avoir			
11	Données qu'une entreprise doit protéger			
12	Choses à faire après une faille de sécurité			
13	Choses qui peuvent perturber une visioconférence			
14	Façons de se connecter en toute sécurité			
15	Raisons de fournir un VPN aux employés			

Point de contrôle 8 : Études de cas sur les VPN et les réseaux

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : IMPOSER LA MFA



Scénario : Un analyste d'affaires tente de se connecter à la base de données de son entreprise en télétravail. Il saisit le bon nom d'utilisateur et le bon mot de passe, mais le portail VPN bloque l'accès et exige le code d'un jeton physique.

Question de discussion : quelle politique de sécurité impose cette étape de double vérification ?

ÉTUDE DE CAS 2 : CONFORMITÉ DU POSTE



Scénario : Un prestataire connecte son ordinateur portable personnel au réseau distant de l'entreprise. Le client VPN coupe immédiatement la connexion et l'informe que les définitions de son antivirus ne sont pas à jour.

Question de discussion : Quelle vérification spécifique de la passerelle VPN a bloqué cette tentative de connexion ?

Point de contrôle 9 : Déchiffrer le code

Un ingénieur réseau sécurise les canaux de routage et les tunnels des clients. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

12	5		22	16	14		16	18	15	20	5	7	5		12	5	19

20	5	18	13	9	14	1	21	24		4	9	19	20	1	14	20	19

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur les VPN (Partie A)

Passez en revue les questions et réponses les plus courantes sur les réseaux privés virtuels (VPN) et le tunneling.

Q1: Qu'est-ce qu'un VPN d'accès à distance ?

Une méthode de connexion sécurisée qui permet aux employés travaillant hors site de se connecter directement aux serveurs privés de l'entreprise.

Q2: En quoi le client-à-site diffère-t-il du site-à-site ?

Le mode client à site connecte des appareils d'utilisateurs individuels, alors que le mode site à site relie des bureaux physiques entiers.

Q3: Qu'est-ce qu'un contrôle de conformité de l'appareil ?

Une analyse qui vérifie l'état de sécurité d'un appareil distant (antivirus, niveau de correctifs du système d'exploitation) avant d'accorder l'accès.

Q4: Pourquoi OpenVPN est-il utilisé pour l'accès à distance ?

Grâce à son protocole de sécurité robuste, sa compatibilité multiplateforme et sa capacité à gérer des connexions individuelles.

Q5: Comment la MFA protège-t-elle l'accès à distance ?

Elle ajoute un jeton de vérification secondaire, ce qui empêche l'accès même si les mots de passe des employés sont divulgués ou volés.

Point de contrôle 10 : Questions fréquentes de base sur les VPN (Partie B)

Passez en revue les questions et réponses les plus courantes sur les réseaux privés virtuels (VPN) et le tunneling.

Q6: Qu'est-ce qu'un serveur syslog ?

Un référentiel centralisé de journaux qui conserve les événements de connexion, les ouvertures de session et les alertes système pour les audits de conformité.

Q7: Qu'est-ce qui provoque la saturation de la bande passante ?

Lorsque la demande totale de bande passante des télétravailleurs dépasse le plafond de débit Internet de la passerelle de l'entreprise.

Q8: Puis-je connecter mon ordinateur personnel à un VPN professionnel ?

Seulement si l'appareil réussit les contrôles de conformité de l'entreprise et est autorisé par les administrateurs informatiques.

Q9: Qu'est-ce que l'encapsulation réseau ?

L'encapsulation des paquets de données en transit dans des en-têtes de protocole chiffrés pour sécuriser la transmission.

Q10: Comment le split tunneling optimise-t-il l'accès à distance ?

Il permet aux employés d'utiliser leur FAI local pour la navigation courante tout en faisant passer les fichiers professionnels par le VPN.

Point de contrôle 10 : Questions fréquentes avancées sur les VPN (Partie C)

Découvrez les aspects techniques avancés des protocoles de tunnel VPN, de l'intégration des clients mobiles et du déploiement en entreprise.

Q1: Comment l'authentification par certificat renforce-t-elle l'accès à distance ?

Il lie les autorisations de connexion à des certificats numériques préinstallés localement, ce qui bloque les appareils non gérés ou non autorisés.

Q2: Quel est le risque de sécurité du split tunneling en télétravail ?

Cela crée un pont potentiel par lequel un appareil local compromis peut faire entrer des menaces externes dans le réseau privé.

Q3: Comment les contrôles de conformité des appareils inspectent-ils les paramètres du registre ?

Le client VPN exécute des scripts locaux qui interrogent des chemins du registre pour vérifier si le logiciel de sécurité de l'entreprise est bien en cours d'exécution.

Q4: Pourquoi les syslogs utilisent-ils le port UDP 514 par défaut ?

Pour transmettre les journaux rapidement avec un minimum de surcharge, même si les configurations sécurisées exigent désormais une encapsulation TLS sur TCP.

Q5: Comment les entreprises résolvent-elles les goulets d'étranglement de bande passante des passerelles ?

En mettant en place des équilibreurs de charge et en répartissant le trafic distant entre des nœuds de serveurs régionaux.

Point de contrôle 10 : Questions fréquentes avancées sur les VPN (Partie D)

Découvrez les aspects techniques avancés des protocoles de tunnel VPN, de l'intégration des clients mobiles et du déploiement en entreprise.

Q6: À quoi servent les adaptateurs virtuels TAP/TUN sur les clients distants ?

Ils agissent comme des cartes réseau virtuelles et acheminent le trafic TCP/IP de l'appareil directement dans le tunnel VPN chiffré.

Q7: Comment IKEv2 MOBIKE soutient-il la mobilité des équipes en télétravail ?

Il met à jour dynamiquement les associations d'adresses IP, ce qui maintient le VPN actif lorsque l'utilisateur passe du Wi-Fi aux données cellulaires.

Q8: Quelle est la différence entre le routage en tunnel partagé et en tunnel complet ?

Le routage complet fait passer tout le trafic Internet de l'appareil par le VPN, tandis que le routage fractionné n'envoie que les adresses IP de destination de l'entreprise.

Q9: Comment les appareils NAT gèrent-ils les connexions VPN distantes ?

En associant des plages de ports locaux aux adresses IP publiques de la passerelle pour acheminer les paquets de données chiffrées en retour.

Q10: Quelles normes de conformité imposent l'audit des accès à distance ?

Des normes comme HIPAA, SOC 2 et PCI DSS exigent la journalisation et la surveillance de toutes les sessions de connexion à distance.

Partie 11 : 10 faits et enseignements concrets sur les VPN

Découvrez des faits concrets sur les vitesses de chiffrement des VPN, les audits de protocoles, la connectivité mobile et le télétravail en entreprise.

1. APERÇU VPN

Les VPN d'accès à distance établissent des tunnels sécurisés client-à-site pour les personnes qui travaillent hors site.

2. APERÇU VPN

L'authentification multifacteur est exigée par les règles de conformité pour protéger les portails professionnels accessibles à distance.

3. APERÇU VPN

Les contrôles de conformité vérifient les paramètres de sécurité du client local avant d'accorder l'accès au réseau privé.

4. APERÇU VPN

Les serveurs Syslog regroupent les journaux de connexion pour auditer et détecter les tentatives d'accès non autorisées.

5. APERÇU VPN

Les engorgements de bande passante de la passerelle surviennent lorsque la demande cumulée du trafic distant dépasse les limites Internet du serveur.

6. APERÇU VPN

Les adaptateurs réseau virtuels encapsulent les requêtes réseau du système d'exploitation dans des protocoles sécurisés.

7. ZOOM SUR LES VPN

La prise en charge de MOBIKE permet aux clients distants de changer de réseau sans couper le tunnel VPN.

8. ZOOM SUR LES VPN

Le routage en tunnel complet sécurise tout le trafic Internet des employés, mais augmente la charge sur la passerelle de l'entreprise.

9. ZOOM SUR LES VPN

L'authentification par certificat lie l'autorisation de connexion VPN directement au matériel géré par l'entreprise.

10. APERÇU VPN

Des référentiels comme SOC 2 et PCI DSS exigent la journalisation et la surveillance des sessions d'accès à distance.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés de normes techniques, de spécifications et de cadres réglementaires internationaux.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Corrigé : Point de contrôle 1 – Choix multiple

1 **Jetons de connexion** SÉCURITÉ MFA — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

L'authentification multifacteur impose une vérification secondaire lors des connexions. Source : MFA Implementation.

2 **Tunnel OpenVPN** CLIENT À SITE — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

OpenVPN est un protocole standard pour sécuriser les tunnels client-à-site. Source : OpenVPN Client.

3 **Contrôles de conformité** VÉRIFICATION DE L'APPAREIL — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les contrôles de conformité vérifient sur les terminaux la présence de pare-feu et d'antivirus actifs. Source : Posture Compliance.

4 **Agrégateur de journaux** SERVEUR SYSLOG — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les serveurs Syslog collectent les journaux d'événements de sécurité pour surveiller les violations d'accès. Source : Syslog Standard.

5 **Débordement de carte** ENGORGEMENT DE LA PASSERELLE — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

L'engorgement de la bande passante de la passerelle se produit lorsque le trafic des utilisateurs dépasse les limites du serveur. Source : Capacity Planning.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Jetons de connexion** VÉRIFICATIONS MFA — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

L'authentification multifacteur impose une vérification secondaire lors des connexions. Source : MFA Implementation.

7 **Question 7** — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Les vérifications de conformité des appareils bloquent ceux dont le pare-feu ou l'antivirus est désactivé : l'accès leur est donc refusé.

8 **Agrégateur de journaux** SERVEUR SYSLOG — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les serveurs Syslog collectent les journaux d'événements de sécurité pour surveiller les violations d'accès. Source : Syslog Standard.

9 **Question 9** — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

OpenVPN et IPsec sont des protocoles actuels qui chiffrent bel et bien le trafic des clients distants.

10 **Débordement de carte** ENGORGEMENT DE LA PASSERELLE — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

L'engorgement de la bande passante de la passerelle se produit lorsque le trafic des utilisateurs dépasse les limites du serveur. Source : Capacity Planning.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

H 1. MULTIFACTEUR	D 2. OPENVPN	E 3. CONFORMITÉ	B 4. SYSLOG
C 5. BANDE PASSANTE	G 6. CHIFFREMENT	A 7. TUNNELISATION	F 8. PARE-FEU

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 MULTIFACTEUR	2 OPENVPN	3 POSTURE	4 SYSLOG
5 BANDE PASSANTE	6 TUNNELISATION		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 D – SYSLOG	2 H – PAREFEU	3 G – TUNNELISATION	4 F – CHIFFREMENT
5 B – OPENVPN	6 E – BANDEPASSANTE	7 C – POSTURE	8 A – MULTIFACTEUR

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer MULTIFACTEUR, OPENVPN et CONFORMITÉ avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

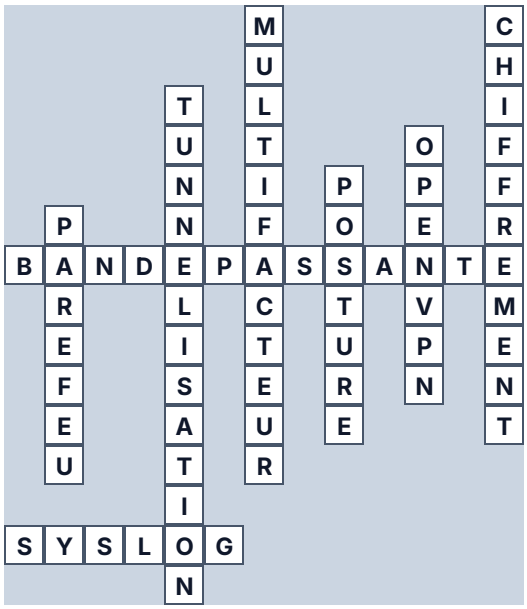
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

N	R	J	M	L	T	O	H	Q	Q	H	Z	A	O	V
O	T	N	E	M	E	R	F	F	I	H	C	G	U	B
I	Y	R	Y	B	H	L	Z	O	P	E	N	V	P	N
T	G	J	O	P	P	N	W	C	M	Z	Y	G	Y	O
A	W	U	K	O	V	P	S	B	N	V	T	M	G	V
S	D	Y	U	S	K	R	Y	B	X	Z	Y	M	R	Q
I	X	I	P	T	D	A	S	D	J	Q	V	W	W	L
L	J	H	T	U	H	G	L	B	E	I	K	T	S	V
E	R	Z	E	R	H	E	O	S	C	A	L	Q	C	Z
N	M	K	V	E	R	U	G	P	A	R	E	F	E	U
N	B	A	N	D	E	P	A	S	S	A	N	T	E	A
U	S	W	J	M	M	H	H	N	H	R	F	K	T	L
T	R	M	U	L	T	I	F	A	C	T	E	U	R	W
H	B	U	F	Y	O	Y	W	S	H	T	X	A	P	U
N	N	Z	O	I	Q	T	I	P	V	U	O	U	U	K

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

7 horizontal: BANDEPASSANTE Limite de capacité de données du réseau (13 lettres)

8 horizontal: SYSLOG Collecteur central des journaux de sécurité (6 lettres)

VERTICALEMENT

1 vertical: MULTIFACTEUR Sécurité de connexion exigeant des jetons supplémentaires (12 lettres)

2 vertical: CHIFFREMENT Brouillage cryptographique des paquets (11 lettres)

3 vertical: TUNNELISATION Encapsulation des données dans un chemin sécurisé (13 lettres)

4 vertical: OPENVPN Protocole client-à-site standard (7 lettres)

5 vertical: POSTURE Validation de l'état de santé des appareils distants (7 lettres)

6 vertical: PAREFEU Règles d'un système de filtrage du trafic (7 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. TFCIUAEMULRT — **MULTIFACTEUR**
2. PSERUTO — **POSTURE**
3. ABSASTENAEPND — **BANDEPASSANTE**
4. LOANSENIITTUN — **TUNNELISATION**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. MFCHETENIRF — **CHIFFREMENT**
8. AEUPEFR — **PAREFEU**

CORRIGÉ DU DÉFI DU CODE SECRET

"LE VPN PROTEGE LES TERMINAUX DISTANTS"

Corrigé des études de cas

A Étude de cas 1 : Imposer la MFA

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un analyste d'entreprise tente de se connecter à la base de données de son entreprise en télétravail. Il saisit son nom d'utilisateur et son mot de passe corrects, mais le portail VPN bloque l'accès et exige le code d'un jeton physique.
- Stratégie et solution recommandées : le portail VPN de l'entreprise impose une politique stricte d'authentification multifacteur (MFA) pour sécuriser les connexions à distance.

B Étude de cas 2 : Conformité du poste

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un prestataire connecte son ordinateur portable personnel au réseau distant de l'entreprise. Le client VPN coupe immédiatement la connexion et l'informe que ses définitions antivirus sont obsolètes.
- Stratégie et solution recommandées : la passerelle d'accès à distance a effectué un contrôle de conformité du terminal et a bloqué l'appareil en raison de configurations de sécurité obsolètes.