Nom : _____ Date : _____ Note : _____

VPN d'entreprise

Mise en place de l'accès réseau Zero Trust, de nœuds de passerelle dédiés et de contrôles d'administration centralisés pour l'entreprise.

RÉSEAUX VPN D'ENTREPRISE : 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'entreprise. Vous étudierez les architectures Zero Trust, les passerelles à IP statique dédiée, les consoles d'administration, le provisionnement et les tunnels IPsec de site à site.

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/entreprise/

Votre parcours d'apprentissage : réseau VPN d'entreprise

- Mettre en œuvre des cadres d'accès réseau Zero Trust (ZTNA).
- Configurez des adresses IP de passerelle de serveur dédiées pour les filtres de liste blanche.
- Gérer les panneaux d'administration centralisés de l'entreprise et les listes de licences utilisateurs.
- Auditer les journaux d'accès au réseau et les historiques de connexion des utilisateurs.
- Configurez des règles d'authentification unique (SSO) et d'authentification multifacteur.
- Mettre en place des tunnels IPsec de site à site entre succursales.

RÉSEAUX VPN D'ENTREPRISE : 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 au Zero Trust et à l'IPsec site à site. Terminez par l'activité bonus Réflexion rapide.

ARCHITECTURES ZERO TRUST ET PASSERELLES DÉDIÉES (INTRODUCTION)

Les VPN d'entreprise sécurisent les actifs de l'entreprise en passant à des cadres d'accès réseau zero trust (ZTNA) et en ajoutant des passerelles à IP statique dédiée à une liste blanche. Les responsables informatiques utilisent des consoles d'administration centralisées pour orchestrer des tunnels IPsec site à site et des liaisons d'authentification unique (SSO).

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

Point de contrôle 1 : Défi QCM

1. **1. Quel modèle de sécurité remplace les anciens VPN d'entreprise ?**
   - A) Zero Trust
   - B) Multi-saut
   - C) Pair à pair
   - D) Passerelle unique

2. **2. Quelle fonctionnalité faut-il pour limiter l'accès à la base de données aux serveurs de l'entreprise ?**
   - A) IP dédiée
   - B) Routage dynamique
   - C) Tunnel fractionné
   - D) Proxy DNS

3. **3. Quel protocole est la norme pour les tunnels de site à site en entreprise ?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Quel outil central permet aux administrateurs de gérer les licences des employés ?**
   - A) Console d'administration
   - B) Clé de registre
   - C) Firmware du routeur
   - D) Journal système

5. **5. Quelle norme d'authentification permet de se connecter via Okta ou Microsoft Entra ID ?**
   - A) Authentification unique (SSO)
   - B) Secret partagé
   - C) Authentification EPP
   - D) Clé WEP

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Le Zero Trust Network Access n'accorde l'entrée sur le réseau qu'après avoir vérifié en continu la fiabilité de l'appareil.

○ Vrai ○ Faux

7 Question 7

7. Les passerelles à IP dédiée acheminent le trafic des employés en même temps que celui d'utilisateurs grand public aléatoires.

○ Vrai ○ Faux

8 Question 8

8. Les consoles d'administration centralisées permettent aux responsables informatiques de révoquer instantanément la licence d'un employé.

○ Vrai ○ Faux

9 Question 9

9. IPsec est un protocole léger qui ne prend pas en charge les tunnels réseau de site à site.

○ Vrai ○ Faux

10 Question 10

10. L'authentification unique (Single Sign-On) permet une authentification sécurisée des employés via les fournisseurs d'identité de l'entreprise.

○ 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. Les architectures de sécurité modernes remplacent les tunnels traditionnels par un accès _____ .

2. Pour restreindre l'accès aux bases de données, les entreprises configurent une _____ comme adresse de passerelle.

3. Les succursales sont reliées de façon sécurisée par des tunnels _____ site à site.

4. Les administrateurs informatiques attribuent les licences des employés dans le _____ central.

5. L'intégration d'Okta permet aux employés de s'authentifier via la _____ de l'entreprise.

6. Pour protéger les connexions, les portails d'entreprise imposent l'authentification _____ .

BANQUE DE MOTS DE VOCABULAIRE

CONNEXION UNIQUE IP DÉDIÉE IPSEC MULTIFACTEUR PASSERELLE PROVISIONNEMENT TABLEAU DE BORD ZERO TRUST

Écrivez vos réponses ici :

1. 2.
3. 4.
5. 6.

Point de contrôle 4 : Association de notions clés

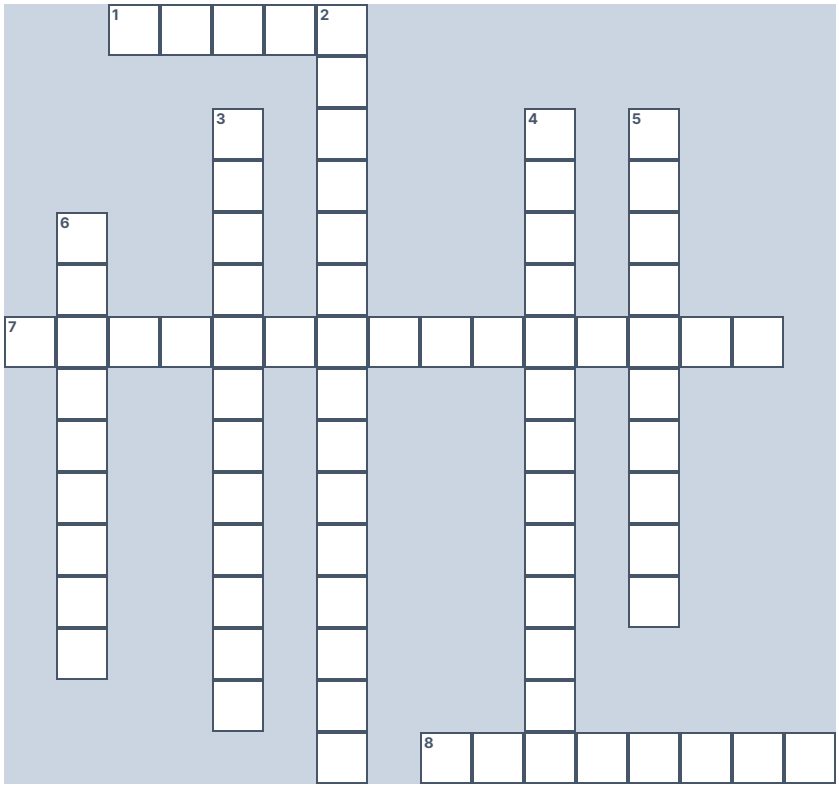
ASSOCIATION DE DÉFINITIONS

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. ZERO TRUST	A	Attribuer les licences d'accès VPN des employés.
☐	2. IP DÉDIÉE	B	Lien d'identité avec Okta et Entra ID.
☐	3. IPSEC	C	Sécurité de connexion exigeant des jetons supplémentaires.
☐	4. CONSOLE D'ADMINISTRATION	D	Adresse de passerelle en liste blanche statique.
☐	5. AUTHENTIFICATION UNIQUE (SSO)	E	Norme de tunnel de site à site.
☐	6. MULTIFACTEUR	F	Nœud de routage d'entrée du réseau.
☐	7. PASSERELLE	G	Portail central de gestion des licences pour le responsable informatique.
☐	8. PROVISIONNER	H	Cadre de vérification continue de la confiance.

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

1. Norme de tunnel site à site (5)

7. Attribution des licences d'accès VPN aux employés (15)

8. Adresse de passerelle statique inscrite sur liste blanche (8)

VERTICALEMENT

2. Liaison d'identité avec Okta et Entra ID (15)

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

4. Portail central où le responsable informatique gère les postes (13)

5. Nœud de routage à l'entrée du réseau (10)

6. Cadre de vérification continue de la confiance (9)

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

1 horizontal: Norme de tunnel site à site (5 lettres):

7 horizontal: Attribution des licences d'accès VPN aux employés (15 lettres):

8 horizontal: Adresse de passerelle statique inscrite sur liste blanche (8 lettres):

VERTICALEMENT

2 vertical: Liaison d'identité avec Okta et Entra ID (15 lettres):

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

4 vertical: Portail central où le responsable informatique gère les postes (13 lettres):

5 vertical: Nœud de routage à l'entrée du réseau (10 lettres):

6 vertical: Cadre de vérification continue de la confiance (9 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.

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

LISTE DE MOTS DE VOCABULAIRE

ZEROTRUST IPDEDIEE IPSEC TABLEAUDEBORD CONNEXIONUNIQUE
MULTIFACTEUR PASSERELLE PROVISIONNEMENT

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. ZEROTRUST
B. IPDEDIEE
C. IPSEC
D. TABLEAUDEBORD
E. CONNEXIONUNIQUE
F. MULTIFACTEUR
G. PASSERELLE
H. PROVISIONNEMENT

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Adresse de passerelle statique inscrite sur liste blanche.
2. Nœud de routage à l'entrée du réseau.
3. Attribution des licences d'accès VPN aux employés.
4. Sécurité de connexion exigeant des jetons supplémentaires.
5. Norme de tunnel site à site.
6. Cadre de vérification continue de la confiance.
7. Liaison d'identité avec Okta et Entra ID.
8. Portail central où le responsable informatique gère les postes.

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. RTOEZUSTR
2. ICESP
3. CNUOUXNNINOEIQE
4. RLEESLEPAS
5. DIPEEIED
6. EBUAOBRETADDL
7. CTIMUAREULFT
8. TENVINNRSPOOEMI

Activité bonus : Réflexion rapide

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

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

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 : MIGRATION VERS LE ZERO TRUST

👷

Scénario : Une grande entreprise souhaite sécuriser ses serveurs locaux en vérifiant en continu les certificats de conformité des appareils, l'état du pare-feu et la localisation des utilisateurs, au lieu de faire confiance à toute personne présente sur le réseau.

Question de discussion : Quel cadre le directeur de la sécurité informatique doit-il mettre en œuvre pour y parvenir ?

ÉTUDE DE CAS 2 : RESTRICTION DE LA PASSERELLE

👷

Scénario : Une entreprise héberge des bases de données financières privées dans le cloud. Elle veut bloquer tout accès Internet public aux panneaux d'administration et n'autoriser les connexions que depuis des terminaux vérifiés de l'entreprise.

Question de discussion : Quelle configuration réseau l'administrateur de bases de données doit-il mettre en place sur le pare-feu cloud ?

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

26	5	18	15		20	18	21	19	20		22	5	18	9	6	9	5
20	15	21	20		1	16	16	1	18	5	9	12					
				3	15	14	14	5	3	20	5						

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'entreprise ?

Un tunnel réseau sécurisé conçu pour les entreprises, qui permet aux télétravailleurs d'accéder aux réseaux de l'entreprise avec une gestion centralisée.

Q2: En quoi le Zero Trust diffère-t-il des VPN traditionnels ?

Les VPN traditionnels font confiance à toute personne présente dans le tunnel, tandis que le Zero Trust vérifie en continu chaque appareil et chaque connexion d'utilisateur.

Q3: Qu'est-ce qu'une IP dédiée dans les VPN d'entreprise ?

Une adresse IP statique réservée uniquement à votre entreprise, que vous pouvez ajouter à une liste blanche pour un accès sécurisé à une base de données cloud.

Q4: Pourquoi le SSO est-il important pour les VPN d'entreprise ?

L'authentification unique (Single Sign-On) permet aux employés d'utiliser leurs identifiants d'entreprise (comme Okta ou Microsoft Entra ID) pour se connecter de manière sécurisée.

Q5: Qu'est-ce qu'un VPN site-à-site ?

Un tunnel qui relie deux bureaux physiques (comme une agence et le siège) via l'Internet public à l'aide d'IPsec.

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: À quoi sert une console d'administration ?

Un tableau de bord permettant aux administrateurs informatiques d'ajouter ou de retirer des licences employés, d'attribuer des passerelles et de surveiller les connexions actives.

Q7: Comment la MFA sécurise-t-elle les VPN d'entreprise ?

En exigeant un code secondaire (comme le jeton d'une application d'authentification) pour empêcher toute connexion non autorisée avec des mots de passe compromis.

Q8: Puis-je auditer l'historique de connexion des employés ?

Oui, les VPN d'entreprise enregistrent l'horodatage des connexions, leur durée et les adresses IP attribuées pour les audits de conformité.

Q9: Qu'est-ce que le ZTNA ?

Zero Trust Network Access, un modèle de sécurité qui n'accorde l'accès qu'à certaines applications plutôt qu'à l'ensemble du réseau.

Q10: Quel est le rôle des nœuds passerelles ?

Ils servent de points d'entrée sécurisés pour le trafic distant et acheminent les données directement vers les serveurs privés de l'entreprise.

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 IPsec protège-t-il les communications site à site d'une entreprise ?

IPsec chiffre le trafic au niveau de la couche réseau à l'aide d'ESP (Encapsulating Security Payload) pour garantir la confidentialité et l'intégrité des données.

Q2: Pourquoi la sécurité périmétrique traditionnelle échoue-t-elle pour les équipes en télétravail ?

Parce que les employés accèdent aux données depuis plusieurs lieux et appareils, ce qui rend obsolète un périmètre unique protégé par un pare-feu réseau.

Q3: Comment les responsables informatiques mettent-ils en œuvre le provisionnement automatisé ?

En associant les protocoles SCIM entre les fournisseurs d'identité (Okta) et la console d'administration du VPN afin de synchroniser les annuaires d'utilisateurs.

Q4: Quel est l'intérêt du split tunneling en environnement d'entreprise ?

Il fait passer le trafic SaaS local (comme Microsoft 365) en dehors du tunnel VPN, préservant ainsi la bande passante de la passerelle de l'entreprise pour les bases de données privées.

Q5: Comment les contrôles de conformité des appareils valident-ils la sécurité des terminaux ?

Le client VPN analyse l'appareil avant la connexion pour vérifier que le pare-feu est actif, que l'antivirus fonctionne et que les correctifs du système d'exploitation sont à jour.

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: Quel est le rôle de la traversée NAT dans les configurations VPN d'entreprise ?

NAT-T encapsule les paquets IPsec dans UDP pour leur permettre de traverser les routeurs domestiques et les pare-feu sans coupure de connexion.

Q7: Comment les entreprises évitent-elles la saturation de la bande passante des passerelles ?

En déployant plusieurs nœuds de passerelle régionaux et en répartissant le trafic entrant des utilisateurs entre eux à l'aide d'équilibreurs de charge.

Q8: Pourquoi les listes blanches d'IP statiques sont-elles préférées aux listes dynamiques ?

Les listes blanches statiques empêchent les adresses IP externes non autorisées de tenter des négociations de connexion, ce qui réduit considérablement la surface d'attaque.

Q9: Quel est le rôle de l'authentification par certificat dans les VPN d'entreprise ?

Il valide des certificats numériques uniques installés sur les appareils gérés par l'entreprise, ce qui bloque les ordinateurs personnels non gérés.

Q10: Comment le ZTNA réduit-il le risque de déplacement latéral ?

En limitant les sessions des utilisateurs à des ressources autorisées précises, ce qui empêche les pirates de se déplacer dans le réseau si un nœud est compromis.

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 architectures Zero Trust vérifient en continu l'état de sécurité de chaque appareil qui tente de se connecter au réseau.

2. APERÇU VPN

Les passerelles à IP dédiée permettent aux entreprises de verrouiller leurs bases de données cloud en ajoutant des adresses statiques à une liste blanche.

3. APERÇU VPN

IPsec est le protocole standard du secteur pour configurer des tunnels sécurisés de site à site entre bureaux.

4. APERÇU VPN

Les consoles d'administration permettent aux services informatiques d'attribuer, de gérer et d'auditer les accès VPN des employés.

5. APERÇU VPN

L'authentification unique (Single Sign-On) intègre l'accès VPN aux fournisseurs d'identité de l'entreprise comme Okta et Entra ID.

6. APERÇU VPN

L'authentification multifacteur bloque les tentatives de connexion non autorisées provenant de mots de passe volés.

7. ZOOM SUR LES VPN

Le tunnel fractionné optimise la bande passante de l'entreprise en excluant du tunnel chiffré le trafic SaaS public.

8. ZOOM SUR LES VPN

Les vérifications de posture des appareils contrôlent les paramètres de sécurité locaux avant d'accorder l'accès aux serveurs de l'entreprise.

9. ZOOM SUR LES VPN

La synchronisation d'annuaire SCIM automatise les contrôles d'accès lors de l'arrivée et du départ des employés.

10. APERÇU VPN

Le Zero Trust Network Access limite l'accès des utilisateurs à certaines applications autorisées, ce qui empêche les déplacements latéraux sur le réseau.

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/

Corrigé : Point de contrôle 1 – Choix multiple

1 **Zero Trust** MODÈLE ZTNA — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les modèles Zero Trust vérifient en continu la conformité des appareils avant l'entrée sur le réseau. Source : NIST Zero Trust.

2 **IP dédiée** IP STATIQUE — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les adresses IP dédiées permettent aux passerelles à liste blanche de bloquer le trafic public. Source : Dedicated IP Guide.

3 **Norme IPsec** TUNNEL IPSEC — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

IPsec est le protocole standard utilisé pour les tunnels de site à site entre agences. Source : IPsec Tunneling.

4 **Allocation informatique** CONSOLE D'ADMINISTRATION — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les tableaux de bord d'administration centralisés permettent aux responsables informatiques d'attribuer des licences utilisateur. Source : CISA Guidelines.

5 **Question 5** — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Quelle norme d'authentification permet de se connecter via Okta ou Microsoft Entra ID ? → Authentification unique (SSO)

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Zero Trust** VÉRIFICATIONS ZTNA — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les modèles Zero Trust vérifient en continu la conformité des appareils avant l'entrée sur le réseau. Source : NIST Zero Trust.

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

NOTE PÉDAGOGIQUE

Les IP dédiées sont réservées à une seule entreprise : son trafic n'est donc pas mélangé à celui d'autres utilisateurs.

8 **Allocation informatique** POSTE ADMIN INFORMATIQUE — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les tableaux de bord d'administration centralisés permettent aux responsables informatiques d'attribuer des licences utilisateur. Source : CISA Guidelines.

9 **Norme IPsec** SITE À SITE — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

IPsec est le protocole standard utilisé pour les tunnels de site à site entre agences. Source : IPsec Tunneling.

10 **Lien SSO Okta** CONNEXION SSO — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

L'authentification unique (Single Sign-On) intègre les connexions VPN aux annuaires de l'entreprise comme Okta. Source : Okta SSO.

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. ZERO TRUST	D 2. IP DÉDIÉE	E 3. IPSEC	G 4. CONSOLE D'ADMINISTRATION
B 5. AUTHENTIFICATION UNIQUE (SSO)	C 6. MULTIFACTEUR	F 7. PASSERELLE	A 8. PROVISIONNER

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 ZERO TRUST	2 IP DÉDIÉE	3 IPSEC	4 TABLEAU DE BORD
5 CONNEXION UNIQUE	6 MULTIFACTEUR		

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

1 B – IPDEDIEE	2 G – PASSERELLE	3 H – PROVISIONNEMENT	4 F – MULTIFACTEUR
5 C – IPSEC	6 A – ZEROTRUST	7 E – CONNEXIONUNIQUE	8 D – TABLEAUDEBORD

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer ZERO TRUST, IP DÉDIÉE et IPSEC 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.

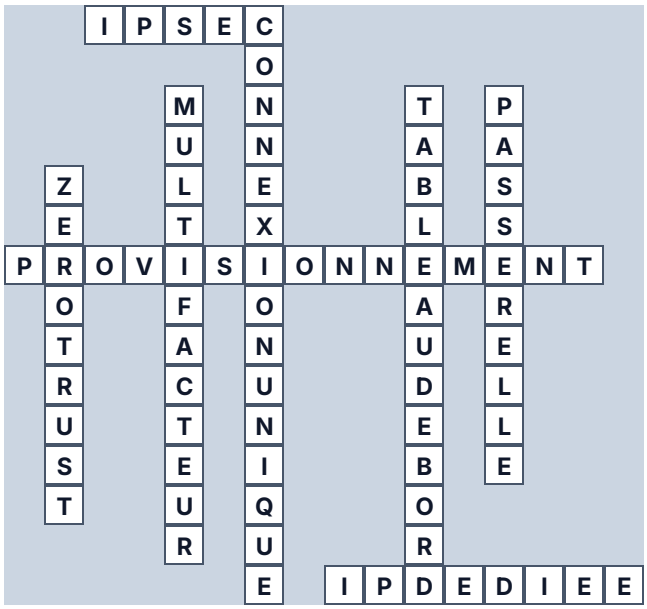
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: IPSEC Norme de tunnel site à site (5 lettres)

7 horizontal: PROVISIONNEMENT Attribution des licences d'accès VPN aux employés (15 lettres)

8 horizontal: IPDEDIEE Adresse de passerelle statique inscrite sur liste blanche (8 lettres)

VERTICALEMENT

2 vertical: CONNEXIONUNIQUE Liaison d'identité avec Okta et Entra ID (15 lettres)

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

4 vertical: TABLEAUDEBORD Portail central où le responsable informatique gère les postes (13 lettres)

5 vertical: PASSERELLE Nœud de routage à l'entrée du réseau (10 lettres)

6 vertical: ZEROTRUST Cadre de vérification continue de la confiance (9 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. RTOEZUSTR — **ZEROTRUST**
2. ICESP — **IPSEC**
3. CNUOUXNNINOEIQE — **CONNEXIONUNIQUE**
4. RLEESLEPAS — **PASSERELLE**
5. DIPEEIED — **IPDEDIEE**
6. EBUAOBRETADDL — **TABLEAUDEBORD**
7. CTIMUAREULFT — **MULTIFACTEUR**
8. TENVINNRSPOOEMI — **PROVISIONNEMENT**

CORRIGÉ DU DÉFI DU CODE SECRET

"ZERO TRUST VERIFIE TOUT APPAREIL CONNECTE"

Corrigé des études de cas

A Étude de cas 1 : Migration vers le Zero Trust

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une entreprise veut sécuriser ses serveurs locaux en vérifiant en continu les certificats de conformité des appareils, l'état du pare-feu et la localisation des utilisateurs, plutôt que de faire confiance à toute personne présente sur le réseau.
- Stratégie et solution recommandées : le directeur doit migrer vers un modèle d'accès réseau Zero Trust (ZTNA), qui impose des contrôles de sécurité continus fondés sur le contexte.

B Étude de cas 2 : Restriction de la passerelle

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une entreprise héberge des bases de données financières privées dans le cloud. Elle veut bloquer tout accès public par Internet aux panneaux d'administration et n'autoriser les connexions que depuis des terminaux vérifiés de l'entreprise.
- Stratégie et solution recommandées : l'administrateur doit configurer une passerelle à IP dédiée sur le VPN d'entreprise et ajouter cette adresse statique à la liste blanche du pare-feu de la base de données cloud.