Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

Réseaux et télécommunications

Session 2026 • Code sujet : **26-BUT-RT-EP1** • Durée : **2 heures** • Coefficient : **3, indicatif**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Analyse fonctionnelle et exigences de sécurité (3 questions) **Page 3**

2. Étude technologique et dimensionnement (3 questions) **Page 5**

3. Préparation de la mise en œuvre et protocole opératoire (3 questions) **Page 8**

4. Prévention, exploitation et réaction à un incident (2 questions) **Page 11**

5. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 12**

Sujet officiel (PDF) : https://butrt.fr/assets/annales/but-rt/C9 - Mettre en œuvre un système d'information sécurisé pour une petite structure/2026/BUT Réseaux et Télécommunications - C9 - Mettre en œuvre un système d'information sécurisé pour une petite structure - Session 2026 - 1-Sujet.pdf

1. Analyse fonctionnelle et exigences de sécurité

L'association Les Ateliers du Canal veut moderniser son système d'information sans interrompre durablement son activité, en séparant notamment les équipements internes des visiteurs. À partir du cahier des charges et des ressources techniques, l'analyse porte sur les besoins, les zones réseau et la protection des données et des accès.

Question 1.1. Relever trois besoins fonctionnels de l'association et associer à chacun un équipement ou un service réseau qui contribue à le satisfaire. Présenter la réponse sous forme de liste structurée.

1. **Accéder à Internet :** la connexion opérateur et le pare-feu assurent l'accès au réseau public et le routage.
2. **Partager les fichiers de l'association :** le serveur de fichiers hébergé dans le local technique fournit un partage aux postes du personnel.
3. **Donner un accès Wi-Fi aux visiteurs sans ouvrir le réseau interne :** les points d'accès diffusent un réseau visiteurs distinct, isolé par les VLAN et filtré par le pare-feu.

Ces équipements répondent aux usages demandés tout en tenant compte de la séparation entre visiteurs et association.

> ✓ **RÉPONSE À RETENIR**
>
> Besoins : accès Internet, partage des fichiers professionnels et Wi-Fi visiteurs distinct du réseau interne.

Question 1.2. Proposer une séparation logique des équipements en zones réseau. Pour chaque zone, préciser les équipements ou usagers concernés et l'objectif de sécurité recherché. Traiter au minimum les réseaux interne et visiteurs, les serveurs et l'administration.

Le commutateur administrable sépare les zones en VLAN et le pare-feu contrôle les échanges interzones. Les équipements et usagers sont répartis ainsi :

Zone	Usagers ou équipements	Objectif de sécurité
Personnel, VLAN 10	Postes internes, imprimantes et téléphones IP	Accéder aux ressources professionnelles autorisées
Visiteurs, VLAN 20	Appareils des visiteurs	Permettre l'accès Internet, sans accès aux zones internes
Serveurs, VLAN 30	Serveur de fichiers	Protéger les données et limiter les flux entrants
Administration, VLAN 99	Postes administrateurs et interfaces de gestion	Réserver la gestion aux personnes autorisées

Le réseau visiteurs ne doit joindre ni le personnel, ni les serveurs, ni l'administration. Les échanges nécessaires sont autorisés explicitement par le pare-feu.

> ✓ **RÉPONSE À RETENIR**
>
> Quatre zones séparées : personnel VLAN 10, visiteurs VLAN 20, serveurs VLAN 30 et administration VLAN 99, avec filtrage interzones.

Question 1.3. Indiquer deux mesures concrètes de protection des données personnelles et deux mesures de sécurisation des comptes ou des équipements. Pour chaque mesure, préciser le risque réduit et tenir compte de la minimisation des données, de la limitation des accès et de la protection des données de l'association.

Les mesures doivent limiter les données traitées et les accès, puis réduire les risques de compromission des comptes et équipements.

- **Données personnelles :** ne conserver que les informations nécessaires aux activités, afin de réduire l'impact d'une fuite.
- **Données personnelles :** attribuer les droits selon le besoin professionnel, afin d'éviter les consultations ou modifications non autorisées.

- **Comptes :** utiliser des comptes nominatifs protégés par des mots de passe robustes, afin de limiter l'usurpation et de tracer les actions.
- **Équipements :** appliquer les mises à jour et désactiver les services inutiles, afin de réduire l'exploitation de vulnérabilités.

> **✓ RÉPONSE À RETENIR**
>
> Minimiser les données conservées, limiter les droits, individualiser les comptes et maintenir les équipements à jour.

2. Étude technologique et dimensionnement

Le projet dispose du bloc privé 192.168.40.0/24 et doit desservir quatre zones réseau de tailles différentes. Les ressources techniques donnent les caractéristiques et les prix des équipements ainsi que les données de stockage et de puissance nécessaires au dimensionnement.

Question 2.1. Compléter le tableau DR 1 pour chaque zone avec le préfixe CIDR, l'adresse réseau, le masque décimal, les première et dernière adresses utilisables, l'adresse de diffusion et l'adresse de passerelle. Attribuer des sous-réseaux sans chevauchement, dans l'ordre décroissant des besoins à partir de 192.168.40.0/24, et justifier chaque préfixe par le nombre d'adresses utilisables.

Le préfixe minimal doit fournir au moins le nombre demandé d'adresses utilisables. Un besoin de 41 impose /26 (62 hôtes), tandis que 15 impose /27 (30 hôtes), car /28 n'en offre que 14. Chaque besoin de 6 correspond à /29 (6 hôtes). Les blocs sont attribués dans l'ordre demandé, aux limites de sous-réseau correspondantes. La première adresse utilisable est réservée à la passerelle.

Zone	Besoin	Préfixe	Adresse réseau	Masque décimal	Première utilisable	Dernière utilisable	Diffusion	Passerelle
Visiteurs VLAN 20	41	/26, 62 utilisables	192.168.40.0	255.255.255.192	192.168.40.1	192.168.40.62	192.168.40.63	192.168.40.1
Personnel VLAN 10	15	/27, 30 utilisables	192.168.40.64	255.255.255.224	192.168.40.65	192.168.40.94	192.168.40.95	192.168.40.65
Serveurs VLAN 30	6	/29, 6 utilisables	192.168.40.96	255.255.255.248	192.168.40.97	192.168.40.102	192.168.40.103	192.168.40.97
Administration VLAN 99	6	/29, 6 utilisables	192.168.40.104	255.255.255.248	192.168.40.105	192.168.40.110	192.168.40.111	192.168.40.105

Plan d'adressage DR 1 complété

Zone et VLAN	Besoin en hôtes	Préfixe CIDR	Adresse réseau	Masque décimal	Première adresse utilisable	Dernière adresse utilisable	Adresse de diffusion	Passerelle
Visiteurs VLAN 20	41	/26	192.168.40.0	255.255.255.192	192.168.40.1	192.168.40.62	192.168.40.63	192.168.40.1
Personnel VLAN 10	15	/27	192.168.40.64	255.255.255.224	192.168.40.65	192.168.40.94	192.168.40.95	192.168.40.65
Serveurs VLAN 30	6	/29	192.168.40.96	255.255.255.248	192.168.40.97	192.168.40.102	192.168.40.103	192.168.40.97
Administration VLAN 99	6	/29	192.168.40.104	255.255.255.248	192.168.40.105	192.168.40.110	192.168.40.111	192.168.40.105

✓ RÉPONSE À RETENIR

Visiteurs /26, personnel /27, serveurs /29, administration /29. Les blocs sont contigus, sans chevauchement, et chaque passerelle est la première adresse utilisable.

Question 2.2. **Calculer la puissance PoE totale nécessaire aux équipements alimentés par le commutateur, appliquer une réserve de dimensionnement de 20 %, puis vérifier si le budget PoE de 120 W est suffisant. Présenter les calculs avec leurs unités.**

Les équipements alimentés par le commutateur sont les deux points d'accès et les deux téléphones IP. La puissance maximale cumulée vaut :

Avant réserve : 2 × 13 W + 2 × 5 W = 36 W.
Avec 20 % de réserve : 36 W × 1,20 = 43,2 W.

Le budget PoE de 120 W dépasse le besoin dimensionné de 43,2 W. Il est donc suffisant, avec une marge disponible de 76,8 W.

Calculs PoE complétés sur le DR 1

Calculs de puissance PoE et de capacité de stockage

Calcul	Expression et résultat	Conclusion
Puissance PoE nécessaire avant réserve	2 × 13 W + 2 × 5 W = 36 W	120 W > 36 W
Puissance PoE avec réserve de 20 %	36 W × 1,20 = 43,2 W	120 W > 43,2 W
Capacité de stockage après croissance de 30 %		

Justifier les résultats et conclure sur la capacité des équipements

✓ **RÉPONSE À RETENIR**

Besoin PoE : 36 W, soit 43,2 W avec réserve. Le budget de 120 W est suffisant, avec 76,8 W de marge.

Question 2.3. **Calculer la capacité minimale de stockage après une croissance des données de 30 %, puis vérifier si deux disques de 2 To en miroir fournissent une capacité utile suffisante. Calculer ensuite le coût total des équipements de la nomenclature et la marge par rapport au plafond de 2 500 € HT, en détaillant les opérations.**

Après croissance, le besoin est de 1,2 To × 1,30 = 1,56 To. Le miroir de deux disques de 2 To fournit 2 To utiles : la capacité convient, avec 0,44 To disponibles au-delà du besoin.

Équipement	Calcul	Sous-total HT
Pare-feu	1 × 420 €	420 €
Commutateur	1 × 360 €	360 €
Points d'accès	2 × 110 €	220 €
Téléphones IP	2 × 75 €	150 €
Serveur	1 × 650 €	650 €
Disques durs	2 × 95 €	190 €
Onduleur	1 × 180 €	180 €
Câblage et accessoires	1 × 160 €	160 €

Le total des équipements est de 2 330 € HT. Soustrait du plafond de 2 500 € HT, il laisse une marge de 170 €.

Capacité de stockage complétée sur le DR 1

Calculs de puissance PoE et de capacité de stockage

Calcul	Expression et résultat	Conclusion
Puissance PoE nécessaire avant réserve	.....	.....
Puissance PoE avec réserve de 20 %	.....	.....
Capacité de stockage après croissance de 30 %	..... 1,2 To × 1,30 = 1,56 To	..... 2 To utiles : suffisant

Justifier les résultats et conclure sur la capacité des équipements.

Nomenclature et budget DR 1 complétés

Équipement	Quantité	Prix unitaire HT	Sous-total HT
Pare-feu	1	420 €	420 €
Commutateur administrable PoE+	1	360 €	360 €
Points d'accès Wi-Fi	2	110 €	220 €
Téléphones IP	2	75 €	150 €
Serveur	1	650 €	650 €
Disques durs	2	95 €	190 €
Onduleur	1	180 €	180 €
Câblage et accessoires	1 lot	160 €	160 €
Total HT et marge budgétaire	.....	.....	2 330 € HT

Marge : 170 €

✓ RÉPONSE À RETENIR

Capacité requise : 1,56 To, couverte par 2 To utiles. Coût total : 2 330 € HT. Marge sous le plafond : 170 €.

3. Préparation de la mise en œuvre et protocole opératoire

La mise en service doit isoler les visiteurs tout en préservant les accès autorisés aux ressources internes. Le pare-feu fournit les services DHCP et DNS, et les ressources techniques précisent les VLAN, les flux autorisés et les contrôles attendus pour la recette.

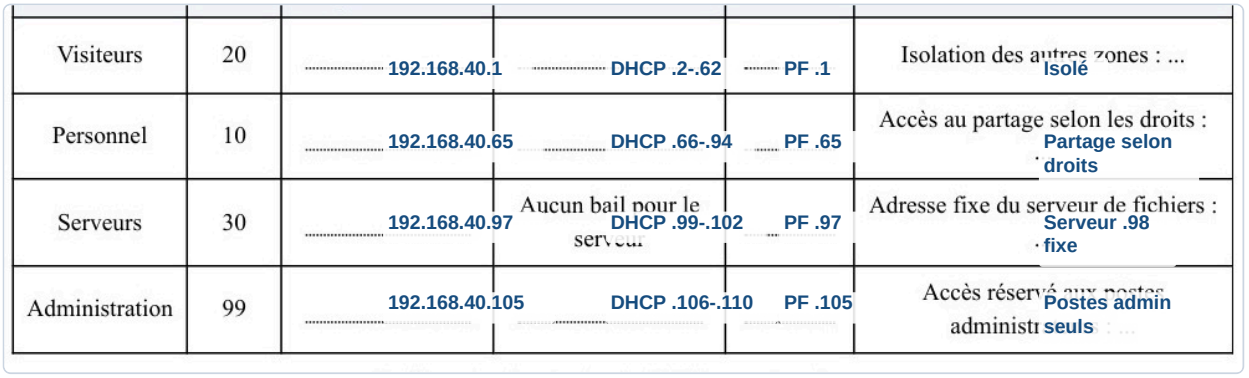
Question 3.1. Compléter le DR 2 par une configuration de principe précisant, pour chaque zone, l'interface ou le VLAN, la passerelle, le service DHCP et l'accès DNS. Indiquer explicitement que le serveur de fichiers de la zone serveurs reçoit une adresse fixe et veiller à la cohérence avec le plan d'adressage du DR 1.

Le pare-feu fournit DHCP et DNS sur les interfaces de chaque VLAN. Les passerelles utilisent la première adresse disponible ; les plages DHCP excluent donc cette adresse réservée. Configuration cohérente avec l'attribution contiguë des sous-réseaux :

Zone	VLAN	Passerelle	DHCP	DNS	Configuration
Visiteurs	20	192.168.40.1	Oui, .2 à .62	192.168.40.1	Accès isolé aux autres zones
Personnel	10	192.168.40.65	Oui, .66 à .94	192.168.40.65	Partage selon les droits du compte
Serveurs	30	192.168.40.97	Oui pour les autres équipements, .99 à .102	192.168.40.97	Serveur fixe : 192.168.40.98
Administration	99	192.168.40.105	Oui, .106 à .110	192.168.40.105	Accès réservé aux postes administrateurs

Le serveur de fichiers est exclu du DHCP et configuré en adresse fixe. Les points d'accès associent les SSID interne et visiteurs à leurs VLAN respectifs. Les plages DHCP indiquées respectent les limites de chaque sous-réseau et ne comprennent ni passerelle ni adresse fixe du serveur.

Configuration logique des VLAN complétée



✓ **RÉPONSE À RETENIR**

Passerelles VLAN 20, 10, 30 et 99 : 192.168.40.1, .65, .97 et .105. DNS : pare-feu. Serveur de fichiers fixe : 192.168.40.98.

Question 3.2. Établir une politique minimale de filtrage conforme aux flux autorisés du DT 3. Présenter au moins quatre règles ordonnées indiquant la source, la destination, le service ou port, l'action et une justification, avec un refus par défaut entre zones.

Appliquer les autorisations ciblées avant le refus par défaut. Le DNS des visiteurs vers le pare-feu reste autorisé, mais ne donne aucun accès aux autres ressources internes.

1. **Personnel et visiteurs vers le pare-feu :** DNS UDP/TCP 53, autoriser vers le service désigné.
2. **Visiteurs vers personnel, serveurs et administration :** tous services, refuser pour assurer l'isolement.
3. **Visiteurs vers Internet :** navigation, autoriser selon le filtrage et avec traduction d'adresses.
4. **Personnel autorisé vers le serveur de fichiers :** TCP 445, autoriser selon les droits du compte.

5. **Administration vers les équipements :** HTTPS TCP 443 et seuls les protocoles d'administration nécessaires, autoriser depuis les postes administrateurs.
6. **Serveur vers Internet :** HTTPS TCP 443 pour les mises à jour, autoriser selon la politique de l'association.

Refuser ensuite tout autre flux interzone non explicitement autorisé.

Règles de filtrage complétées

Ordre	Source	Destination	Service ou port	Action	Justification
1	Personnel + Pare-feu	DNS	UDP/TCP 53	DNS désigné	
2	Visiteurs	Réseaux internes	Tous flux	Isoler visiteurs	
3	Visiteurs	Internet	Navigation filtrée	Accès Internet	
4	Personnel a	Serveur fichiers	TCP 445	Selon droits	
Dernière règle	Toutes zones	Toutes destinations interzones	Tous services non précédemment autorisés	Défaut interzone	

Classer les règles dans l'ordre d'application. Ajouter une règle de refus par défaut.

5. Administration -> équipements : HTTPS TCP 443 et protocoles nécessaires, depuis les postes admin uniquement.
6. Serveur -> Internet : HTTPS TCP 443 pour les mises à jour, selon la politique.

✓ RÉPONSE À RETENIR

Autoriser DNS, navigation visiteurs filtrée, SMB autorisé, administration réservée et mises à jour HTTPS du serveur ; refuser tous les autres flux interzones.

Question 3.3. Rédiger un protocole de recette comprenant trois contrôles vérifiables. Pour chacun, indiquer la manipulation, le résultat attendu et le critère de réussite. Vérifier au minimum l'isolement du réseau visiteurs et l'accès autorisé au serveur de fichiers.

Effectuer les contrôles depuis les VLAN concernés avec un poste personnel, un client connecté au SSID visiteurs et un compte autorisé. Consigner les manipulations et résultats pour rendre les essais reproductibles.

Contrôle	Manipulation	Résultat attendu	Critère de réussite
DHCP personnel	Renouveler le bail puis vérifier la configuration IP.	Adresse du VLAN 10, passerelle et DNS 192.168.40.65.	Adresse dans 192.168.40.66 à .94 ; passerelle et DNS corrects.
Isolement visiteurs	Se connecter au SSID visiteurs et tester Internet, serveur et administration.	Accès Internet fonctionnel ; accès aux zones internes refusé.	Navigation possible ; connexions vers serveur et administration bloquées.
Partage de fichiers	Depuis un poste autorisé, ouvrir le partage sur 192.168.40.98.	Partage accessible en TCP 445 selon les droits du compte.	Accès en lecture ou écriture conforme aux droits attribués.

La recette est validée uniquement si chaque résultat attendu est observé. Pour l'isolement, vérifier séparément l'accès Internet et l'échec des tentatives vers le serveur et l'administration ; pour le partage, confirmer que l'accès correspond aux droits du compte testé.

Protocole de recette complété

Contrôle	Manipulation	Résultat attendu	Critère de réussite
Attribution DHCP d'un poste personnel	Renouveler bail, véri	VLAN 10, GW/DNS .65	IP .66-.94 correcte
Isolement d'un client visiteur	SSID visiteurs, teste	Internet oui, interne non	Interne bloqué
Accès au partage depuis un poste autorisé	Ouvrir partage serve	SMB TCP 445 accessible	Accès conforme aux droits

Décrire des tests reproductibles et leurs critères de réussite.

✓ RÉPONSE À RETENIR

Réussite : DHCP personnel cohérent, Internet accessible aux visiteurs sans accès interne, et partage SMB accessible selon les droits du compte autorisé.

4. Prévention, exploitation et réaction à un incident

Le système est exploité par un salarié référent sans équipe informatique dédiée, et les interventions doivent rester traçables tout en protégeant les données. Le candidat doit envisager des risques courants pour la structure et décrire la conduite à tenir face à un incident affectant des fichiers.

Question 4.1. Identifier quatre risques réalistes liés à l'exploitation de cette petite structure et associer à chacun une mesure de prévention adaptée. Inclure au moins un risque lié aux comptes, un aux sauvegardes et un au réseau sans fil.

Le référent doit privilégier des mesures simples, proportionnées et vérifiables. Les risques et leurs parades peuvent être associés directement :

Risque	Prévention
Compte compromis ou droits excessifs	Comptes nominatifs, mots de passe robustes, accès limités au besoin professionnel et retrait rapide des droits inutiles.
Sauvegarde absente, défaillante ou inutilisable	Effectuer des sauvegardes régulières, protégées et séparées du réseau, puis tester leur restauration.
Intrusion depuis le Wi-Fi visiteurs	Isoler le VLAN visiteurs des zones internes et protéger le Wi-Fi interne par une authentification robuste.
Équipement vulnérable ou configuration perdue	Appliquer les mises à jour, supprimer les services inutiles et protéger les sauvegardes de configuration.

Ces mesures répondent aux risques prioritaires indiqués dans le sujet et les ressources : accès non autorisé aux comptes ou aux données, perte de données, compromission par le réseau sans fil et exploitation de vulnérabilités. La limitation des droits et l'isolement des visiteurs réduisent l'impact d'une intrusion. Les sauvegardes doivent être testées, et les interventions de maintenance tracées afin de connaître les changements effectués et leur auteur.

> **✓ RÉPONSE À RETENIR**
>
> Comptes nominatifs aux droits limités, sauvegardes protégées et testées, Wi-Fi visiteurs isolé, équipements mis à jour et configurations sauvegardées.

Question 4.2. Face à un poste interne au comportement anormal et à des fichiers devenus illisibles, décrire dans l'ordre quatre actions immédiates pour limiter l'incident et préserver les éléments utiles à son analyse. Préciser une action à éviter et expliquer comment vérifier ultérieurement que les données peuvent être restaurées.

1. Isoler immédiatement le poste du réseau en débranchant le câble ou en désactivant le Wi-Fi. Éviter de l'éteindre si cela peut être fait sans danger.
2. Alerter le référent et les personnes compétentes. Noter l'heure, les symptômes, les messages affichés et les actions déjà réalisées.
3. Préserver les éléments utiles à l'analyse : conserver les journaux et captures disponibles, et ne pas modifier les fichiers touchés.
4. Depuis un équipement sain, sécuriser les comptes concernés et suspendre les accès ou partages potentiellement compromis.

Éviter de supprimer les fichiers, de réinstaller le poste ou de lancer des outils de nettoyage avant d'avoir préservé les éléments utiles. Vérifier ultérieurement la restauration d'un fichier de test dans un emplacement isolé : le fichier doit être lisible et contrôlé par le référent.

> **✓ RÉPONSE À RETENIR**
>
> Isoler le poste, alerter et consigner les faits, préserver les éléments d'analyse, sécuriser les accès, puis tester une restauration isolée.

Ce qu'il faut retenir de ce sujet (Session 2026)

Bilan de l'épreuve : Cette évaluation locale du BUT Réseaux et Télécommunications, session 2026, code 26-BUT-RT-EP1, dure 2 heures et porte un coefficient indicatif de 3. À partir du projet de système d'information sécurisé de l'association Les Ateliers du Canal, elle évalue l'analyse des besoins, l'adressage, le dimensionnement, le filtrage, la recette, la prévention des risques et la réaction à un incident.

Notions-clés, formules & règles à maîtriser

- Un sous-réseau IPv4 de préfixe /n fournit 2^(32-n) - 2 adresses utilisables, hors cas particuliers.
- La première adresse utilisable de chaque sous-réseau est réservée à la passerelle.
- Le dimensionnement PoE intègre une réserve de 20 % à la puissance totale des appareils alimentés.
- En miroir à deux disques, la capacité utile correspond à celle d'un seul disque.

Points de vigilance & attentes du jury

- Attribuer les sous-réseaux selon les besoins décroissants et vérifier qu'ils ne se chevauchent pas.
- Présenter les calculs de puissance avec les unités, puis comparer le résultat au budget PoE disponible.
- Ordonner les règles de filtrage et terminer par le refus des flux interzones non explicitement autorisés.
- Pour chaque test de recette, préciser une manipulation reproductible et un critère de réussite vérifiable.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment choisir le préfixe d'un sous-réseau pour le nombre d'hôtes demandé ?

Choisissez le plus petit bloc d'adresses qui couvre le besoin : le nombre d'adresses utilisables est 2^(32-n) - 2 pour un préfixe /n. Vérifiez que ce nombre inclut la passerelle réservée et les équipements à connecter.

Q : Comment construire une politique de filtrage interzones cohérente avec les flux demandés ?

Énoncez d'abord les autorisations nécessaires avec source, destination et port précis, puis appliquez le refus par défaut à tout flux interzone non prévu. Limitez les accès aux équipements et comptes autorisés, et respectez l'ordre d'évaluation des règles.

Q : Comment gérer les deux heures de l'épreuve et les points attribués ?

Le sujet attribue 5 points à la partie 1, 6 à la partie 2, 5 à la partie 3 et 4 à la partie 4. Répartissez le temps selon ces pondérations, gardez une marge pour vérifier les calculs et complétez les documents réponses demandés.

Q : Quels éléments rendent une réponse de recette ou de sécurité vérifiable par le jury ?

Le sujet demande des consignes explicites et des résultats contrôlables : indiquez les sources, destinations, ports et actions des règles, puis, pour chaque test, la manipulation, le résultat attendu et le critère de réussite. N'ajoutez pas de flux non justifiés.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C9 - Mettre en œuvre un système d'information sécurisé pour une petite structure/2026/BUT Réseaux et Télécommunications - C9 - Mettre en œuvre un système d'information sécurisé pour une petite structure - Session 2026 - 1-Sujet.pdf
Ressources BUT Réseaux et Télécommunications : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.