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

BREVET DE TECHNICIEN SUPÉRIEUR

SERVICES INFORMATIQUES AUX ORGANISATIONS : OPTION SOLUTIONS D'INFRASTRUCTURE, SYSTÈMES ET RÉSEAUX

ÉPREUVE E7 : CYBERSÉCURITÉ DES SERVICES INFORMATIQUES, SPÉCIFIQUE À L'OPTION

SESSION 2026

Durée : 4 heures

SPÉCIALITÉ / UNITÉ	COEFF
SERVICES INFORMATIQUES AUX ORGANISATIONS : OPTION SOLUTIONS D'INFRASTRUCTURE, SYSTÈMES ET RÉSEAUX	4

Moyens de calculs et matériel autorisés :

L'usage de la calculatrice n'est pas autorisé.

Aucun document ou matériel autorisé en dehors de ceux fournis avec le sujet.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 6 pages numérotées de 1/6 à 6/6.

Les documents réponses en fin de sujet sont à rendre avec la copie.

DOSSIER SUJET

MISE EN SITUATION PROFESSIONNELLE ET CONSIGNES GÉNÉRALES : NORDALIM, LILLE (NORD)

NORDALIM est une entreprise de distribution alimentaire qui emploie 85 personnes sur son site de Lille. Son système d'information comprend un réseau local segmenté, des serveurs hébergés dans les locaux, un service de sauvegarde externalisé et une application de gestion accessible aux employés. L'entreprise traite des données relatives à ses clients et à ses salariés.

Vous intervenez au sein de l'équipe informatique. Une alerte de sécurité signale des tentatives répétées de connexion au service VPN, suivies d'une authentification réussie avec un compte technique. La direction vous demande de vérifier le plan d'adressage, d'exploiter les traces d'authentification et de proposer des mesures de traitement et de prévention.

Les documents techniques DT 1 et DT 2 fournissent les éléments nécessaires. Les documents réponse DR 1 sont à compléter et à rendre avec la copie. Toute hypothèse nécessaire doit être explicitement formulée. Les réponses doivent être justifiées et adaptées au contexte de NORDALIM.

PARTIE 1 : Segmentation réseau, adressage et routage (7 points)

Sécuriser et documenter l'infrastructure réseau

Le réseau local doit être organisé en trois VLAN distincts. Les capacités minimales attendues et les paramètres de liaison avec le pare-feu figurent dans le DT 1. Le commutateur de couche 3 assure le routage entre les VLAN. La première adresse utilisable de chaque sous-réseau IPv4 est réservée à la passerelle du VLAN.

1.1 (3 points) Pour chacun des trois VLAN du DT 1, déterminez le plus petit préfixe IPv4 permettant d'accueillir le nombre d'équipements indiqué, passerelle comprise. Complétez dans le DR 1 le préfixe, l'adresse réseau, l'adresse de diffusion et la passerelle. Les sous-réseaux doivent être distincts et appartenir au bloc 10.20.0.0/24.

1.2 (2 points) Complétez dans le DR 1 la table de routage du commutateur de couche 3. Indiquez les trois routes directement connectées correspondant aux VLAN et la route par défaut vers le pare-feu. Utilisez les interfaces et l'adresse du pare-feu données dans le DT 1.

1.3 (2 points) À partir du préfixe IPv6 attribué dans le DT 1, proposez un sous-réseau IPv6 /64 pour chacun des trois VLAN, en conservant le numéro de VLAN comme valeur du quatrième groupe hexadécimal. Indiquez également, pour chaque VLAN, l'adresse IPv6 de passerelle attendue, définie comme la première adresse de ce sous-réseau.

PARTIE 2 : Exploitation des traces et requête SQL (6 points)

Analyser des événements d'authentification et produire une requête d'audit

Le DT 2 contient un extrait de la table d'événements d'authentification recueillis par le service VPN. Les horodatages sont exprimés en UTC. Le responsable de la sécurité souhaite repérer les adresses IP à l'origine d'au moins cinq authentifications refusées pendant la période étudiée.

2.1 (2 points) À partir des lignes du DT 2 comprises entre 08:00:00 inclus et 08:10:00 exclu le 12 mars 2026, comptez les événements dont le résultat est « REFUSE », regroupés par adresse IP source. Présentez le résultat pour chaque adresse IP présente dans l'extrait et identifiez celle qui atteint le seuil de cinq refus.

2.2 (2,5 points) Rédigez une requête SQL qui réalise ce comptage à partir de la table auth_event décrite dans le DT 2. La requête doit filtrer les dates et heures demandées, ne retenir que les événements « REFUSE », regrouper les résultats par adresse IP source et ne restituer que les adresses comptant au moins cinq refus.

2.3 (1,5 point) Le DT 2 indique qu'un événement « ACCEPTE » suit les refus pour le même compte et la même adresse IP. Expliquez ce que l'analyse des traces permet d'établir et ce qu'elle ne permet pas, à elle seule, de conclure. Citez deux vérifications complémentaires à effectuer pour déterminer si le compte ou les ressources internes ont été compromis.

PARTIE 3 : Traitement de l'incident et durcissement des accès (7 points)

Prévenir, détecter et traiter une atteinte à la sécurité du système d'information

Les éléments techniques du DT 2 signalent une série d'échecs de connexion au VPN suivie d'une connexion acceptée. Le compte utilisé est un compte technique dont le profil VPN ne requiert pas de second facteur. L'accès a été suivi d'une connexion au serveur de fichiers. Vous devez proposer une réponse proportionnée, préserver les éléments utiles à l'analyse et tenir compte de la présence de données à caractère personnel dans le système d'information.

3.1 (2 points) Reconstituez la chronologie des faits observables dans le DT 2. Qualifiez l'événement de sécurité le plus probable et indiquez les éléments disponibles qui justifient cette qualification.

3.2 (2 points) Présentez, dans un ordre cohérent, quatre mesures immédiates à prendre pour contenir l'incident et préserver les éléments nécessaires à son analyse. Pour chaque mesure, indiquez brièvement son objectif.

3.3 (2 points) Proposez quatre mesures de durcissement des accès au VPN et aux serveurs, couvrant au minimum l'authentification, les privilèges et la surveillance. Reliez chaque mesure au risque qu'elle réduit.

3.4 (1 point) Si l'analyse établit que des données à caractère personnel ont été consultées ou copiées sans autorisation, indiquez deux actions à engager au titre de la protection des données et précisez à qui elles incombent dans l'entreprise.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : ARCHITECTURE RÉSEAU ET PARAMÈTRES D'ADRESSAGE DE NORDALIM

Le bloc IPv4 10.20.0.0/24 est réservé aux réseaux utilisateurs et serveurs du site. Le commutateur de couche 3 SW-L3 assure le routage inter-VLAN. Les interfaces virtuelles de chaque VLAN portent la passerelle IPv4 et IPv6. La liaison entre SW-L3 et le pare-feu FW-01 est un réseau de transit indépendant. Le pare-feu est la sortie vers Internet. Le préfixe IPv6 global délégué au site est 2001:db8:4a10:1200::/56. Pour les questions, une adresse IPv4 de sous-réseau comporte une adresse réseau et une adresse de diffusion non attribuables aux équipements.

Topologie logique du site

Équipement ou réseau	Raccordement	Rôle
PC et imprimantes des employés	SW-L3, VLAN 10	Réseau utilisateurs
Serveurs AD, fichiers et application	SW-L3, VLAN 20	Réseau serveurs
Postes d'administration	SW-L3, VLAN 30	Réseau administration
SW-L3	Liaison de transit vers FW-01	Routage inter-VLAN et sortie vers le pare-feu
FW-01	Transit 172.16.0.0/30, puis Internet	Filtrage et accès Internet
Service VPN	Terminé sur FW-01	Accès distant des utilisateurs et comptes techniques

Les équipements reliés à SW-L3 sont raccordés au VLAN indiqué.

Besoins et paramètres connus

VLAN	Usage	Capacité minimale	Interface de routage
10	Utilisateurs	50 adresses	SVI VLAN 10 sur SW-L3
20	Serveurs	25 adresses	SVI VLAN 20 sur SW-L3
30	Administration	10 adresses	SVI VLAN 30 sur SW-L3
Transit	SW-L3 vers FW-01	Réseau attribué : 172.16.0.0/30	SW-L3 : 172.16.0.2/30 ; FW-01 : 172.16.0.1/30
IPv6	Préfixe global du site	2001:db8:4a10:1200::/56	Une passerelle par VLAN

Les capacités indiquées sont les nombres minimaux d'adresses d'équipements à attribuer, passerelle comprise.

DT 2 : TRACES D'AUTHENTIFICATION VPN ET INFORMATIONS D'INCIDENT

Les événements ci-dessous proviennent de la table auth_event du service VPN. Le champ event_time est un horodatage UTC. Le champ src_ip contient l'adresse IP source observée par le service. Les valeurs

possibles de result sont « REFUSE » et « ACCEPTE ». Les événements couvrant la période utile sont reproduits intégralement.

Schéma de la table : auth_event(event_time TIMESTAMP, src_ip VARCHAR(45), username VARCHAR(64), result VARCHAR(10)). Chaque ligne représente un événement d'authentification. L'extrait a été collecté le 12 mars 2026.

Les journaux de FW-01 indiquent qu'à 08:08:41 UTC, une connexion VPN a été acceptée pour svc-backup depuis 203.0.113.77. Le profil de ce compte ne requiert pas de second facteur. À 08:11:03 UTC, le même compte a ouvert une session SMB vers le serveur de fichiers FS-01. Les traces fournies ne donnent aucune information sur les fichiers consultés ou copiés. Les journaux sont exportés dans un espace de collecte dédié, en lecture seule pour les analystes.

Extrait de la table auth_event

event_time	src_ip	username	result
2026-03-12 08:01:12	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:02:04	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:03:19	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:04:26	198.51.100.24	jmartin	REFUSE
2026-03-12 08:05:33	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:06:40	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:07:11	198.51.100.24	jmartin	REFUSE
2026-03-12 08:07:52	203.0.113.77	svc-backup	REFUSE
2026-03-12 08:08:41	203.0.113.77	svc-backup	ACCEPTE

Horodatages en UTC, le 12 mars 2026.

Éléments complémentaires issus des journaux

Horodatage UTC	Source	Observation
12 mars 2026, 08:08:41	FW-01	Connexion VPN acceptée pour svc-backup depuis 203.0.113.77
12 mars 2026, 08:11:03	FW-01	Session SMB ouverte vers FS-01 avec le compte svc-backup
Collecte	Système de journalisation	Export conservé dans un espace dédié, en lecture seule pour les analystes
Périmètre connu	Système d'information	Présence de données clients et de données relatives aux salariés

Les observations sont limitées aux faits consignés dans les journaux.

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Document réponse à rendre avec la copie : questions 1.1 et 1.2 **À RENDRE AVEC LA COPIE**

Compléter les cellules marquées « ... ». Pour la question 1.1, inscrire les valeurs IPv4 demandées. Pour la question 1.2, inscrire les routes nécessaires au routage sur SW-L3, en utilisant les interfaces et adresses indiquées dans le DT 1. Ce document est à rendre avec la copie.

Plan d'adressage IPv4 à compléter

VLAN	Nombre minimal d'adresses	Préfixe CIDR	Adresse réseau	Adresse de diffusion	Passerelle
10	50	.....	.....	.....	.....
20	25	.....	.....	.....	.....
30	10	.....	.....	.....	.....

Une ligne par VLAN. Les préfixes doivent être compatibles avec les besoins du DT 1.

Table de routage de SW-L3 à compléter

Destination	Préfixe	Prochain saut	Interface ou VLAN
.....	.....	Directement connecté	VLAN 10
.....	.....	Directement connecté	VLAN 20
.....	.....	Directement connecté	VLAN 30
.....	.....	.....	Liaison vers FW-01

Indiquer les routes directement connectées et la route par défaut.

Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :

.....

.....

.....

.....

.....

.....

.....

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.