CAS Gaura

Barème

DOSSIER A	**Audit de sécurité du réseau de la CCPG et proposition de remédiation**	52 points
DOSSIER B	**Intégration des équipements personnels des télétravailleurs**	28 points
	TOTAL	80 points

Éléments de corrigé

Dossier A – Audit de sécurité et remédiation de l'infrastructure réseau

Mission A1 – Réalisation de tests d'intrusion sur le réseau interne et proposition de remédiation

Question A1.1 En utilisant le compte-rendu technique correspondant à cette attaque : a) Indiquer le service visé.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		Le service visé a été correctement identifié
Bonne Maîtrise		
Maîtrise partielle		
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

a. Service visé

Le service visé est le service BOOTP/DHCP *port UDP 67 (non exigé)*.

Question A1.1 b) Expliquer le fonctionnement de cette attaque.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		La description de l'attaque témoigne d'une bonne compréhension de celle-ci
Bonne Maîtrise		
Maîtrise partielle		La description de l'attaque est peu convaincante et ne permet pas de déterminer le niveau de compréhension du candidat
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

b. Fonctionnement

Scapy permet de concevoir des trames et de les envoyer. Ici les trames envoyées sont des trames DISCOVER DHCP (c'est-à-dire des requêtes de demande d'attribution de paramètres IP). Elles sont envoyées en grand nombre (ici il s'agit même d'une boucle infinie) via des trames de diffusion avec des adresses MAC sources différentes.

Non demandé : si on analyse la composition du paquet émis on voit les différentes couches :

- *couche 2 : Ether() pour Ethernet avec une adresse MAC source (aléatoire) et MAC destination de diffusion (ff :ff :ff :ff :ff :ff).*
- *couche 3 : IP() avec IP source 0.0.0.0 et IP dest diffusion 255.255.255.255 (on ne connaît pas l'adresse IP du serveur DHCP) et BOOTP() sur lequel se base DHCP qui utilise les ports 67 (serveur) et 68 (client).*
- *Couche 4 : UDP car DHCP utilise ce protocole avec les ports source 68 et destination 67.*
- *Couche 7 : DHCP() permet d'indiquer le type de message, ici on veut saturer le serveur avec des messages de type DISCOVER.*

Question A1.1 c) Préciser l'objectif et les conséquences d'une telle attaque. *Vous préciserez le type d'attaque.*		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		L'objectif et les conséquences sont correctement expliqués
Bonne Maîtrise		L'objectif et les conséquences sont correctement définis mais l'explication est incomplète
Maîtrise partielle		Seuls l'objectif et les conséquences sont fournis par le candidat
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

c. Objectif et conséquences

Il s'agit de saturer le service DHCP et donc le serveur DHCP de la CCPG afin de créer une attaque de type DOS (Déni de Services). Le serveur reçoit les requêtes DISCOVER et va réserver une adresse IP par paquet dans son pool d'adresse disponible (il y a effectivement un pool pour le VLAN 90 192.168.90.50 à 192.168.90.149 qui ne comprend que 100 IP).

Les statistiques montrent, qu'après l'attaque, il n'y a plus d'adresses disponibles.

Lors de requêtes légitimes, le serveur DHCP ne pourra donc plus attribuer de bail. L'accès au réseau de la CCPG ne sera plus possible.

Non demandé :

- *C'est une attaque de type DHCP starvation c'est-à-dire un flooding de requêtes DISCOVER de façon à réaliser un déni de services (DOS). On le voit sur les statistiques, après l'attaque plus aucune adresse n'est disponible dans le pool wifi (VLAN90).*
- *on ne voit rien dans les baux (qui ne sont pas réellement attribués) car notre attaque n'envoie pas de DHCP Request.*
- *A la suite de cette attaque, on enchaîne généralement avec une attaque DHCP Rogue (=DHCP illégitime) également appelé DHCP spoofing/snooping. On passe d'une attaque de type DOS à une attaque MITM (Man in the Middle)*

Question A1.1 d) Proposer, en justifiant, deux contre-mesures à utiliser.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		Les deux contre-mesures sont correctement justifiées.
Bonne Maîtrise		Les deux contre-mesures sont correctement fournies mais insuffisamment justifiées OU une seule contre-mesure est justifiée
Maîtrise partielle		Une seule mesure est fournie sans aucune justification
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

d. Parades

- NIDS et NIPS (Network Intrusion Detection/Prevention System) pour détecter des envois massifs de paquets DHCP Discover ou DHCP OFFER par des serveurs illégitimes.
- Mise en place d'une authentification des accès via 802.1x et serveur RADIUS.
- Mise en place du mécanisme port-security sur les commutateurs.
- Pas de plage DHCP mais réservation d'adresses.
- Pas de serveur DHCP mais un adressage statique.
- Supervision des baux DHCP libres/attribués (avec un outil si possible et alerte en cas dépassement seuil via SMS ou email).
- Configuration de la fonction DHCP Snooping avec limitation de nombre de requêtes envoyées par unité de temps.

Question A1.2 Rédiger le compte-rendu en intégrant les éléments suivants : a) les étapes essentielles de la démarche permettant d'arriver à l'objectif demandé.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		La description des deux étapes est pertinente
Bonne Maîtrise		Les deux étapes sont présentes mais la description reste superficielle OU la description d'une étape est pertinente
Maîtrise partielle		Une seule étape insuffisamment décrite
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

a) Le service DHCP légitime étant indisponible suite à la première attaque DHCP Starvation, l'idée est ensuite de réaliser une attaque DHCP Rogue de la façon suivante :

1. Création d'un serveur DHCP pirate illégitime qui fournira une configuration réseau qui pointera vers la machine attaquante au niveau de la passerelle par défaut (et/ou du service DNS).
2. *Désactivation de l'ICMP redirect sur la machine attaquante afin d'éviter que la victime ne soit amenée à renvoyer ses paquets à la passerelle par défaut légitime.*
3. Activation du routage sur la machine attaquante pour permettre l'acheminement des paquets vers la passerelle par défaut légitime.

4. *Analyse du trafic reçu sur la machine attaquante à l'aide de Wireshark ou de tcpdump pour récupérer des données pertinentes.*

Question A1.2 Rédiger le compte-rendu en intégrant les éléments suivants : b) les finalités de cette seconde attaque.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		La description des finalités témoigne d'une bonne compréhension de celles-ci
Bonne Maîtrise		
Maîtrise partielle		La description des finalités est peu convaincante et ne permet pas de déterminer le niveau de compréhension du candidat
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

b) Cette seconde attaque a pour objectif de fournir une configuration réseau aux victimes permettant à l'attaquant de récupérer tous les paquets émis vers l'extérieur du réseau (et éventuellement toutes les requêtes DNS). Pour cela, l'attaquant définit comme passerelle par défaut et serveur DNS à distribuer au client DHCP l'adresse de sa propre machine.

Question A1.2 Rédiger le compte-rendu en intégrant les éléments suivants : c) une contre-mesure à mettre en œuvre afin d'empêcher qu'une attaque comme celle-ci puisse se produire.		
Compétence évaluée : Sécuriser les équipements et les usages des utilisateurs • Identifier les menaces et mettre en œuvre les défenses appropriées		
Excellente Maîtrise		La contre-mesure est pertinente et correctement justifiée
Bonne Maîtrise		La contre-mesure est pertinente mais insuffisamment justifié
Maîtrise partielle		La contre-mesure est peu pertinente mais empêche partiellement l'attaque
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

c) Mettre en place la fonction de sécurité « DHCP Snooping » sur l'ensemble des commutateurs concernés. Le DHCP Snooping permet de définir sur quels ports seront connectés les serveurs DHCP légitimes. Ainsi, tout serveur pirate qui essaiera d'émettre des requêtes DHCP Offer sur un port non prévu à cet effet se verra rejeter sa requête.

On acceptera aussi d'autres solutions comme la mise en place d'une authentification filaire par le protocole 802.1x.

Mission A2 – Audit de la DMZ et mise en œuvre d'une nouvelle architecture

Question A2.1 a) Expliquer quels sont les risques techniques inhérents au protocole HTTP au regard des critères de sécurité concernés (authentification, intégrité, confidentialité).		
Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Caractériser les risques liés à l'utilisation malveillante d'un service informatique		
Excellente Maîtrise		Deux risques sur trois sont correctement expliqués
Bonne Maîtrise		
Maîtrise partielle		Les deux risques ne sont pas correctement expliqués OU un seul risque identifié et expliqué
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

Le protocole HTTP présente les risques suivants :

- Les communications ne sont pas chiffrées, les données circulent en clair, elles peuvent donc être interceptées par un tiers malveillant. Ainsi la confidentialité n'est pas assurée.
- Il n'existe aucun mécanisme permettant de s'assurer que les données n'ont pas été modifiées (le principe d'intégrité des données n'est pas assuré).
- Le serveur sur lequel le personnel et les usagers se connectent n'est pas authentifié. Ces derniers peuvent être victimes d'une usurpation d'URL.

Le protocole HTTP n'est pas un protocole sécurisé. Il est absolument à proscrire, notamment lorsque l'on se connecte à une interface avec une nécessité d'authentification.

Question A2.1 b) Identifier les conséquences économiques et juridiques pour la communauté de communes si lesdits risques techniques identifiés venaient à être exploités par un tiers malveillant.		
Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité		
Excellente Maîtrise		Une conséquence économique et une conséquence juridique correctement fournies par le candidat
Bonne Maîtrise		
Maîtrise partielle		Une seule conséquence apportée
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

En dehors d'une dégradation de la qualité du service pouvant engendrer une altération de l'image des collectivités avec une perte de confiance dans le service public les conséquences peuvent être les suivantes :

- Préjudices financiers directs (éventuellement investigation, réinstallation, reconfiguration…).
- Préjudices financiers indirects (pertes de recettes de services comme la piscine ou le stationnement).

- Dans l'hypothèse d'une cyberattaque frappant une collectivité locale et occasionnant une fuite de données personnelles (ex. : données issues des comptes utilisateurs d'un téléservice), la CNIL pourrait décider de sanctions pécuniaires dès lors qu'elle considérerait que cette fuite de données résulte en partie de manquements graves aux mesures de sécurité nécessaires à la protection des données personnelles.
- Des entreprises ou des administrés pourraient réclamer l'indemnisation des préjudices subis du fait des conséquences d'une cyberattaque, s'il peut être établi que les conséquences dommageables de l'attaque sont imputables à des manquements de l'administration dans l'application de la réglementation relative aux systèmes d'information.

Question A2.2 Expliquer quel est l'inconvénient d'utiliser la même clé privée et donc le même certificat SSL/TLS multi-domaine sur chacun des serveurs *web*.		
Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure		
Excellente Maîtrise		L'inconvénient est correctement expliqué
Bonne Maîtrise		
Maîtrise partielle		Inconvénient insuffisamment expliqué
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

Le certificat multi-domaine offre une grande souplesse, car il est unique et peut-être déployé sur plusieurs hôtes différents. Ce type de certificat est très souvent utilisé dans le cas d'hébergement mutualisé ou lorsque l'on utilise des réseaux de diffusion de contenus (CDN) tels que AKAMAI ou CloudFlare.

L'inconvénient est que si le certificat ou la clé privée du certificat multi-domaines sont compromis, ce sont l'ensemble des hôtes concernés qui peuvent directement être impactés.

- Dans le cas présent, la compromission du certificat multi-domaine utilisé impacterait les trois serveurs web.

Question A2.3 Justifier l'intérêt d'utiliser des clés privées et des certificats distincts sur le serveur mandataire inversé (reverse proxy) et les serveurs *web*.		
Compétence évaluée : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Prévenir les attaques		
Excellente Maîtrise		Les deux éléments de justification sont présents
Bonne Maîtrise		
Maîtrise partielle		Un seul élément de justification présent
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

- L'intérêt de cette solution est de limiter l'impact d'une éventuelle compromission d'un certificat et de sa clé privée. Ainsi, il ne sera pas nécessaire de révoquer l'ensemble des certificats présents. L'authentification, l'intégrité et le chiffrement seront toujours préservés sur au moins une partie du trajet.
- La surface d'attaque sera réduite puisque le pirate devrait cibler uniquement le réseau interne ou externe (en fonction du certificat compromis) pour réaliser une éventuelle attaque MITM.

Question A2.4 Justifier l'intérêt de mettre en œuvre un chiffrement TLS depuis le client jusqu'aux trois serveurs *web* hébergés dans la zone démilitarisée intermédiaire.		
Compétence évaluée : Préserver l'identité numérique de l'organisation • Protéger l'identité numérique d'une organisation		
Excellente Maîtrise		La justification fournie témoigne de la bonne compréhension de la problématique
Bonne Maîtrise		
Maîtrise partielle		La justification témoigne d'une compréhension incomplète de la problématique
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

Le chiffrement du début à la fin de la connexion TLS permet de réduire les risques d'interception et d'attaques depuis l'extérieur mais également depuis le réseau interne.

- En cas de compromission du réseau local ou au sein des DMZ, le chiffrement entre le reverse-proxy et les serveurs web permet de se prémunir contre certaines attaques et contre la récupération de flux et données sensibles.

On a tendance à mésestimer à tort le risque d'attaque ou de compromission depuis l'intérieur de l'infrastructure alors que c'est l'un des scénarios les plus courant (malveillance, attaque par charge utile).

Question A2.5 a) Écrire la configuration du serveur mandataire inversé (*reverse proxy*) « NGINX ModSecurity WAF » concernant l'accès aux serveurs *web* en arrière-plan (*backend*).		
Compétence évaluée : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure • Prévenir les attaques		
Excellente Maîtrise		La configuration proposée est correcte
Bonne Maîtrise		La partie concernant les certificats est bien maîtrisée mais une erreur est présente dans l'une des autres parties à modifier
Maîtrise partielle		Plusieurs erreurs apparaissent dans les différentes parties de la configuration proposée
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

a) Modification (en gras) de la configuration du WAF pour l'accès aux serveurs web en arrière-plan :

```
http {
  …
  upstream cluster.dmz.ccpg.fr {
…
    server web1.dmz.ccpg.fr :443 max_fails=3 fail_timeout=10s;
    server web2.dmz.ccpg.fr :443 max_fails=3 fail_timeout=10s;
    server web3.dmz.ccpg.fr :443 max_fails=3 fail_timeout=10s;
  }
  proxy_ssl_trusted_certificate /etc/ssl/certs/pki_local.crt;
  …
}
```

Question A2.5 b) Apporter les modifications nécessaires au fichier de configuration des serveurs *web* Apache.		
Compétence évaluée : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure		
Excellente Maîtrise		Les deux éléments à modifier sont justes
Bonne Maîtrise		
Maîtrise partielle		
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

b) Modification de la configuration des serveurs Web Apache

```
http {
…
        SSLCertificateFile "/etc/ssl/certs/cluster.crt"
        SSLCertificateKeyFile "/etc/ssl/private/cluster.key"
…
```

}

Question A2.6 a) Indiquer, dans les pistes d'évolution à moyen terme, quels éléments peuvent être encore considérés comme des points uniques de défaillance (*single points of failure*) dans cette nouvelle architecture.		
Compétence évaluée : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique		
Excellente Maîtrise		Au moins trois éléments ont été identifiés et la réponse a été justifiée
Bonne Maîtrise		Au moins deux éléments ont été identifiés et la réponse a été justifiée
Maîtrise partielle		Un seul élément a été identifié et justifié OU les justifications fournies ne sont pas convaincantes
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

1. Le reverse-proxy est considéré comme un SPOF puisqu'il est seul à prendre en charge les connexions des clients web depuis Internet.
2. Les pare-feux externes et internes semblent aussi ne pas bénéficier de haute-disponibilité. Si l'un de ces 2 équipements dysfonctionne ou tombe en panne, les services extranet seront forcément impactés.
3. Sur le schéma, le pare-feu externe ne semble disposer que d'une seule adresse IP publique et d'une seule connexion internet via un opérateur. Si un incident survient sur cette connexion, c'est l'accès à l'extranet qui est directement impacté.
4. Liens ou commutateurs dans les DMZ.
5. Un seul site géographique existe.

Question A2.6 b) Proposer, pour chaque élément, une solution afin d'améliorer la haute-disponibilité et éliminer ces points uniques de défaillance.		
Compétence évaluée : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique		
Excellente Maîtrise		Au moins trois solutions pertinentes proposées
Bonne Maîtrise		Au moins deux solutions pertinentes proposées
Maîtrise partielle		Une seule solution pertinente proposée
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

1. Mise en place d'un cluster au niveau du service reverse-proxy
2. Mise en place d'un cluster de pare-feux au niveau interne et externe.
3. Mise en place de deux connexions internet utilisant deux opérateurs distincts ne faisant pas appel aux mêmes infrastructures physiques (sous-répartiteur et répartiteur).

4. Redonder les liens et les commutateurs à l'aide de protocoles appropriés.

Mission B1 – Intégration d'un système d'authentification sur le réseau filaire

Question B1.1

Décrire, pour chacun des éléments impactés (client et serveur RADIUS), les différentes configurations à mettre en œuvre pour étendre l'infrastructure 802.1x au réseau filaire.

Compétence évaluée :

Sécuriser les équipements et les usages des utilisateurs

- Gérer les accès et les privilèges appropriés

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

- Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
- Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité

Excellente Maîtrise		L'ensemble des configurations sont proposées
Bonne Maîtrise		Configurations pertinentes mais incomplètes présentes sur le client et le serveur
Maîtrise partielle		Réponse peu pertinente ou très incomplète
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

Configuration du nouveau client RADIUS qui est le commutateur SW-03 :

- paramétrage général 802.1x avec un secret partagé distinct de celui utilisé sur la borne WiFi.
- déclaration du serveur RADIUS ;
- Paramétrage des quatre ports contrôlés 802.1x.

Configuration du serveur RADIUS pour déclarer le nouveau client Radius et les nouvelles stratégies de connexion et d'accès réseau.

Question B1.2

Proposer au chef de projet la ou les règles à ajouter à la table de filtrage pour permettre l'authentification Radius sur le réseau filaire.

Compétence évaluée :

Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

- Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
- Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité

Excellente Maîtrise		L'ensemble des règles sont présentes
Bonne Maîtrise		
Maîtrise partielle		Une seule règle s'avère pertinente
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

N° de règle	Adresse source	Port source	Adresse dest	Port dest	Action
...					
	192.168.70.3/32	*	192.168.10.40/32	UDP/1812	Autoriser
	192.168.70.3/32	*	192.168.10.40/32	UDP/1813	Autoriser
…					
Défaut	Toutes	Tous	Toutes	Tous	Refuser

Question B1.3

Lister deux éléments à prendre en compte vis à vis de l'utilisation du matériel personnel à inclure dans la charte.

Compétence évaluée :

Sécuriser les équipements et les usages des utilisateurs

- Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter

Excellente Maîtrise		Deux éléments pertinents et contextualisés sont cités
Bonne Maîtrise		Un élément pertinent et contextualisé est cité (avec éventuellement un autre élément non pertinent)
Maîtrise partielle		
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

- Définition du matériel personnel : clarification des types de matériel concernés (pc, smartphones, …), conditions d'admissibilité du matériel (âge, état, compatibilité, etc.).
- Sécurité : exigences en matière d'antivirus et de sécurité, responsabilité de l'utilisateur pour la mise à jour et la maintenance de son équipement, directives concernant le verrouillage et la sécurisation du matériel dans les locaux.
- Connexion au réseau : procédure d'accès au réseau, restrictions d'utilisation.

- *Gestion des données et confidentialité.*
- *Responsabilité légale.*

Mission B2 – Détermination des risques restants et évaluation de la solution Cisco ISE

Question B2.1 Identifier pour chacune des trois mesures, les technologies utilisées en justifiant les risques auxquels elles permettent de répondre. *Présenter la réponse sous forme de tableau.*		
Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Caractériser les risques liés à l'utilisation malveillante d'un service informatique		
Excellente Maîtrise		Technologies et risques clairement identifiés et justifiés pour chacune des mesures
Bonne Maîtrise		Il manque quelques éléments attendus
Maîtrise partielle		Il manque un grand nombre d'éléments
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

Les trois mesures identifiées dans le tableau ci-dessous sont mises en œuvre :

Mesures	Technologie mises en œuvre	Risques
Cloisonner les communications des appareils personnels dans un réseau dédié	Vlan et filtrage (pare-feu)	Risque d'atteinte à la confidentialité et à l'intégrité des données : par exemple, quand le télétravailleur s'authentifie via le WiFi, il reste cantonné dans le Vlan BYOD. Le filtrage inter-vlan contribue à restreindre les accès des utilisateurs aux seules données autorisées.
Mettre en place des mesures de chiffrement des flux d'informations	Protocole 802.1x (radius) avec l'authentification PEAP Serveur FTPS Serveur HTTPS	Risque d'atteinte à la confidentialité et à l'intégrité des données : le protocole PEAP permet également le chiffrement des communications lors de la phase d'authentification : les données qui circulent lors de cette phase sont particulièrement sensibles.
Contrôler l'accès au réseau par un dispositif d'authentification robuste de l'utilisateur	Infrastructure RADIUS : Protocole 802.1x, authentification PEAP, *habilitations*	Risque d'atteinte à la confidentialité et à l'intégrité des données : le protocole PEAP est un protocole fiable d'authentification des utilisateurs et il permet également l'authentification du serveur via un certificat. Le protocole PEAP permet également d'assurer l'intégrité des messages échangés lors de la phase d'authentification (phase sensible). Les habilitations contribuent à restreindre les accès des utilisateurs au réseau et aux seules données autorisées.

Question B2.2 Expliquer les apports de la solution *Cisco* ISE pour la CCPG, au regard des mesures préconisées et des risques identifiés.		
Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Caractériser les risques liés à l'utilisation malveillante d'un service informatique		
Excellente Maîtrise		Les apports sont correctement établis et justifiés
Bonne Maîtrise		Les apports sont correctement établis et insuffisamment justifiés
Maîtrise partielle		
Non maitrisée		Réponse non adaptée
Non évaluable		Non répondu

La mesure supplémentaire mise en œuvre par la solution proposée consiste à **exiger le respect de mesures de sécurité élémentaires** pour les terminaux qui se connectent au réseau.

La solution gère donc en plus le risque de compromission générale du système d'information en gérant les terminaux « malsains » (intrusion, virus, chevaux de Troie, etc.) : si, par exemple, le télétravailleur ne met pas son antivirus à jour, il ne pourra pas se connecter au réseau.

La solution proposée renforce également les dispositifs déjà en place pour lutter contre le **risque de confidentialité et d'intégrité des données** en :

- identifiant et classant automatiquement les éléments connectés pour les affecter à un VLAN bien défini : seuls les **équipements dûment autorisés** pourront se connecter, ainsi l'intégration des équipements personnels dépend aussi de l'équipement lui-même et n'est plus basé que sur l'authentification du télétravailleur ;
- contrôlant l'utilisation de certaines fonctionnalités : les équipements peuvent par exemple n'être autorisés qu'à utiliser les courriels et/ou l'accès internet : ceci vient en appui des VLAN et des règles d'habilitation mises en place.