BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

U7 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2025

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document n'est autorisé.

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

Le sujet comporte 19 pages, numérotées de 1/19 à 19/19.

Cas SA Blanca

Ce sujet comporte 19 pages dont un dossier documentaire de 13 pages.

Barème

DOSSIER A	**Gestion d'un incident sur le réseau local**	46 points
DOSSIER B	**Sécurisation de l'infrastructure Wi-Fi existante**	34 points
	TOTAL	80 points

Dossier documentaire

Présentation du contexte

La société mulhousienne BLANCA, dirigée par Samia BOGART, est spécialisée depuis 20 ans dans la formation de salariés d'entreprises du bassin industriel local sur le domaine de la gestion d'entreprise (contrats commerciaux, fiscalité, gestion administrative, etc.). Elle a étendu progressivement ses activités à l'usage de logiciels de bureautique, de gestion et de progiciels de gestion intégrés à travers ses partenariats avec les sociétés étasunienne Infor et française Divalto.

Pour développer son service global de formation, la société a investi récemment dans une plateforme applicative LMS (*learning management system*) en client/serveur pour gérer les apprentissages et le management de l'organisation. Cette application de gestion intégrée spécialisée est implémentée sur les serveurs de la zone démilitarisée (*DMZ - demilitarized zone)*.

Le secteur de la formation est très exposé et sensible aux attaques qui peuvent facilement conduire à des situations critiques. Cette situation s'est amplifiée depuis les périodes récentes de confinement et ont conduit les entreprises de formation à se réorienter vers un contact client plus distant.

BLANCA vise à devenir un acteur majeur de la formation pour les entreprises, ce qui exige une conformité stricte en matière de sécurité et de confidentialité pour ses activités et l'accueil de ses clients. Elle doit rester réactive face aux incidents et offrir différents modes de formation (présentiel, à distance ou mixte).

La gestion du réseau informatique est assurée par un seul technicien. Cependant, la croissance des activités et les évolutions du secteur ont incité madame BOGART à solliciter l'expertise de la société Impact Informatique, une équipe de sept personnes dirigée par Hervé HENTZLER, pour l'accompagner dans la gestion de son système d'information, notamment sur les aspects sécuritaires.

Vous avez rejoint récemment l'entreprise Impact Informatique, un prestataire reconnu dans l'est de la France qui inclut un département spécifique dédié à la sécurité et aux risques, dirigé par Maud IMBERT. Vous intégrez spécifiquement ce service.

Il y a peu, BLANCA a subi un blocage majeur affectant son réseau. Dans votre première mission, vous êtes chargé(e) de contribuer à la gestion de cette alerte informatique.

Par ailleurs, madame IMBERT a initié des actions visant à modifier l'infrastructure Wi-Fi de BLANCA, constituant ainsi le deuxième volet de votre mission.

Pour mener à bien vos missions, vous vous appuierez sur le dossier documentaire mis à votre disposition.

Dossier A – Gestion d'un incident sur le réseau local

Le réseau informatique de la société est victime d'un incident entraînant la dégradation progressive de l'ensemble des services. Vous êtes chargé(e) d'analyser le problème, d'y remédier en urgence puis d'en déterminer les causes et l'origine et enfin de définir un ensemble de procédures pour s'en prémunir.

Mission A1 – Analyse de l'incident et interventions immédiates

Depuis quelques heures, tous les utilisateurs constatent des lenteurs dans l'enregistrement des données, l'accès à internet, l'ouverture des sessions, etc. Tout le réseau semble devenir très lent. Le technicien informatique qui vous accompagne vous propose de vérifier l'état du matériel.

Les symptômes observés sur le réseau VLAN 10 sont les suivants :

1. Lenteur extrême généralisée de toutes les communications.
2. Les voyants des commutateurs sont dans les états suivants :
    - la LED du module d'extension est en orange clignotant ;
    - les LED des ports clignotent en orange très rapidement ;
    - les autres indicateurs LED sont allumés en vert sans clignotement.

Afin de caractériser le phénomène observé, madame JOUANDEAU, responsable en charge de l'audit, vous propose d'analyser la documentation généraliste et celle accompagnant le matériel concerné qu'elle vous transmet.

Question A1.1
Interpréter l'état des LED du commutateur D2 expliquant les raisons des lenteurs observées. *Justifier la réponse*.

Le micrologiciel *(firmware)* des commutateurs stocke la table d'adresses *MAC (media access control)* dans la mémoire RAM interne qui est limitée en taille.

Par ailleurs, une analyse de trames réalisée à partir de l'ordinateur ayant l'adresse IP 192.168.10.86 révèle que ce dernier reçoit des trames à destination de différentes adresses IP du réseau dont quelques-unes sont illustrées dans le dossier documentaire.

Le contenu de la table d'adresses MAC, l'extrait de la capture de trames et la documentation sur le fonctionnement des commutateurs pourraient éclairer sur la cause des lenteurs observées.

Question A1.2
a) Préciser quelles sont les trames qui ne devraient pas apparaître sur l'analyse de trame. *Justifier la réponse.*
b) Analyser le contenu de la table d'adresses MAC en fonction de la situation observée, en déduire et expliquer le mode de fonctionnement actuel du commutateur en défaut.
c) Expliquer l'impact sur les autres commutateurs et en déduire les conséquences sur le réseau VLAN 10.

L'adresse IP 192.168.10.243 est celle d'un serveur *NAS (network attached storage)* servant au partage réseau de fichiers contenant des données relatives à des clients et des utilisateurs.

Question A1.3
a) Expliquer en quoi la situation actuelle présente un risque au niveau du règlement général sur la protection des données (RGPD).
b) Proposer une évolution de l'architecture réseau existante qui permettrait de limiter le risque identifié vis à vis des serveurs. *Justifier la réponse.*

Il y a une heure votre responsable qualifiait la gravité de l'incident comme étant une priorité de type P2 élevée selon les recommandations de *l'ITIL (information technologies infrastructure library).* Cependant la situation ayant encore évolué, vous recevez maintenant de nombreux appels des utilisateurs de tous les services se plaignant de l'impossibilité d'utiliser le réseau informatique et du blocage de l'ensemble de l'activité de l'organisation.

Question A1.4
Analyser si le niveau de priorité de risque défini par le responsable est toujours d'actualité et proposer, le cas échéant, une nouvelle évaluation de ce dernier.

L'ensemble des commutateurs du cœur de réseau, de distribution et d'accès sont disposés dans une armoire disposant d'un interrupteur d'arrêt d'urgence.
L'infrastructure informatique est bloquée au point qu'il est maintenant impossible de vous connecter à l'interface de contrôle des commutateurs. À ce stade il est important de tenter une action d'urgence permettant de retrouver au moins provisoirement une situation normale.

Question A1.5
Proposer une action d'urgence et le point de blocage qu'elle permettrait de résoudre dans l'immédiat. *Justifier la réponse.*

Mission A2 – Recherche des causes de l'incident

Suite à votre intervention, la situation est redevenue normale. Il reste cependant à déterminer la cause de l'incident et trouver un moyen de le résoudre. Vous participez à une réunion d'analyse de la cascade des événements associés à l'incident afin d'en déterminer les causes. Au vu des observations, deux hypothèses sont avancées : la première concerne l'éventualité d'une attaque par usurpation ARP (*spoofing ARP*) et la seconde par inondation MAC (*MAC flooding*).

Question A2.1
Définir laquelle des deux hypothèses semble être la cause la plus plausible de cet incident. *Justifier la réponse.*

Afin de trouver quel est l'appareil responsable de l'attaque, il vous est demandé d'analyser les statistiques du nombre d'adresses *MAC* associées à chaque port dans les tables d'adresses MAC de tous les commutateurs dont un extrait est donné dans le dossier documentaire. Un éventuel problème provenant du protocole *Spanning-Tree* (STP) a déjà été écarté.

Question A2.2
Identifier, à partir de l'extrait du schéma du réseau et des statistiques sur les tables d'adresses *MAC*, l'appareil à l'origine de la défaillance. *Justifier la réponse.*

Vous avez identifié l'appareil responsable. Un examen de ce dernier révèle une défaillance logicielle du micrologiciel (*firmware)* qu'une mise à jour permettra de corriger. Néanmoins, cet incident ayant provoqué une immobilisation du réseau informatique, la possibilité d'une origine malveillante de ce dernier n'est pas à négliger et doit être prise en compte.

Question A2.3
Dans l'hypothèse d'un acte de cybermalveillance, caractériser le ou les types d'attaque en question.

Mission A3 – Mise en œuvre d'une remédiation

L'incident est résolu et sa cause est identifiée. Il est désormais essentiel de mettre en place un mécanisme permettant de détecter rapidement et de tracer tout équipement qui pourrait être utilisé intentionnellement par des attaquants pour reproduire cet incident, afin de l'isoler et de le neutraliser efficacement. Madame JOUANDEAU vous demande de produire un compte-rendu exposant la remédiation choisie et démontrant si cette dernière est opérationnelle. De plus, elle souhaite aussi être alertée automatiquement si la situation venait à se reproduire.

Question A3.1
a) Expliquer en quoi le mécanisme de sécurité des ports répond partiellement à la demande exprimée.
b) Préciser quel type de réaction des commutateurs à une violation de la sécurité des ports est le plus adapté. *Justifier la réponse.*

Pour répondre complètement aux attentes formulées par votre responsable, il est décidé de mettre en place une supervision permettant de générer une alerte spécifique si l'incident se reproduit à nouveau. Vous configurez les commutateurs (un extrait de la configuration est fourni dans le dossier documentaire) et vous mettez à jour la documentation dans laquelle vous devez justifier l'utilisation :

- d'un *trap* SNMP[1] ;
- de la version 3 de SNMP.

Question A3.2
a) Expliquer pourquoi l'utilisation d'un *trap* SNMP est plus pertinente dans ce contexte qu'une supervision active (requête SNMP classique).
b) Expliquer les principes techniques des deux paramètres de configuration de la version 3 du protocole SNMP permettant d'assurer sa sécurité.

Maintenant que le mécanisme proposé est correctement implémenté, il est nécessaire de s'assurer de son bon fonctionnement.
Vous récupérez une liste de commandes présente sur Kali Linux.

Question A3.3
Choisir la commande la plus pertinente à saisir sur votre système Kali Linux pour réaliser un test sur le commutateur en défaut. *Justifier la réponse.*

[1] Un *trap* SNMP est une notification non sollicitée envoyée par un agent SNMP d'un appareil géré par un serveur de supervision pour signaler un événement important.

Dossier B – Sécurisation de l'infrastructure Wi-Fi existante

Madame JOUANDEAU effectue une analyse structurelle de l'entreprise. Il ressort de cet audit que des incidents, liés à l'utilisation du réseau sans-fil interne, pourraient se produire. En effet, toute personne disposant de l'identifiant (SSID) et du mot de passe associé peut se connecter en Wi-Fi.

Madame JOUANDEAU préconise de mettre en place des technologies de contrôle des utilisateurs connectés selon les politiques d'accès aux services de l'organisation et à internet.

Actuellement, les employés permanents (administratifs, commerciaux, formateurs, etc.) ainsi que les apprenants bénéficiant d'une formation de longue durée accèdent au réseau interne et à internet, selon des autorisations spécifiques, à partir des terminaux filaires connectés aux ports contrôlés par le protocole 802.1x[2] qui permet à un utilisateur final, souhaitant accéder à un réseau, de s'authentifier grâce à un serveur central d'authentification. Ce serveur AAA[3] implémentant le protocole RADIUS mis en place est lié au serveur LDAPS dans lequel les utilisateurs sont centralisés.

La solution préconisée par madame JOUANDEAU se décline en deux points :

1. Pour l'accès au réseau Wi-Fi interne, les employés permanents et les apprenants bénéficiant d'une formation de longue durée seraient authentifiés en utilisant le protocole 802.1x (de la même façon que lorsqu'ils se connectent au réseau filaire).
2. Les apprenants inscrits à une formation ponctuelle de courte durée pourront bénéficier d'un accès Wi-Fi (réseau Wi-Fi Invité) à partir de leur propre machine ou d'un ordinateur emprunté au centre de formation BLANCA. Cet accès leur permettra uniquement d'accéder à internet. Pour cela, il est envisagé de mettre en place un portail captif qui leur permettrait de s'inscrire en toute liberté afin d'avoir un accès à internet.

Vous intégrez le groupe en charge de la formalisation et de la mise en œuvre de cette solution.

Mission B1 – Justification de la solution envisagée

Madame JOUANDEAU doit fournir un rapport détaillé à la directrice du centre de formation, qui doit justifier par écrit de la préconisation et de la solution choisie.

Elle vous demande dans un premier temps de justifier la nécessité de pallier les risques liés aux accès via le réseau Wi-Fi interne auxquels s'expose BLANCA dans la configuration initiale du réseau (document 1).

Question B1.1
Expliquer, en complétant avec des exemples, quels problèmes de sécurité pose l'architecture réseau actuelle, en précisant quels critères de sécurité (disponibilité, intégrité, confidentialité) ne seraient pas respectés.

Vous avez ensuite la charge de justifier la solution du portail captif pour les accès libres en utilisant la connexion internet de l'entreprise.

Question B1.2
Proposer deux arguments qui justifient l'installation du portail captif pour les apprenants ponctuels.

Le réseau Wi-Fi ouvert sera directement connecté au pare-feu interne et non au commutateur cœur de réseau.

Question B1.3
Justifier le choix de connexion directe au pare-feu interne.

[2] Le protocole 802.1X est une solution standard de sécurisation de réseaux qui permet de contrôler l'accès d'équipements informatiques à des réseaux locaux, qu'ils soient filaires ou Wi-Fi.

[3] Un serveur AAA (*authentication, authorization, accounting*) offre les services d'authentification, d'autorisation et de journalisation des évènements.

Mission B2 – Mise en place de la solution du portail captif

La solution du portail captif a été validée. Vous participez à sa mise en œuvre.

La configuration du portail captif sur le pare-feu interne permet à tout utilisateur de s'inscrire afin d'avoir un accès à internet.

Dans les conditions générales d'utilisation (*CGU)* du portail, BLANCA se propose d'utiliser les données saisies dans le formulaire d'inscription afin de pouvoir réaliser les traitements suivants :

Traitement A : créer les comptes d'accès à internet (comptes créés automatiquement par le portail captif).

Traitement B : constituer des fiches client pour contacter les utilisateurs dans une démarche commerciale.

Traitement C : établir des statistiques d'évaluation des formations en corrélation avec la liste des participants aux formations, fournie par les clients.

L'écran d'inscription est proposé dans le dossier documentaire.

Madame JOUANDEAU s'interroge au sujet de la présence, dans le formulaire, des données suivantes : téléphone professionnel et téléphone personnel, poste de travail, service dans l'entreprise, type d'emploi, et formation suivie.

Elle vous demande de construire un tableau qui indique, pour chacune de ces données à caractère personnel, l'évaluation de la pertinence de leur présence et le traitement associé effectué par l'organisation.

Question B2.1
Justifier la pertinence des données personnelles, qui interrogent Mme JOUANDEAU, par la réalisation d'un tableau à trois colonnes : la donnée, la justification de la pertinence dans le formulaire, le traitement effectué par l'organisation parmi les traitements prévus ci-dessus.

Madame JOUANDEAU vous demande d'activer le portail captif et de mettre en œuvre la politique de filtrage sur le pare-feu interne nécessaire pour que les clients connectés au réseau Wi-Fi Invité aient accès à internet via les protocoles HTTP et HTTPS. Le principe de fonctionnement de cette solution est décrit dans le dossier documentaire.

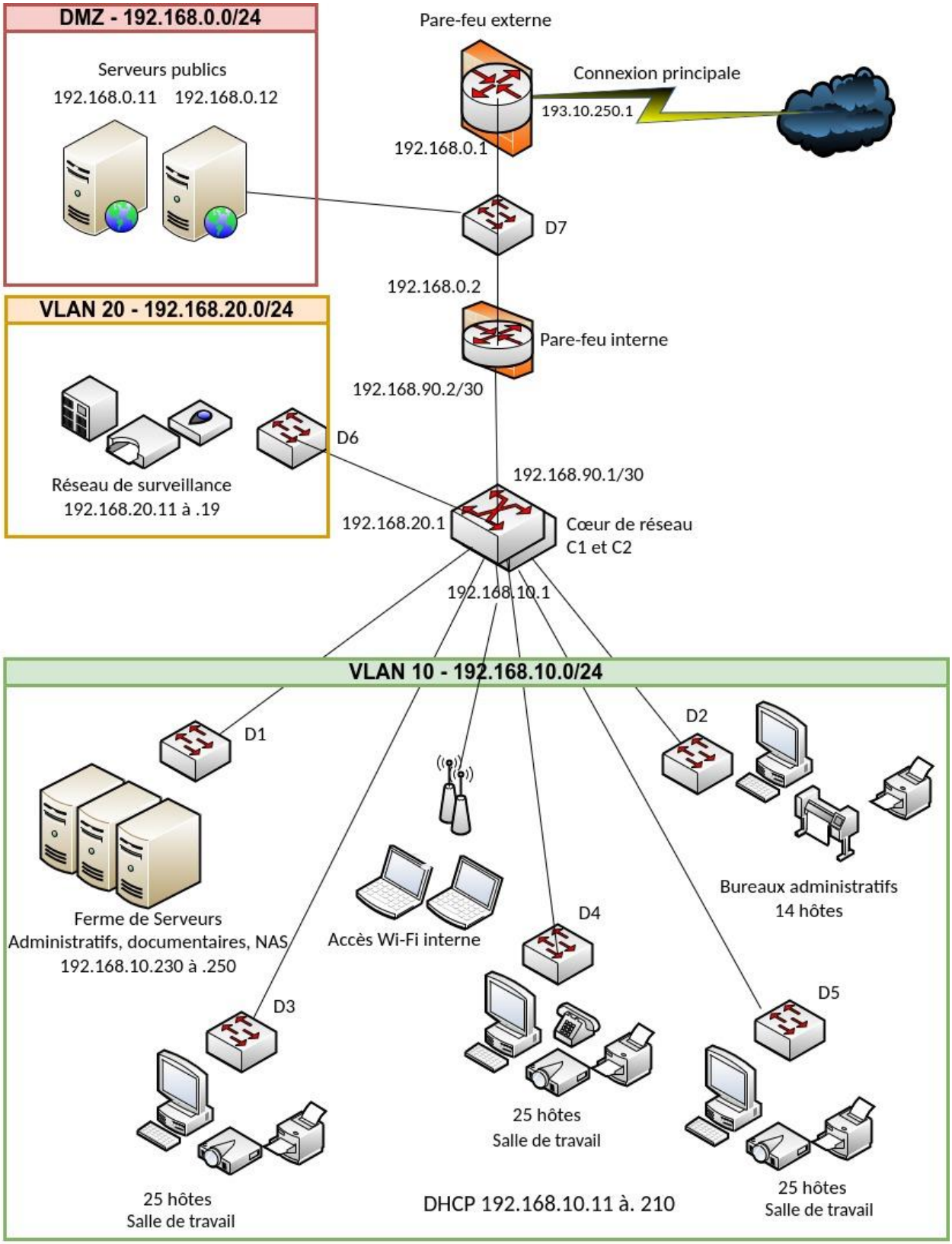
Bien que certaines règles soient automatiquement générées par le pare-feu lors de l'activation du portail, madame JOUANDEAU souhaite un rapport listant l'ensemble des règles mises en place sur le flux entrant de l'interface Wi-Fi du pare-feu interne, y compris celles créées implicitement, afin de vérifier leur conformité avec les exigences de sécurité.

Question B2.2
Écrire les règles de redirection afin que les utilisateurs connectés sur le réseau Wi-Fi Invité soient redirigés vers la page d'authentification du portail captif lorsqu'ils tentent d'accéder à des sites *web*.

Question B2.3
Écrire les règles de filtrage afin que les utilisateurs connectés sur le réseau Wi-Fi Invité puissent ou non accéder à internet selon qu'ils sont authentifiés ou non.

Documents associés au dossier commun

Document 1 : Plan du réseau



Document 2 : Description de l'infrastructure logique et physique

Le réseau du centre de formation dispose de trois réseaux logiques :

- Le réseau de production composé de :
  - serveurs virtualisés accueillant les applications métiers ainsi que les services système et réseau ;
  - serveur de sauvegarde et partage de fichier (NAS) ;
  - trois salles de travail composées chacune de 25 postes, d'une imprimante et de périphériques divers ;
  - cinq bureaux administratifs ;
  - deux bornes Wi-Fi couvrant les salles de travail et les bureaux administratifs.
- Le réseau de surveillance composé de serveurs virtualisés de supervision et métrologie.
- une zone démilitarisée (DMZ) constituée de l'ensemble des serveurs exposés sur internet (serveur *web* et serveur Moodle) permettant l'accès à distance d'un certain nombre de formation).

Le réseau physique est quant à lui articulé autour de :

- deux commutateurs de niveau 3 (C1 et C2) qui assurent le routage inter-VLAN ;
- sept commutateurs de niveau 2 (D1 à D7) ;
- deux pares-feux Stormshield SN 510 sur lesquels les fonctionnalités suivantes sont activées :
  - routage et filtrage de paquets (la politique de sécurité utilisée est celle du « tout interdit par défaut ») ;
  - filtrage applicatif ;
  - systèmes de détection d'intrusion / de prévention d'intrusion IDS/IPS ;
  - antivirus ;
  - réseau privé virtuel (VPN).

Adressage IP des principaux serveurs et des principaux services en écoute

N° VLAN	Nom VLAN IP Réseau	Adresses IP	Rôle serveur	Protocole
10	PRODUCTION 192.168.10.0/24	192.168.10.230	Annuaire centralisé (LDAPS)	TCP/636
			Serveur DNS	TCP/UDP/53
			Serveur DHCP	UDP/67
		192.168.10.231	Serveur administratif	TCP/1665
		192.168.10.232	Serveur Moodle interne	TCP/443
		192.168.10.243	NAS (Rsync over SSH) Serveur de fichier (SMBv2)	TCP/7654 TCP/445
20	SURVEILLANCE 192.168.20.0/24	192.168.20.11	Serveur supervision (interface) Traps SNMP	TCP/443 UDP/162
DMZ : 192.168.0.0/24			**Adresse IP des serveurs**	**Protocole**
Serveur *web*			192.168.0.11	TCP/443
Serveur Moodle public			192.168.0.12	TCP/443

Remarque : tous les serveurs et les éléments d'interconnexion sont administrables via le protocole SSH sur le port TCP/4567.

Salles de travail, réseau Wi-Fi, bureaux administratifs : plage d'adresses délivrée par le serveur DHCP de 192.168.10.11 à 192.168.10.210.

Documents associés au dossier A

Document A1 : Fonctionnement des commutateurs

Source : https://fr.wikipedia.org/ (texte adapté pour les besoins du sujet)

Le commutateur établit et met à jour une table. Dans le cas du commutateur pour un réseau Ethernet il s'agit de la table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port. Le commutateur construit donc dynamiquement une table qui associe numéro de port et adresses MAC.

Lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, le commutateur renvoie la trame sur le port correspondant. Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise. Si l'adresse du destinataire est inconnue dans la table, alors la trame est transmise à tous les ports du commutateur à l'exception du port auquel est relié l'émetteur.

À l'inverse d'un concentrateur, chaque port d'un commutateur de niveau 2 a son propre domaine de collision.

Problèmes de sécurité

Plusieurs techniques permettent de perturber le comportement d'un commutateur dans l'objectif de surveiller ou d'intercepter les communications réseau :

- **Usurpation ARP (ARP spoofing)** : trompe l'ordinateur ciblé de l'utilisateur en utilisant votre propre adresse MAC au lieu de celle de la passerelle de réseau ou en utilisant le mode d'émission *broadcast*.

- **Inondation d'adresses MAC (MAC flooding)** : surcharge le commutateur avec des milliers d'adresses MAC pour qu'il tombe dans un mode « échec d'ouverture » (*failopen).* Ce dernier se comporte alors comme un simple concentrateur et diffuse les trames à tous les postes appartenant au même VLAN. Ce problème a été détecté et corrigé dans la majorité des commutateurs récents. Pour les plus anciens, une mise à jour du micrologiciel (*firmware*) devrait permettre d'éviter ce comportement chaotique.

Une situation identique peut apparaître aussi suite à un dysfonctionnement d'une interface réseau ou d'une prise Ethernet générant des trames de façon aléatoire qui saturent les tables MAC des commutateurs. Un redémarrage de ces derniers permet de vider ces tables et de retrouver provisoirement un fonctionnement normal.

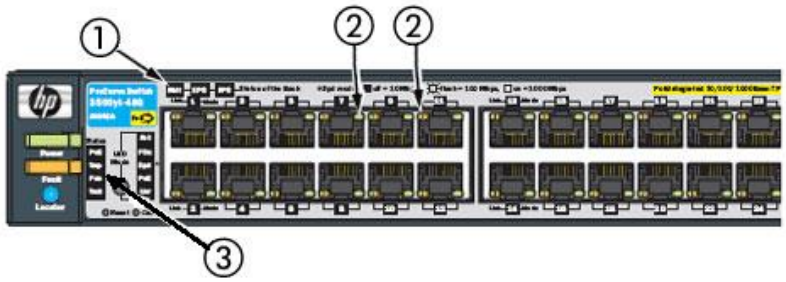
Document A2 : Extrait de l'affichage de la table MAC sur le commutateur en défaut

HP Switch # show mac-address

```
==================- CONSOLE – MANAGER Mode - ==========================
                      Status and counters – Address Table
NUM   VLAN        MAC Address       Located on Port
----  ----        -----------       ---------------
1     10          0030c1-7f4935     A2
..    ....        ...........       ..............
7997  10          0030c1-7f49c0     A3
7998  10          0030c1-7f4940     A1
7999  10          0030c1-7f49b5     A3
8000  10          0030c1-7f4932     A3
```

Total de 8000 lignes affichées sur une capacité de 8000 entrées dans la table.

Document A3 : Spécifications du commutateur HP 3500-48G-PoE yl



Source : HP

Légende	Indicateur LED
1	LED du module d'extension
2	LED d'état des ports (vert à droite, orange à gauche)
3	LED d'état du ventilateur et de la température

Indicateurs LED

Numéro de LED	LED du commutateur	Statut	Description
1	Démarrage (vert)	Allumée	Le commutateur est alimenté.
		Éteinte	Le commutateur n'est pas alimenté.
1	En défaut (orange)	Éteinte	Indique que le commutateur fonctionne normalement.
		Orange clignotant	Un dysfonctionnement s'est produit sur le commutateur : défaillance de l'un des ports, du module situé à l'arrière ou du ventilateur.
		Allumée	Allumée brièvement après la mise sous tension ou la réinitialisation du commutateur, au début de l'autotest. Si ce voyant reste allumé pendant une période prolongée, le commutateur a rencontré une panne matérielle fatale ou son autotest a échoué.
2	*LED de gauche* Collision (orange)	Éteinte	Aucune collision n'a été détectée.
		Orange clignotant	Des collisions ont été détectées : la fréquence de clignotement est proportionnelle à la fréquence des collisions.
2	*LED de droite* Port actif (vert)	Allumée	Port actif
		Éteinte	Port non actif
3	Température et ventilateur (vert/orange)	Allumée	La température ou le ventilateur du commutateur est normal.
		Orange clignotant	Une surchauffe a été détectée ou le ventilateur est défaillant

…

Spécifications électriques et avertissement

Les commutateurs peuvent être arrêtés par l'intermédiaire d'un interrupteur d'arrêt d'urgence en cas d'incident grave.

Document A4 : Extrait de l'analyse des trames effectuée avec un outil du type Wireshark

N°	IP source	IP destination	MAC source	MAC destination	Protocole
01	192.168.10.45	192.168.10.243	0030C1-7F49C0	00:1B:44:11:56:23	SMB
02	192.168.10.99	192.168.10.232	0030C1-AC47D4	00:1B:44:12:AA:C5	HTTPS
03	192.168.10.61	192.168.10.86	0030C1-6ADC68	00:1B:44:11:45:3A	SMB
04	192.168.10.20	192.168.10.243	0030C1-7F9AD5	00:1B:44:11:56:23	SMB

Remarque : Le protocole SMB dans sa version 2 (non chiffré) est utilisé dans le cadre de l'échange des données des fichiers partagés sur le réseau.

Document A5 : Échelle de gravité des risques informatiques selon Octopus (référence ITIL)

Source : Octopus.com, en référence aux recommandations d'ITIL (texte adapté pour les besoins du sujet)

Définition

L'impact : mesure de l'effet d'un incident sur l'organisation. L'impact peut être évalué selon :

- Le nombre d'utilisateurs affectés.
- Le nombre de services affectés.
- La réputation de l'entreprise.
- Les pertes financières potentielles.
- Les manquements aux règlements et aux lois.
- Autres critères.

L'urgence : mesure la vitesse à laquelle une entreprise doit apporter une solution à un problème ou une panne. Elle dépend de plusieurs facteurs, notamment :

- La période critique d'utilisation : certains systèmes sont essentiels à des moments spécifiques.
- Les systèmes critiques : certains systèmes jugés stratégiques pour l'entreprise en raison de leur rôle central dans l'activité sont souvent associés à des exigences élevées en termes de disponibilité.

La priorité : combinaison de l'impact et de l'urgence, servant à identifier le délai acceptable dans la mise en œuvre d'une action. L'allocation d'un code de priorité détermine comment l'incident est traité par l'outil et le personnel de soutien.

Matrice de dérivation de priorité

La matrice ci-dessous est un modèle pour vous inspirer dans l'établissement de votre propre matrice de dérivation de priorité. Son critère d'impact est basé sur le nombre d'utilisateurs et il est monté sur 3 niveaux d'impact et 2 niveaux d'urgence, menant ainsi à 4 niveaux de priorité. Les niveaux, ainsi que la terminologie de ce modèle peuvent être modifiés pour s'adapter à votre contexte.

		Impact		
		Élevé (Organisation en entier)	Moyen (Département, service ou > 5 utilisateurs)	Bas (1 à 5 utilisateurs)
Urgence	Urgent	P1 – Majeure	P2 – Élevée	P3 – Normale
	Normal	P2 – Élevée	P3 – Normale	P4 – Basse
	Faible	P3 – Normale	P4 – Basse	P4 – Basse

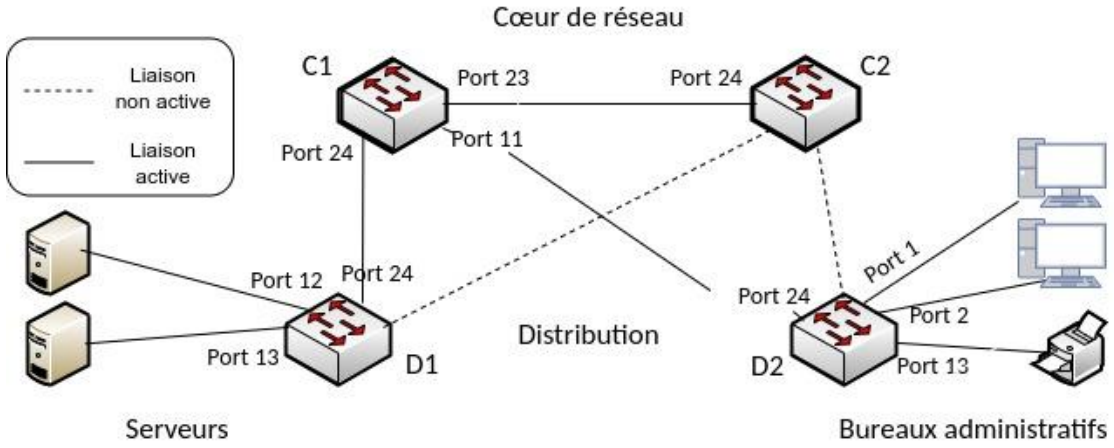
Définition des niveaux de service de base

Le tableau suivant représente un exemple de définition des niveaux de service de base pour les incidents, permettant aux organisations de concevoir leurs propres définitions, selon leur contexte organisationnel et leurs propres critères de priorité.

Elles servent de guide d'évaluation et de compréhension pour les intervenants techniciens lors de la classification de l'incident. À chaque priorité est alloué un délai de résolution cible ; l'objectif sera de résoudre les incidents à l'intérieur de ces cibles.

Priorité	Nom	Définition	Résolution
P1	Majeure	Interruption complète d'un service, application ou système, du réseau ou d'un élément de configuration identifié comme critique.	2 heures
P2	Élevée	Appliquée lorsque le service, l'application, le système, le réseau ou l'élément de configuration peut fonctionner mais avec une performance fortement réduite ou des fonctionnalités très limitées.	4 heures
P3	Normale	Événement qui provoque la perte minime d'un service. Une solution permanente ou de contournement est disponible pour restaurer la fonctionnalité du service.	1 jour
P4	Basse	Événement constituant un dérangement mais non bloquant pour l'utilisateur et pour lequel il existe une alternative ou un correctif.	2 jours

Document A6 : Extrait du schéma du réseau d'entreprise



Le cœur de réseau est composé des commutateurs C1 et C2. Les commutateurs de distribution D1 et D2 sont reliés de façon redondante aux deux commutateurs de cœur de réseau. Le protocole STP est activé.

Les numéros présents sur chaque lien spécifient les numéros de port du commutateur auquel est connecté le lien. Par exemple, le lien entre C1 et C2 est connecté au port n°23 de C1 et au port n°24 de C2.

Document A7 : Extrait des tables d'adresses MAC des commutateurs

Le tableau ci-dessous précise le nombre d'adresses MAC associées à certains ports actifs quelques temps après l'incident.

Commutateurs *distribution*	**N° de port**	**Nombre d'adresses MAC**	**Commutateurs** *cœur de réseau*	**N° de port**	**Nombre d'adresses MAC**
D1	12	1	C2	24	***601 ****
D1	13	1	C1	11	***601 ****
D1	24	***603 ****			
D2	2	1			
D2	13	***527 ****			

***(*)** Valeurs en augmentation rapide.*

Document A8 : Mécanisme de sécurité des ports sur les commutateurs

Le mécanisme de sécurité des ports consiste à enregistrer de façon statique ou dynamique une ou un nombre déterminé d'adresses MAC sources associées à un port.

La violation de la sécurité des ports est détectée lorsqu'une adresse MAC d'un périphérique connecté est différente de celle ou celles définie(s) précédemment.

Description de deux types de réaction en cas de violation de la sécurité des ports

- *shutdown* : Le port est désactivé, le compteur de violation est incrémenté et la violation est journalisée. Seul un administrateur peut réactiver le port concerné.
- *protect* : Le port supprime seulement le trafic émanant d'adresses MAC sources inconnues.

Comparaison de deux types de réaction en cas de violation de la sécurité des ports

Type de réaction	Rejet du trafic illégitime	Extinction du port	Incrémentation du compteur de violation	Journalisation de la violation
arrêter (*shutdown*)	Oui	Oui	Oui	Oui
protéger (*protect*)	Oui	Non	Non	Non

Document A9 : Configuration du service SNMP et d'un message trap SNMP sur un commutateur

```
HP-Switch(config)# snmpv3 enable
HP-Switch(config)# snmpv3 user <username> auth sha <password> priv aes <priv password>
HP-Switch(config)# snmp-server trap port-security
```

« auth sha <password> » : définit l'algorithme d'authentification et le mot de passe associés à l'utilisateur.
« priv aes <priv password> » : définit l'algorithme et le mot de passe du chiffrement.

Document A10 : Extrait des commandes disponibles sur Kali Linux

aircrack-ng : pirate des clés 802.11.

Arpspoof : envoie des réponses ARP falsifiées (« spoofées ») aux machines cibles pour empoisonner leur cache ARP.

Ettercap : analyse le réseau et réalise différents types d'attaque de l'homme du milieu.

Dhcpig : sature une étendue DHCP et empêche les nouveaux hôtes d'obtenir une configuration réseau.

Hydra : *cracke* une authentification identifiant (*login*) et mot de passe sur différents services réseaux.

Macchanger : modifie les adresses MAC des interfaces réseaux sur le système.

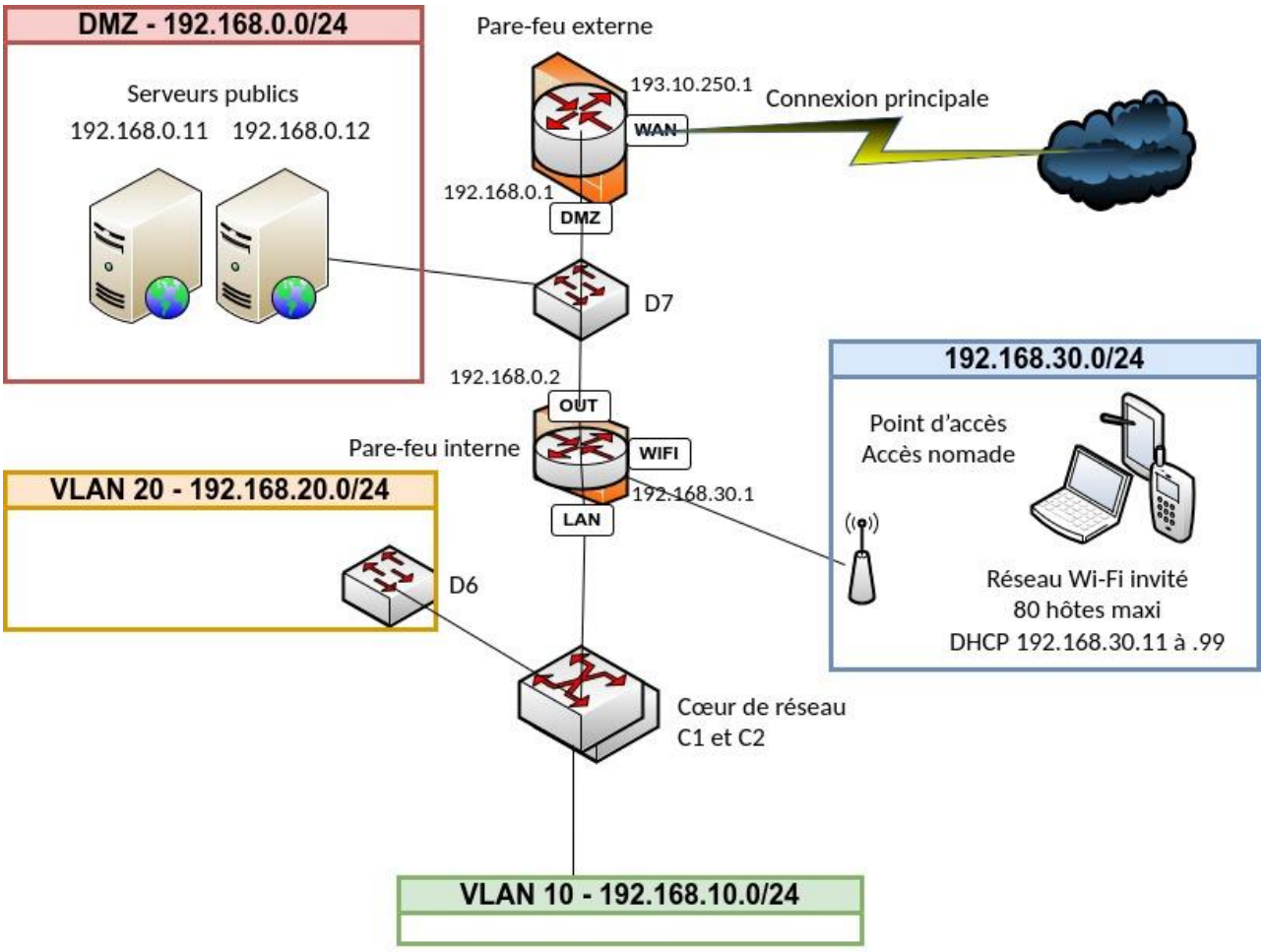
Macof : envoie des trames Ethernet avec des adresses MAC sources aléatoires.

Nmap : explore le réseau et réalise des *scans* de ports et de sécurité.

Tcpdump : récupère le trafic sur un réseau.

Documents associés au dossier B

Document B1 : Schéma réseau modifié



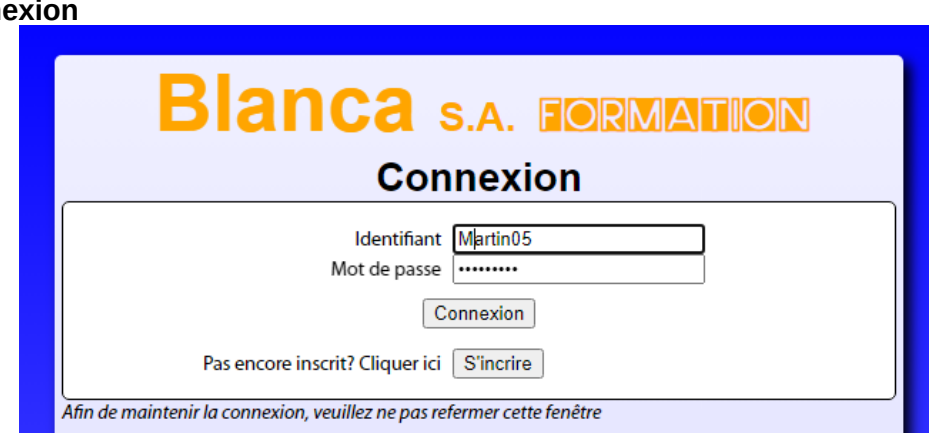
Le contenu du réseau VLAN 10 reste à l'identique du document 1, notamment l'accès au réseau Wi-Fi interne.

Le portail captif est configuré sur le pare-feu interne et sa page d'authentification est accessible via l'adresse IP 192.168.30.1.

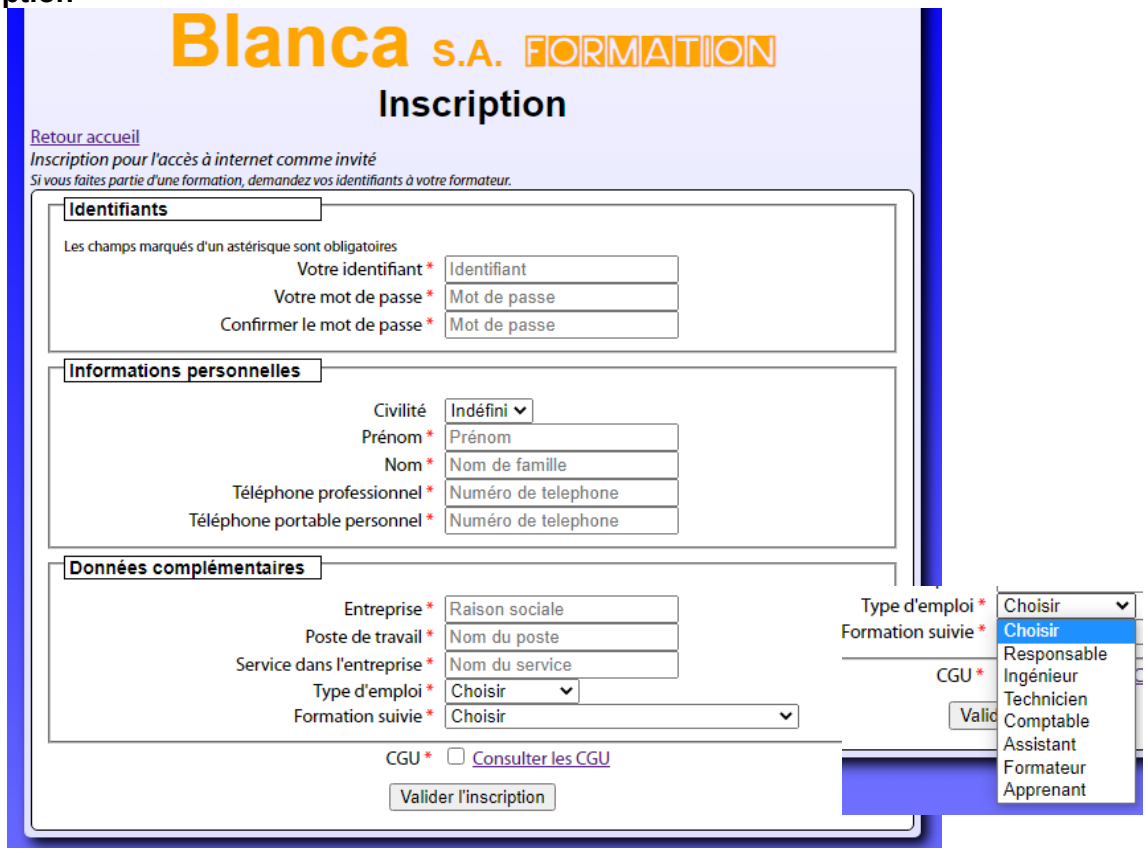
Le protocole de sécurité utilisé pour le Wi-Fi est WPA2 (*Wi-Fi Protected Access 2*).

Document B2 : Portail captif, écrans affichés

1) Connexion



2) Inscription

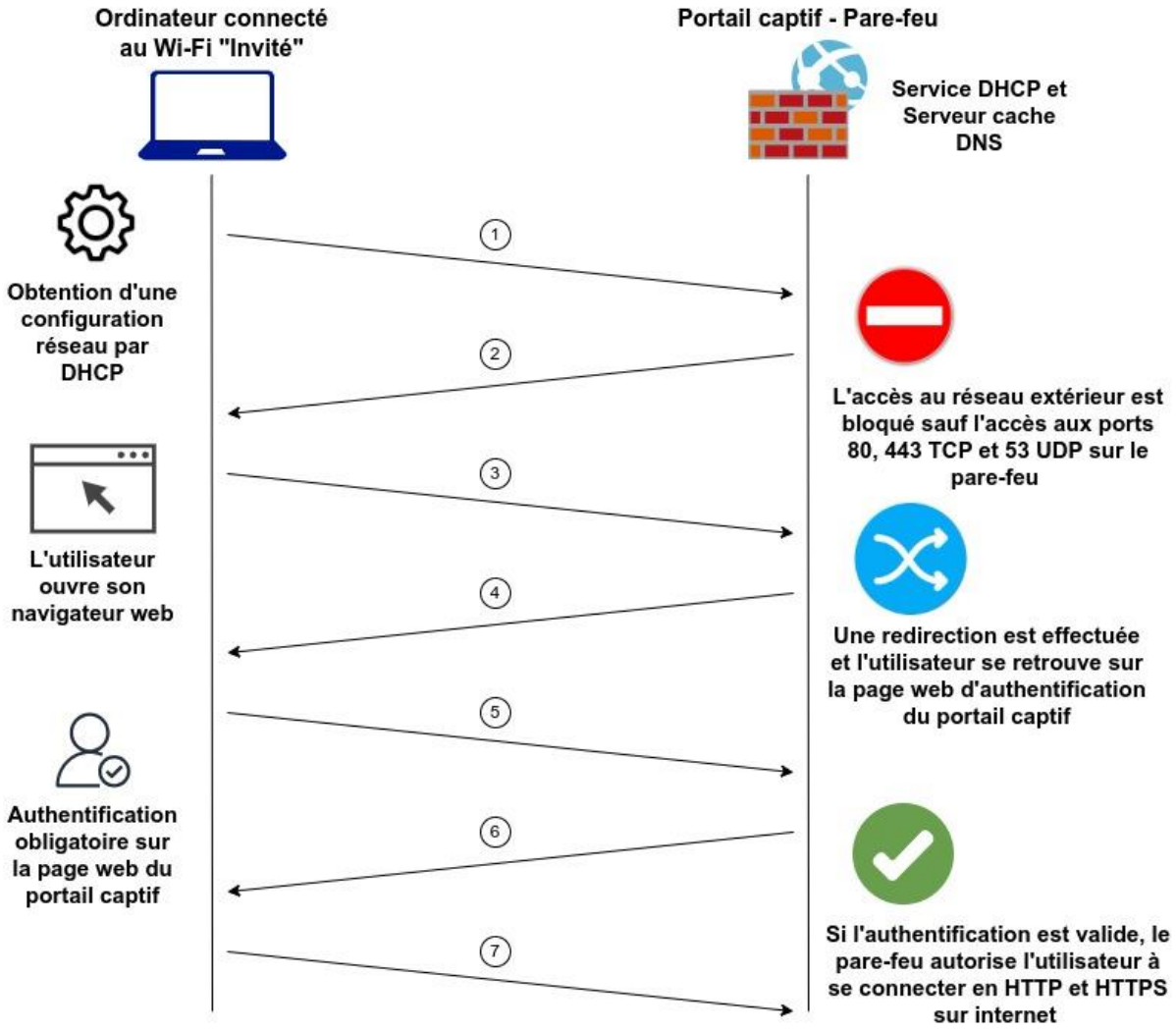


Exemples de postes : directeur, technicien, employé, responsable de production, analyste.

Le symbole * indique une saisie obligatoire.

3) Affichage après connexion

Document B3 : Principe du portail captif activé sur le pare-feu interne



Les apprenants ponctuels n'ont aucune légitimité à se connecter aux serveurs de BLANCA mais doivent pouvoir accéder, via le réseau Wi-Fi Invité, à internet.

Lorsque ces derniers se connecteront au point d'accès, le portail captif leur affectera dynamiquement une adresse IP qui ne leur fournira aucun accès au réseau de BLANCA mais leur permettra, à terme sous réserve d'authentification, d'accéder à internet où ils pourront utiliser les différents services web mis à leur disposition.

Lorsque l'apprenant lance son navigateur web et valide l'URL sollicitée (en HTTP ou HTTPS), le pare-feu bloque tout accès réseau, sauf les connexions à destination du pare-feu lui-même sur les ports TCP 80 et 443 ainsi que sur le port UDP/53 (le pare-feu étant relai DNS).

Le flux HTTP ou HTTPS est ensuite redirigé vers le portail captif qui forcera le navigateur de l'intervenant à afficher une page d'authentification avant d'accéder à internet. Cela est donc obtenu en bloquant tous les paquets liés à ces protocoles quelles que soient leurs destinations jusqu'à ce que l'utilisateur s'authentifie. Une fois ce dernier authentifié, les règles de pare-feu le concernant sont modifiées et celui-ci est autorisé à utiliser l'accès internet, sous contrôle du serveur mandataire (*proxy*), pour une durée fixée à 4 heures (témoin de connexion - *cookie* - défini dans le navigateur client). À la fin de cette durée, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session.

La connexion en HTTPS au pare-feu est sécurisée par les protocoles SSL/TLS. Le portail captif présente un certificat qui doit être approuvé par les utilisateurs finaux (l'autorité de certification qui émet le certificat doit être présente dans le magasin racine de confiance sur l'ordinateur client). À noter que le certificat utilisé par le portail captif activé sur le pare-feu interne émane d'une autorité de certification de confiance interne.

Document B4 : Extrait des règles établies sur les pares-feux

Extrait des règles de redirection sur le flux entrant de l'interface WAN du pare-feu externe

	IP source	Port source	IP destination	Port destination	IP translaté	Port translaté	Protocole
1	*	*	193.10.250.1	443	192.168.0.11/32	443	TCP
2	*	*	193.10.250.1	443	192.168.0.12/32	443	TCP

Le symbole « * » représente n'importe quelle adresse IP ou n'importe quel port.

Extrait des règles de filtrage sur le flux entrant de l'interface LAN du pare-feu interne

	Authenti-fication	IP source	Port source	IP destination	Port destination	Protocole	Action
1	NON	192.168.10.0/24	*	*	53	TCP/UDP	Autorisé
2	NON	192.168.20.0/24	*	*	53	TCP/UDP	Autorisé
3	NON	192.168.10.0/24	*	*	80	TCP	Autorisé
4	NON	192.168.20.0/24	*	*	80	TCP	Autorisé
5	NON	192.168.10.0/24	*	*	443	TCP	Autorisé
6	NON	192.168.20.0/24	*	*	443	TCP	Autorisé
...		...	...	...	...	...	...
20		*	*	*	*	*	Bloqué

La colonne « Authentification » indique si le flux entrant nécessite une authentification préalable pour être autorisé :

- « NON » : le flux est autorisé sans nécessiter d'authentification préalable.
- « OUI » : le flux nécessite une authentification préalable pour être autorisé.

À noter que, lorsqu'un paquet est intercepté par le pare-feu, celui-ci applique d'abord une règle de filtrage, suivie, si nécessaire, d'une règle de redirection.