

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

**U5 – PRODUCTION ET FOURNITURE DE
SERVICES INFORMATIQUES**

SESSION 2021

Durée : 4 heures
Coefficient : 5

Matériel autorisé :

Aucun matériel ni document est autorisé.

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

Le sujet comporte 17 pages, numérotées de 1/17 à 17/17
(sans compter la page de garde).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 0 sur 17

CAS LINS

Ce sujet comporte 17 pages dont 10 pages de documentation.

Il est constitué de deux parties qui peuvent être traitées de façon indépendante.

Dossier documentaire

Documents communs aux 2 dossiers

Document 1 : Schéma simplifié du réseau PRESBOIS.....	8
Document 2 : Description des réseaux et des systèmes de sûreté des données.....	9
Document 3 : Liste des réseaux locaux virtuels (VLAN) et adressage des serveurs.....	9
Document 4 : Liste de ports courants et de protocoles industriels	10
Document 5 : Extrait des règles de filtrage du pare-feu PF1.....	10

Documents associés au dossier A

Document A.1 : Exemple de configuration d'une interface réseau sous Linux	11
Document A.2 : Règles de redirection de port NAT	11
Document A.3 : Extrait du fichier de configuration du serveur <i>Web</i>	11
Document A.4 : Zone DNS	12
Document A.5 : Commandes NMAP	12
Document A.6 : Table de routage du commutateur de niveau 3 SW-Core.....	12
Document A.7 : Configuration de l'interface réseau du serveur SRV-sauv	13
Document A.8 : Extrait des règles de filtrage du commutateur SW-CORE	13
Document A.9 : Synchronisation de fichiers vers un serveur distant avec le logiciel Rsync	13
Document A.10 : Planification de tâches	14

Documents associés au dossier B

Document B.1 : Extraits de la documentation Microsoft à propos du protocole SMB	14
Document B.2 : Extrait du bulletin d'alerte du CERT-FR du 11 mars 2020	15
Document B.3 : Extrait des captures de trames.....	16
Document B.4 : Extraits de la base MIB (Management Information Base).....	17

Barème

DOSSIER A	Mise en production d'un site <i>Web</i> à destination des partenaires	50 points
DOSSIER B	Résolution de problèmes de sécurité et de performances	50 points
	TOTAL	100 points

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 1 sur 17

Présentation du contexte

PRESBOIS SAS (société par actions simplifiée), créée en 1998, est une entreprise dont l'activité consiste en la production de panneaux de particules, de panneaux MDF¹, et à l'offre de solutions pour constructions en ossature bois. Ses besoins en matières premières sont conséquents puisqu'un million de tonnes de bois sont nécessaires à sa production chaque année et en font la plus grosse usine de production de panneaux en fibres de bois en France.

Forte de ses 195 salariés, implantée sur un terrain de 30 hectares, cette entreprise industrielle, connaît depuis sa création une croissance solide et continue. En 2018, elle a vendu 550 000 m³ de panneaux et réalisé un chiffre d'affaires de 133 millions d'euros. Pour 2020, PRESBOIS prévoit des ventes à hauteur de 580 000 m³ pour un chiffre d'affaires estimé à 142 millions d'euros, dont environ 94 % à l'export. Les panneaux vendus en France sont destinés aux grandes surfaces de bricolage, à des clients industriels et à des négociants.

Soucieuse de la qualité de ses produits, l'entreprise l'est aussi quant à la performance et à la sécurité de son réseau informatique.

Le service informatique de PRESBOIS assure plusieurs fonctions parmi lesquelles :

- demande d'achats de logiciels et de matériels en fonction des besoins des utilisateurs ;
- entretien du câblage et des prises ;
- maintenance du matériel et des réseaux ;
- installation et configuration de postes en réseau ;
- mise à jour du parc informatique ;
- sauvegarde quotidienne des données sensibles ;
- aide aux utilisateurs.

L'entreprise PRESBOIS fait appel à l'ESN (entreprise de services du numérique) SARL LINS (*Legacy Industrial Networks Security*) pour l'aider dans la maintenance et l'évolution de son système d'information.

Vous travaillez depuis quelques mois par LINS, vous êtes affecté(e) à l'entreprise PRESBOIS en qualité de prestataire et vous avez pour mission d'assister Mme Volfoni, responsable des systèmes d'information de la société PRESBOIS dans les missions suivantes :

- installation d'un serveur *Web* dans la zone démilitarisée - DMZ publique (dossier A) ;
- résolution de divers problèmes de sécurité et de performances du réseau (dossier B).

¹ MDF est un sigle qui signifie : Medium Density Fibreboard, c'est-à-dire « panneau en fibres (de bois) de densité moyenne »

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 2 sur 17

Dossier A – Mise en production d'un site *Web* à destination des partenaires

La société PRESBOIS dispose d'un serveur *Web* interne hébergé au sein d'un serveur virtualisé dans le réseau local virtuel (Vlan) « serveurs internes ».

Afin de s'ouvrir à ses partenaires, elle a souhaité un nouveau site *Web* extranet dédié à l'accès de ses clients. Ce dernier a été développé en interne sur une machine virtuelle hébergée dans le réseau Vlan « serveurs internes ».

Vous avez la responsabilité de la mise en production de ce service et vous devez rédiger un rapport d'activité présentant vos configurations et justifiant vos choix.

Mission A1 – Transférer le serveur *Web* extranet vers la zone démilitarisée (DMZ)

Dans un premier temps, vous transférez la machine virtuelle accueillant le serveur *Web* dans la zone démilitarisée (DMZ).

Question A1.1

Expliquer le choix de cette localisation.

Vous vous connectez sur celle-ci via l'hyperviseur afin d'en finaliser les paramètres réseau.

Question A1.2

Écrire le fichier de configuration de l'interface réseau de la machine virtuelle SRV-Web-Extranet.

Vous testez l'accès local au site *Web* depuis un navigateur et vous constatez que le site est fonctionnel avec le protocole HTTP. Cependant, vous désirez que le site ne soit accessible qu'avec le protocole HTTPS.

Question A1.3

- a) Expliquer ce qui différencie les protocoles HTTPS et HTTP, en termes de protocole, d'échanges des données et de comportements des navigateurs.
- b) Donner les éléments à installer sur le serveur afin de permettre l'accès via le protocole HTTPS.
- c) Corriger l'extrait du fichier de configuration du serveur *Web*.

Les tests de connexion via le protocole HTTPS sont réussis aussi bien avec l'adresse de boucle locale qu'avec l'adresse IP locale.

Vous devez maintenant paramétrer l'accès extérieur vers le site *Web*. Vous vous connectez sur l'interface *Web* du pare-feu PF1.

Question A1.4

- a) Expliquer le mécanisme nécessaire permettant aux partenaires externes d'accéder au serveur *Web* de la DMZ.
- b) Proposer la configuration de ce mécanisme.

La configuration de ce mécanisme a été effectuée correctement.

Vous devez intervenir maintenant sur le fichier DNS afin que le site réponde aux requêtes envoyées à *www.presbois.fr*.

Question A1.5

Ajouter la ou les lignes au fichier de zone qui permettront d'accéder au site *Web* par l'adresse (URL) *www.presbois.fr*.

Vous vous positionnez à l'extérieur de la société PRESBOIS pour réaliser des tests.

Le test d'accès au serveur *Web* depuis l'extérieur échoue. Après avoir vérifié que le nom de domaine n'était pas en cause, vous utilisez l'outil NMAP afin de vérifier quels sont les ports ouverts.

Question A1.6

Écrire la commande *nmap* permettant d'effectuer un test de l'accès extérieur principal sur tous les ports TCP.

Ce test confirme que le service *Web* est inaccessible de l'extérieur de l'entreprise.

Après examen, vous constatez que les règles de filtrage du pare-feu PF1 ne sont pas appropriées.

Question A1.7

Rédiger la ou les règles qui autoriseront l'accès à ce service *Web*.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 4 sur 17

Mission A2 – Sauvegarder le site

Maintenant que le site est en ligne, votre mission consiste à assurer la sécurité de ses données. Il a été décidé, dans un premier temps, de réaliser deux sauvegardes journalières du site *Web* sur le serveur "SRV-sauv" du réseau Vlan « serveurs internes » à l'aide de la commande *Rsync*.

Vous vous connectez sur la machine virtuelle qui héberge le service *Web* et vous commencez par un test de connectivité à l'aide de la commande *ping* vers le serveur SRV-sauv. Le résultat est « Délai de la demande dépassé ». Cependant, il apparaît que la table de routage du pare-feu PF1 est correctement configurée.

Question A2.1

Proposer une configuration permettant les échanges entre le serveur *Web* et le serveur de sauvegarde.

La configuration a été correctement réalisée, mais malgré votre intervention, le serveur de sauvegarde reste toujours inaccessible. Vous analysez les listes de contrôle d'accès du commutateur SW-Core.

Question A2.2

Ajouter la ligne qui permettra la communication entre le serveur *Web* extranet et le serveur de sauvegarde uniquement pour le service concerné.

La communication entre le serveur *Web* et le serveur de sauvegarde fonctionne. Dans un premier temps, vous effectuez une copie des fichiers vers le serveur distant. L'identifiant utilisateur utilisé pour cette tâche est "it".

Question A2.3

Écrire la commande pour effectuer une première synchronisation des fichiers contenus dans le répertoire */var/www* du serveur *Web* vers le répertoire */var/sauv-w-ext* du serveur de sauvegarde.

La commande de synchronisation a été enregistrée dans un programme de type *script* *sauv.sh*, situé dans le répertoire */it/scripts*.

Question A2.4

Modifier le fichier *crontab* afin de permettre l'exécution de cette commande deux fois par jour.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 5 sur 17

Dossier B – Résolution de problèmes de sécurité et de performances

Mme Volfoni, responsable des systèmes d'information (RSI) de PRESBOIS, vous charge de certaines tâches.

Mission B1 – Gérer une vulnérabilité qui n'a pas encore de correctif

Mme Volfoni est nouvellement abonnée aux alertes du site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR). L'avis du 11 mars 2020 concernant notamment une vulnérabilité publiquement connue (CVE) a attiré son attention.

Cette vulnérabilité dans l'implémentation du protocole SMB par Microsoft décrit une faille de sécurité découverte dans un protocole utilisé dans le réseau bureautique et depuis l'extérieur de la société lorsque les commerciaux se connectent au serveur de fichiers de la DMZ à partir de leur poste de travail portable. Mme Volfoni vous charge de faire un état des lieux concernant ce risque. Vous devez préparer les éléments qui seront exposés lors d'une réunion avec Mme Volfoni.

Question B1.1

- a) Rédiger une courte note décrivant la manière dont cette faille pourrait être exploitée par un tiers malveillant.
- b) Décrire les conséquences techniques et économiques qui découleraient de l'exploitation de cette faille.

Suite à cette réunion, Mme Volfoni décide de prendre les mesures correctives proposées par Microsoft même si cela doit restreindre les fonctionnalités offertes à certains utilisateurs. Vous devez préparer les contre-mesures à mettre en place. Un extrait de la politique de filtrage du pare-feu PF1 est fourni dans le dossier documentaire.

Question B1.2

- a) Indiquer quelles mesures temporaires peuvent être rapidement mises en œuvre pour éviter l'exploitation de cette faille.
- b) Donner la ou les règles à ajouter sur le pare-feu situé en bordure du réseau pour empêcher l'exploitation de cette vulnérabilité.

Les règles ont été ajoutées au pare-feu mais les utilisateurs ayant besoin d'accéder au serveur de fichier depuis l'extérieur de l'entreprise se sont plaints à Mme Volfoni qu'ils ne pouvaient plus travailler correctement.

Question B1.3

Proposer une solution technique permettant à ces utilisateurs d'accéder au serveur de fichier avec un bon niveau de sécurité depuis l'extérieur, lorsqu'ils utilisent leur poste de travail portable fourni par l'entreprise.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 6 sur 17

Mission B2 – Analyser le trafic sur le réseau

Les opérateurs du service presse ont alerté Mme Volfoni de lenteurs qu'ils ont constatées dans le fonctionnement de certains ordinateurs de production reliés au réseau.

Pourtant, ceux-ci sont exclusivement dédiés à la production ; aucune tâche bureautique n'est effectuée à partir de ces ordinateurs et aucun autre matériel ne devrait être connecté à ce réseau.

Mme Volfoni vous charge de réaliser les investigations pour trouver la cause de ces problèmes et de rédiger un compte-rendu détaillé.

Celles-ci vous ont conduit à exclure des anomalies "système". Vous soupçonnez alors une surcharge de l'interface réseau de ces ordinateurs.

À partir d'un ordinateur portable, vous réalisez une capture de trames sur la partie « presse » du sous réseau de production.

Question B2.1

Écrire la procédure détaillant les différentes actions à entreprendre pour mener à bien cette capture. *Vous préciserez les matériels concernés, les éventuelles configurations à effectuer et les logiciels utilisés.*

La capture de trame a été réalisée et des extraits sont fournies dans le dossier documentaire.

Afin de trouver la cause du problème du service presse, vous vous intéressez principalement aux protocoles applicatifs.

Question B2.2

- a) Lister les protocoles applicatifs utilisés par certains ordinateurs du service presse.
 - b) Identifier les services trouvés qui ne devraient pas être détectés dans ce réseau.
- Justifier votre réponse.*

Certaines trames capturées à destination des ordinateurs du service presse concernent le service SNMP.

Question B2.3

- a) Expliquer le rôle de ce service et son utilité dans ce contexte.
- b) Expliquer en quoi des requêtes de l'identifiant OID 1.3.6.1.2.1.31.1.1.1.6 pourraient permettre de valider l'hypothèse d'une surcharge réseau sur l'interface des ordinateurs du service presse.

Mission B3 – Optimiser l'accès à internet

Le site de PRESBOIS bénéficie d'un lien vers l'extérieur par fibre optique depuis quelques mois. Du point de vue du directeur, monsieur Naudin, l'abonnement SDSL souscrit il y a des années auprès d'un second fournisseur d'accès à internet (FAI) n'est désormais plus pertinent. Il est en désaccord avec Mme Volfoni à ce propos et profite de votre intervention dans les locaux pour obtenir l'avis d'une tierce personne sur la question.

Actuellement, le lien SDSL n'est utilisé ponctuellement que pour le diagnostic et la mise à jour des automates de production.

Question B3.1

Proposer une utilisation pertinente du second lien afin d'améliorer les performances et la disponibilité de l'accès à internet. *Justifier votre réponse.*

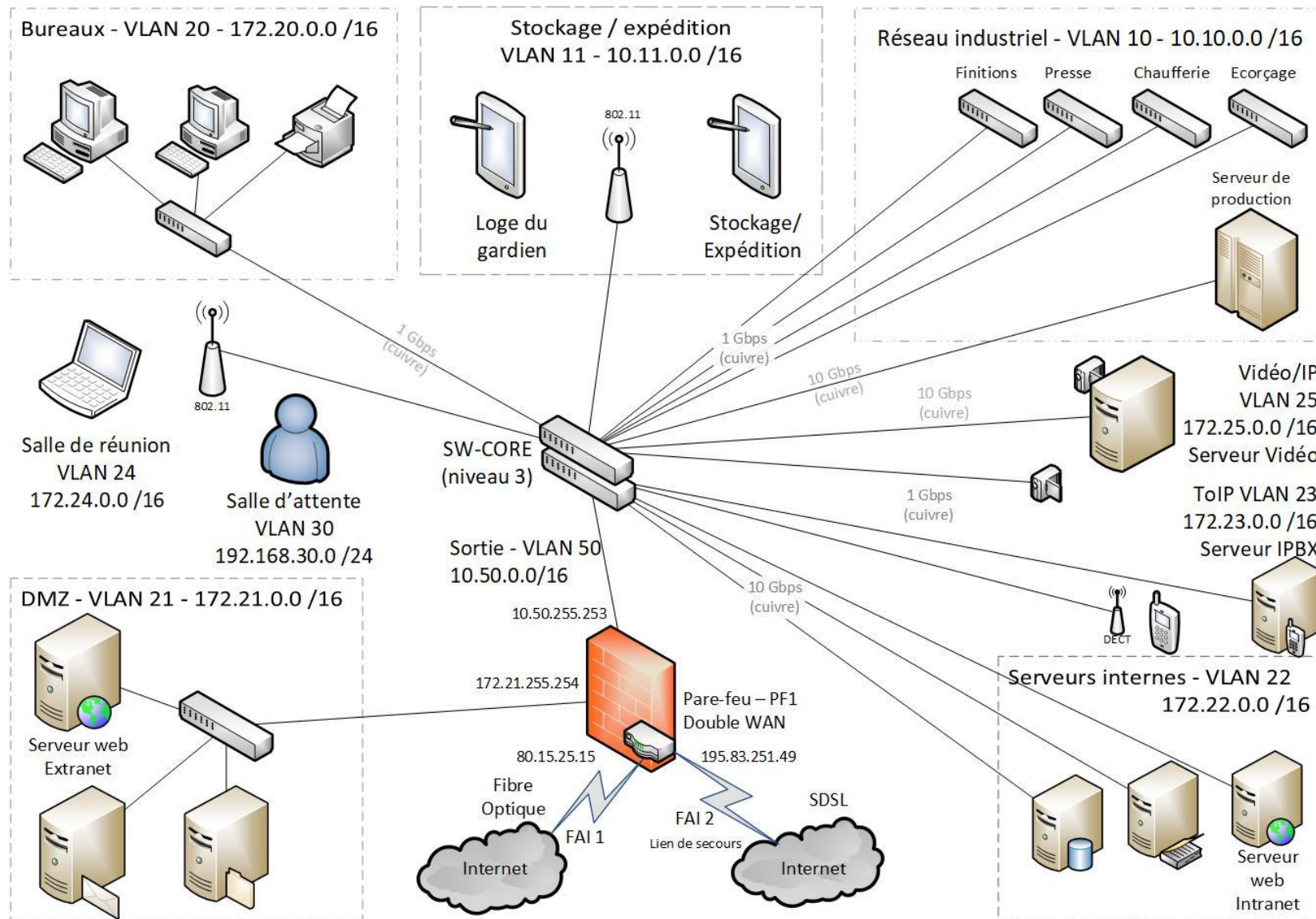
Question B3.2

Rédiger à destination de F. Naudin une liste d'au moins deux avantages liés au recours à ces deux fournisseurs d'accès, chacun utilisant des médias distincts pour permettre un accès à internet.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 7 sur 17

Documents communs aux 2 dossiers

Document 1 : Schéma simplifié du réseau PRESBOIS



Document 2 : Description des réseaux et des systèmes de sûreté des données

Le réseau informatique de l'entreprise PRESBOIS est basé sur la pile de protocoles TCP/IPv4. Il utilise la technologie Ethernet commuté à 1Gb/s pour la connexion des solutions techniques d'accès. Le cœur de réseau repose sur deux commutateurs de niveau 3 empilés avec des liaisons en 10 GbE (Gigabit Ethernet) pour la plupart des serveurs.

La salle des serveurs contient toutes les machines y compris celles de la zone démilitarisée (DMZ). Les accès y sont restreints par une porte d'accès munie d'un lecteur de badge et sas d'entrée avec gardiennage vidéo 24h/24.

Les serveurs locaux assurant les fonctions de base (DHCP, DNS, annuaire) et les fonctions de communication (intranet, messagerie, agenda partagé, etc.) ainsi que les applications métier et les fonctions plus génériques de toute entreprise (progiciel de gestion intégré avec ses modules ressources humaines, gestion de la relation client, etc.) fonctionnent sur deux serveurs dédiés à la virtualisation, exploités par la technologie Hyper-V et une solution de type SAN. Les serveurs de production, vidéo et de TOIP sont des serveurs physiques.

Chaque serveur physique est basé sur un RAID 1 SSD (*Solid State Drive*) pour les systèmes d'exploitation et un RAID 5 HDD (*Hard Disk Drive*) pour les données.

L'accès au réseau DMZ et à internet est réalisé au travers du pare-feu. Il existe deux accès internet, un principal très haut débit par fibre optique et un secondaire en technique SDSL dit de secours. Leurs noms DNS respectifs sont "ac1.presbois.fr" et "ac2.presbois.fr".

Le lien SDSL, en fonctionnement normal, est utilisé actuellement exclusivement pour la télémaintenance en réseau privé virtuel (VPN) des automates du réseau industriel.

Document 3 : Liste des réseaux locaux virtuels (VLAN) et adressage des serveurs

VLAN	Nom	Adresse réseau	Commentaires
10	Réseau industriel	10.10.0.0 /16	Regroupe les outils de production
11	Stockage / Expédition	10.11.0.0 /16	Contient les outils de gestion des stocks
20	Bureaux	172.20.0.0 /16	Concerne les outils dédiés à la bureautique
21	DMZ	172.21.0.0 /16	Serveur Hyper-v Machines virtuelles : <ul style="list-style-type: none">• 172.21.0.1 ac1 (DNS)• 172.21.0.20 server1 (Mail)• 172.21.0.30 server2 (Fichiers)• 172.21.0.10 SRV-Web-extranet
22	Serveurs internes	172.22.0.0 /16	Machines virtualisées LAN <ul style="list-style-type: none">• 172.22.0.10 SRV-Web-intranet• 172.22.0.100 SRV-Sauv
23	Téléphonie	172.23.0.0 /16	Système de VOIP
24	Salle de réunion	172.24.0.0 /16	Non commenté
25	Vidéo	172.25.0.0 /16	Système Vidéo/IP
30	Salle d'attente	192.168.30.0 / 24	Accès à l'internet uniquement
50	Sortie	10.50.0.0 /16	Réseau interne d'accès au pare-feu
100	Administration	10.100.0.0 /16	Réseau d'administration des équipements actifs

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 9 sur 17

Document 4 : Liste de ports courants et de protocoles industriels

N°	Protocole	Description
20	TCP	FTP - Data - File Transfer Protocol [flux de données]
21	TCP	FTP - File Transfer Protocol - commandes
22	TCP	SSH - Secure Shell
25	TCP	SMTP - Simple Mail Transfer Protocol RFC 5321
53	UDP/TCP	Domain - Domain Name Service (DNS)
69	UDP	TFTP - Trivial File Transfer
80	TCP	www - HTTP - World Wide Web HTTP
88	TCP	Kerberos
102	TCP	S7comm S7 Siemens PDC proprietary protocol
123	UDP	NTP - Network Time Protocol RFC 5905
139	UDP	NetBios Datagram Service
143	TCP	IMAP - Internet Message Access Protocol - RFC 3501
161	UDP	SNMP - Simple Network Management Protocol
443	TCP	HTTPS
445	TCP	Microsoft-DS SMB file sharing
502	TCP	Modbus/TCP PDC protocol (communication automates programmables)
873	TCP	Rsync
993	TCP	IMAP-SSL - IMAP4+SSL
3306	MYSQL	Structured Query Language Database Service
5060	UDP	SIP Session Initiation Protocol (ToIP)
*	RTP	Real-time Transport Protocol (ToIP)

Document 5 : Extrait des règles de filtrage du pare-feu PF1

Note : Si une règle autorise un paquet caractérisé par un quadruplet (IP source, port source, IP destination, port destination) à passer, la réponse caractérisée par le quadruplet inversé sera autorisée automatiquement.

N°	Interface entrée	Protocole	IP source	Port source	IP destination	Port destination	Action
...	
12	WAN	Tous	Toutes	Tous	172.21.0.30	Tous	Autorise
13	LAN	Tous	Toutes	Tous	Toutes	Web ⁽¹⁾	Autorise
...	
40	Toutes	Tous	Toutes	Tous	Toutes	Tous	Bloque

⁽¹⁾ : Le groupe de services « Web » regroupe les ports 53 (DNS), 80 (HTTP) et 443 (HTTPS).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 10 sur 17

Documents associés au dossier A

Document A.1 : Exemple de configuration d'une interface réseau sous Linux

Fichier /etc/network/interfaces

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
iface eth0 inet static
address 192.168.1.116
netmask 255.255.255.0
gateway 192.168.1.254
```

Document A.2 : Règles de redirection de port NAT

Protocole	Adresse source	Port source	Adresse destination	Port dest.	IP NAT	Ports NAT
UDP	*	*	80.15.25.15	139	172.21.0.30	139
TCP	*	*	80.15.25.15	445	172.21.0.30	445
TCP/UDP	*	*	80.15.25.15	53	172.21.0.1	53

Document A.3 : Extrait du fichier de configuration du serveur Web

```
ThreadsPerChild 250
MaxRequestsPerChild 0

Listen 80

ServerRoot "/www/Apache22"
DocumentRoot "/THDL/thdl-site"
## was /www/webroot

ServerName localhost:80
ServerAdmin admin@localhost

ErrorLog logs/error.log
LogLevel error
```

Document A.4 : Zone DNS

\$ORIGIN presbois.fr.

\$TTL 3h

```
@      IN SOA ac1.presbois.fr. it.presbois.fr. (
20200703328      ; Serial yyyymmddnn
3h      ; Refresh After 3 hours
1h      ; Retry Retry after 1 hour
1w      ; Expire after 1 week
1h)      ; Minimum negative caching of 1 hour
```

IN NS ac1.presbois.fr.

IN MX 10 server1.presbois.fr.

```
ac1      IN A    80.15.25.15
server1  IN A    80.15.25.15
server2  IN A    80.15.25.15
```

```
mail      IN CNAME server1
fichiers  IN CNAME server2
```

Document A.5 : Commande NMAP

La commande Nmap est un scanneur de ports. Elle peut être très utile pour vérifier qu'un service est ouvert sur un serveur ou pour retrouver une machine sur un réseau. Les cibles peuvent être désignées par leur adresse ou par leur nom DNS. Par défaut elle scanne les 1000 ports les plus utilisés.

Quelques exemples de commandes

```
nmap 192.168.1.1-254          nmap 192.168.1.0/24
```

Ces commandes scannent respectivement une plage d'adresses, un réseau entier

nmap -sP 192.168.1.* - Cette commande envoie une requête ICMP ECHO (Ping) à toutes les machines du sous-réseau 192.168.1.0/24.

nmap -sS 192.168.1.3 - Cette commande répertorie les ports TCP ouverts par l'envoi de messages SYN. Cela permet d'éviter que cette découverte soit loguée sur la machine cible.

nmap -sU 192.168.1.3- Cette commande répertorie les port UDP ouverts sur la machine cible.

On peut cumuler les options

```
nmap -sS -sU -A -v
```

Cette commande répertorie tous les ports TCP -sS et UDP -sU. L'option -A (agressif) tentera de déterminer les services, les versions et le système d'exploitation. La sortie verbeuse -v, permettra d'avoir tous les commentaires.

Document A.6 : Table de routage du commutateur de niveau 3 SW-Core

Réseau de destination	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	10.50.255.253	10.50.255.254
10.10.0.0	255.255.0.0	10.10.255.254	10.10.255.254
10.11.0.0	255.255.0.0	10.11.255.254	10.11.255.254
172.20.0.0	255.255.0.0	172.20.255.254	172.20.255.254
172.22.0.0	255.255.0.0	172.22.255.254	172.22.255.254
172.23.0.0	255.255.0.0	172.23.255.254	172.23.255.254
172.24.0.0	255.255.0.0	172.24.255.254	172.24.255.254
172.25.0.0	255.255.0.0	172.25.255.254	172.25.255.254
10.50.0.0	255.255.0.0	10.50.255.254	10.50.255.254
10.100.0.0	255.255.0.0	10.100.255.254	10.100.255.254
192.168.30.0	255.255.255.0	192.168.30.254	192.168.30.254

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 12 sur 17

Document A.7 : Configuration de l'interface réseau du serveur SRV-sauv

Fichier /etc/network/interfaces du serveur SRV-sauv

```
# The primary network interface
iface eth0 inet static
address 172.22.0.100
netmask 255.255.0.0
gateway 172.21.255.254
```

Document A.8 : Extrait des règles de filtrage du commutateur SW-CORE

Note : Si une règle autorise un paquet caractérisé par un quadruplet (IP source, port source, IP destination, port destination) à passer, la réponse caractérisée par le quadruplet inversé sera autorisée automatiquement.

N°	Protocole	IP source	Port source	IP destination	Port destination	Action
1	ICMP	Toutes	N/A	Toutes	N/A	Autorise
...
37	TCP	10.100.0.0/16	Tous	Toutes	Tous	Autorise
38	TCP	172.20.0.0/16	Tous	172.22.0.0/16	Tous	Autorise
...
100	Tous	Toutes	Tous	Toutes	Tous	Bloque

Document A.9 : Synchronisation de fichiers vers un serveur distant avec le logiciel Rsync

Rsync (pour remote synchronization ou synchronisation à distance), est un logiciel de synchronisation de fichiers. Il est fréquemment utilisé pour mettre en place des systèmes de sauvegarde distante ou des points de restauration du système.

```
rsync -az source/ login@serveur.org:/destination/
```

L'option -a de rsync indique l'utilisation du mode archive, -z est pour activer la compression.

L'option supplémentaire -v permet d'activer le mode verbeux qui affiche les détails de l'exécution.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 13 sur 17

Document A.10 : Planification de tâches

Crontab est un outil Linux qui permet de planifier des tâches.

Exemple de définition de tâches :

```
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user command to be executed
```

Exemples de tâches

Exécution d'une commande toutes les 6 heures :

```
00 */6 * * * /root/scripts/synchronisation-ftp.sh
```

Exécution d'une commande toutes les minutes uniquement le lundi :

```
* * * * 1 /root/script/commandes-du-lundi.sh
```

Exécution d'une commande une fois par an à une heure précise :

```
15 00 25 12 * /root/script/script-de-noel.sh
```

Documents associés au dossier B

Document B.1 : Extraits de la documentation Microsoft à propos du protocole SMB

SMB (*Server Message Block*) est un protocole de partage de fichiers et de tissu de données (*data fabric*). Ce protocole est utilisé par des milliards d'appareils dans une grande variété de systèmes d'exploitation, y compris Windows, MacOS, iOS, Linux et Android. Les clients utilisent ce protocole pour accéder aux données sur les serveurs. Cela permet le partage de fichiers, la gestion centralisée des données et permet aussi de réduire les besoins en capacité de stockage des appareils mobiles. Les serveurs utilisent également le protocole SMB dans les centres de données à définition logicielle, pour les charges de travail telles que le *clustering* et la réplication.

Étant donné que SMB est un système de fichiers distant, il nécessite une protection contre les attaques dans lesquelles un ordinateur Windows risque d'être piégé en entrant en contact avec un serveur malveillant exécuté sur un réseau fiable ou avec un serveur distant en dehors du périmètre du réseau. Les meilleures pratiques et configurations de pare-feu peuvent améliorer la sécurité, en empêchant le trafic malveillant de quitter l'ordinateur ou son réseau. Le blocage de la connectivité vers le trafic SMB peut entraîner le dysfonctionnement d'un grand nombre d'applications ou de services.

[...] Le matériel et les dispositifs des pare-feu de périmètre qui sont positionnés à la périphérie du réseau sont censés bloquer la communication non sollicitée (depuis internet) et le trafic sortant (vers internet).

Il est peu probable qu'une communication SMB depuis ou vers internet soit légitime. Le cas le plus courant est celui d'un serveur ou d'un service *cloud* tel qu'*Azure Files* requérant la création de restrictions basées sur l'adresse IP dans votre pare-feu de périmètre pour n'autoriser que ces points de terminaison spécifiques. Il convient également de n'autoriser que le trafic SMB 3.x et d'exiger le chiffrement SMB AES-128.

[...] Pour les clients et serveurs Windows qui n'hébergent pas de partages SMB, vous pouvez bloquer tout le trafic SMB entrant à l'aide du pare-feu *Windows Defender*, afin d'empêcher les connexions à distance provenant d'appareils malveillants ou compromis.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 14 sur 17

Document B.2 : Extrait du bulletin d'alerte du CERT-FR du 11 mars 2020

Objet : Vulnérabilité dans l'implémentation du protocole SMB par Microsoft

Risque : Exécution de code arbitraire à distance

Des codes d'exploitation ont été publiés publiquement pour la vulnérabilité CVE-2020-0796. Celle-ci affecte l'implémentation du protocole SMB par Microsoft et permet une exécution de code arbitraire à distance.

[...] Les solutions Microsoft reposent sur un grand nombre de services réseau dont un service de partage de ressources (fichiers, imprimantes, ...) dénommé SMB. Ce service est présent à la fois sur les postes de travail et sur les serveurs Windows.

[...] Microsoft a ajouté une extension au protocole SMB V3.1.1 permettant la compression des flux. Cette extension, activée par défaut, est implémentée depuis certaines versions de Windows.

[...] Le 10 mars 2020, l'éditeur a publié un avis concernant une vulnérabilité affectant la gestion de la compression dans son implémentation du protocole SMB. Cette vulnérabilité est de type débordement de tampon et permet à un attaquant de provoquer une exécution de code arbitraire à distance sans authentification.

La fonction vulnérable est utilisée à la fois par le client et le serveur qui partage des ressources (fichier, imprimante). Par conséquent, une personne malveillante pourrait exploiter cette vulnérabilité pour compromettre un serveur de ressources SMB, puis, par rebond, toutes les machines qui se connecteraient à ce serveur : la compromission en chaîne de machines vulnérables est donc possible.

Des informations sur cette vulnérabilité ont été divulguées par des chercheurs alors que Microsoft n'a pas publié de correctif.

Le CERT-FR estime que des codes d'exploitation sont susceptibles d'être publiés rapidement.

[...] Dans l'attente d'un correctif de l'éditeur, le CERT-FR demande que le contournement publié par l'éditeur soit immédiatement appliqué.

Il est important de souligner que ce contournement protège le service 'serveur' SMB et ne nécessite pas de redémarrage. En revanche, les clients SMB restent vulnérables.

Le CERT-FR rappelle que les règles de bonnes pratiques de sécurisation des environnements Microsoft doivent être scrupuleusement respectées :

- Interdire tout flux SMB sur les ports TCP/139 et TCP/445 en entrée et en sortie du Système d'Information ;
- Pour le cloisonnement interne : n'autoriser les flux SMB que lorsque cela est nécessaire (contrôleurs de domaine, serveurs de fichiers, etc.) et bloquer ce flux entre postes de travail ;
- Pour les postes nomades : interdire tous les flux SMB entrants et sortants et n'autoriser ces flux vers des serveurs SMB qu'au travers d'un VPN sécurisé.

Ces mesures sont de portée générale et doivent être appliquées systématiquement au sein d'un système d'Information.

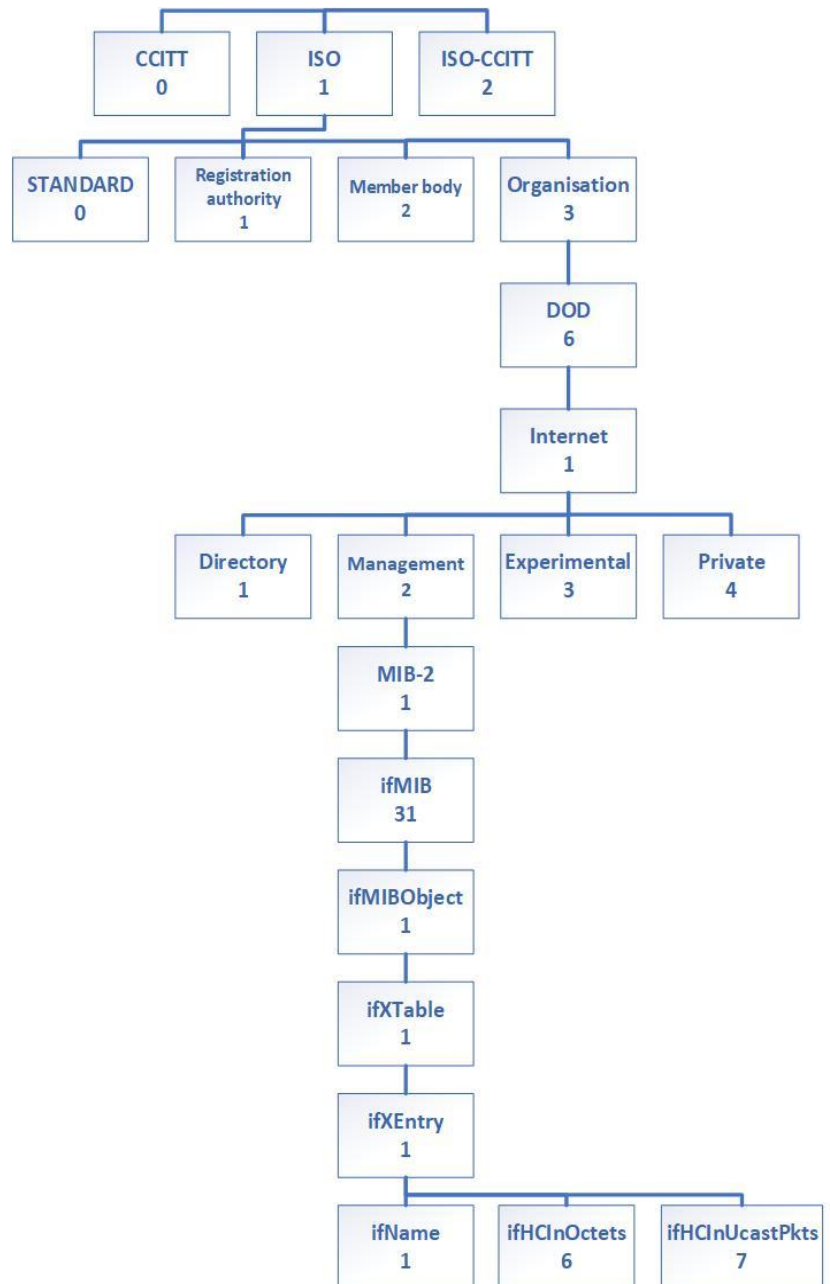
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 15 sur 17

Document B.3 : Extrait des captures de trames

No.	Time	Source	Destination	Protocol	
198	30.601995	10.10.2.46	172.22.0.2	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
199	30.602250	172.22.0.2	10.10.2.46	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
200	30.602882	10.10.2.46	172.22.0.2	SMB2	Session Setup Request, NTLMSSP_AUTH, User: .administrateur
201	30.603453	172.22.0.2	10.10.2.46	SMB2	Session Setup Response
211	30.606350	172.22.0.2	10.10.2.46	SMB2	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
212	30.606623	10.10.2.46	172.22.0.2	TCP	8564 → 445 [ACK] Seq=1977 Ack=3925 Win=2102272 Len=0
...					
485	82.086289	172.23.33.4	172.23.33.11	SIP	Request: REGISTER sip:172.23.33.11 (1 binding)
489	82.092874	172.23.33.4	172.23.33.11	SIP	Request: REGISTER sip:172.23.33.11 (1 binding)
527	123.149709	172.23. 33.4	172.23.33.11	SIP/SDP	Request: INVITE sip:801@172.23.33.11;user=phone
...					
4570	1471.175211	Inventec_a0:98:e5	Broadcast	ARP	Who has 10.10.1.1? Tell 10.10.1.100
4571	1471.861769	Cisco-Li_74:6e:94	Spanning-tree-(for-bridges)_00	STP	RST. Root = 16384/0/00:18:fe:e4:3e:40 Cost = 20000 Port = 0x8008
4572	1472.103934	HewlettP_87:83:09	Broadcast	ARP	Who has 10.10.80.36? Tell 10.10.14.223
4585	1475.732267	Micro-St_5e:99:0f	HewlettP_dc:eb:7a	ARP	10.10.177.178 is at 00:10:dc:5e:99:0f
4529	1487.856664	Cisco-Li_74:6e:94	Spanning-tree-(for-bridges)_00	STP	RST. Root = 16384/0/00:18:fe:e4:3e:40 Cost = 20000 Port = 0x8008
4537	1489.855129	Cisco-Li_74:6e:94	Spanning-tree-(for-bridges)_00	STP	RST. Root = 16384/0/00:18:fe:e4:3e:40 Cost = 20000 Port = 0x8008
...					
4591	1499.439948	10.10.224.178	10.10.12.2	SNMP	get-next-request 1.3.6.1.2.1.31.1.1.1.6
4592	1499.441215	10.10.12.2	10.10.224.178	SNMP	get-response 1.3.6.1.2.1.31.1.1.1.6
4596	1499.960108	10.10.224.178	10.10.12.2	SNMP	get-next-request 1.3.6.1.2.1.31.1.1.1.6
4597	1499.961036	10.10.12.2	10.10.224.178	SNMP	get-response 1.3.6.1.2.1.31.1.1.1.6
...					
6169	1887.170370	10.10.2.166	10.10.88.60	Modbus/TCP	Query: Trans: 170; Unit: 1, Func: 1: Read Coils
6170	1887.170477	10.10.10.20	10.10.10.10	S7COMM	ROSCTR:[Job] Function:[Read Var]
6179	1887.180406	10.10.2.166	10.10.88.60	Modbus/TCP	Query: Trans: 170; Unit: 1, Func: 1: Read Coils
6180	1887.183558	10.10.10.10	10.10.10.20	S7COMM	ROSCTR:[Ack_Data] Function:[Read Var]

Document B.4 : Extraits de la base MIB (Management Information Base)

Une base MIB (*Management Information Base*, base d'information pour la gestion du réseau) est un ensemble d'informations structuré sur une entité réseau, par exemple un routeur, un commutateur ou un serveur. Ces informations peuvent être récupérées, ou parfois modifiées, par un protocole comme SNMP.



ifName : Nom de l'interface réseau

ifHCInOctets : Nombre total d'octets reçus sur l'interface réseau

ifHCInUcastPkts : Nombre de paquets reçus en Unicast sur l'interface réseau

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2021
U5 – Production et fourniture de services informatiques	Durée : 4 heures
Code sujet : SI5SISR	Page 17 sur 17