

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

**U6 – CYBERSÉCURITÉ DES SERVICES  
INFORMATIQUES**

SESSION 2023

---

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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 1 sur 19

# Cas SAINT-JACQUES

Ce sujet comporte 19 pages dont un dossier documentaire de 10 pages.

## Barème

DOSSIER A	Audit général de la sécurité du réseau	44 points
DOSSIER B	Amélioration de la sécurité du réseau	36 points
	TOTAL	80 points

## Dossier documentaire

<b>Documents communs .....</b>	<b>10</b>
Document 1 : Organisation générale des services de la mairie .....	10
Document 2 : Durées de conservation et archives .....	10
Document 3 : Applications mises à disposition via le réseau informatique .....	11
Document 4 : Matériel utilisateur de chaque service .....	12
Document 5 : Description des liaisons.....	12
Document 6 : Schéma de positionnement matériel .....	13
Document 7 : Stockage des données et applications du système d'information .....	14
<b>Documents associés au dossier A.....</b>	<b>15</b>
Document A1 : La continuité d'activité en cas de sinistre.....	15
Document A2 : Haute disponibilité des pare-feux.....	15
<b>Documents associés au dossier B.....</b>	<b>16</b>
Document B1 : Concepts et généralités des réseaux privés virtuels de type VPN IPSec.....	16
Document B2 : Certificats et infrastructure de gestion de clés (PKI).....	17
Document B3 : Protocole IPSec et authentification des correspondants .....	17
Document B4 : Tunnel VPN IPSec nomade (pare-feu UTM SNS Stormshield mairie) .....	18
Document B5 : Règles de filtrage du pare-feu UTM SNS Stormshield de la mairie (FW-SEC) ..	19

## Présentation du contexte

Saint-Jacques-sur-Argens<sup>1</sup> est une commune française située dans le département du Var, en région Provence-Alpes-Côte d'Azur. Sa population a connu une croissance forte sur les 50 dernières années jusqu'à atteindre 10 000 habitants cette année. De nombreuses entreprises, grandes enseignes de distribution et industries sont installées au sud du territoire communal.

Afin d'assurer ses missions, la mairie est organisée en services communaux :

- les services principaux réalisant les missions essentielles de toute mairie (état civil, élections, cadastre, urbanisme, marchés publics) ;
- les services aux administrés destinés à satisfaire les demandes des habitants, des associations et des entreprises de la commune (affaires scolaires, culture, sport, médiathèque, police municipale, etc.) ;
- les services de support qui facilitent le travail des deux catégories de services précédentes (accueil, secrétariat, communication, ressources humaines, affaires juridiques, centre technique, archives, etc. et bien sûr le service informatique).

Les missions du maire sont de deux ordres :

- Il représente la commune auprès des tiers. Il est notamment chargé :
  - d'exécuter les délibérations du conseil municipal,
  - d'assurer sa fonction d'administration municipale,
  - d'exercer les pouvoirs de police dans sa commune.
- Il est aussi agent de l'État et doit garantir ses missions liées :
  - aux actes d'état civil (naissances, unions, décès, etc.),
  - aux élections (tenue des listes électorales, organisation des élections, etc.),
  - au recensement citoyen,
  - aux activités judiciaires (sous l'autorité du procureur de la République),
  - à la sécurité civile.

Concernant ce dernier point, la commune doit respecter des contraintes spécifiques en matière de sécurité.

En effet, la commune de Saint-Jacques-sur-Argens accueille sur son territoire des sites sensibles classés Seveso 2<sup>2</sup> :

- un dépôt de carburant et un terminal pétrolier présentant des risques de rejets de boues chargées d'hydrocarbures, d'explosion et d'émanation de gaz toxiques ;
- une entreprise industrielle présentant des risques de rejets d'hydrocarbures, de fluor et de boue hydroxyde.

De plus, comme de nombreuses autres communes du département, Saint-Jacques-sur-Argens est bordé par un fleuve côtier qui déborde régulièrement lors d'épisodes méditerranéens et a donc subi des inondations particulièrement importantes par le passé.

Dans ce contexte, le maire doit s'assurer de la disponibilité des services municipaux jugés comme critiques lors d'une éventuelle crise.

Le service informatique agit non seulement selon le cadre réglementaire numérique des mairies, mais doit aussi tenir compte des spécificités sécuritaires énoncées précédemment. Il doit notamment garantir la continuité des services critiques lors d'une éventuelle attaque informatique ou d'un incident majeur.

Vous venez d'être recruté(e) au sein du service informatique en tant que responsable-adjoint(e) sécurité des systèmes d'information. M. Hopada, le directeur du service informatique, vous a confié l'étude et la réalisation de certaines missions liées à la sécurité du réseau de la mairie.

**Vous vous appuyerez sur le dossier documentaire mis à votre disposition.**

<sup>1</sup>Pour des raisons de confidentialité, le nom de la commune et les données s'y référant ont été modifiées.

<sup>2</sup>Seveso 2 : directive concernant les risques d'accidents majeurs

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 3 sur 19

### **Mission A1 – Vérification des accès au réseau**

Cette première mission consiste à vérifier la sécurité des différents points d'accès du réseau de la mairie.

La mairie dispose d'un certain nombre de services répondant aux besoins de la population (les « administrés »), des entreprises et des associations de la commune.

Il convient de distinguer deux usages des applications :

- d'une part, les applications métier permettant au personnel de la mairie de réaliser leurs différentes missions. Ces applications ne sont accessibles qu'aux personnes habilitées, jamais au public ;
- d'autre part, les applications destinées au public. Elles permettent la consultation, la formulation de demande ou le paiement de certains actes. Elles sont accessibles via le portail internet de la mairie de Saint-Jacques-sur-Argens ou via les postes mis à disposition du public au sein des locaux communaux.

M. Hopada s'interroge sur la sécurité des accès aux ressources informatiques par le public.

#### **Question A1.1**

Identifier les différentes façons (emplacements, équipements) par lesquelles le public peut accéder aux applications qui lui sont dédiées.

Les personnels de la mairie sont considérés comme des utilisateurs loyaux et fiables, ils n'accèdent qu'aux applications et ressources qui leur sont nécessaires pour effectuer leur travail. M. Hopada s'interroge sur la possibilité d'accès malveillant aux données de la mairie par des personnes externes à l'organisation.

#### **Question A1.2**

Indiquer au moins trois cas de figure permettant l'accès d'une personne malveillante aux postes de travail ou aux comptes personnels des personnels de la mairie.

L'un des membres du personnel de la médiathèque a récemment ouvert un ticket d'incident contenant les informations suivantes :

- un poste de la médiathèque (destiné au public) semble au premier abord fonctionnel, mais ne permet plus d'accéder à l'application de recherche documentaire ;
- des feuilles portant le message « Hacké par K » ont été trouvées dans les imprimantes de la médiathèque.

Une lecture rapide des journaux d'évènements indiquait que le poste incriminé était à l'origine des impressions.

Les réseaux sont actuellement cloisonnés via des réseaux locaux virtuels (*VLAN*) basés sur les adresses *MAC* : un « *VLAN* » pour les services de la mairie et un « *VLAN* » pour les accès du public.

#### **Question A1.3**

Expliquer pourquoi cette stratégie de réseaux locaux virtuels (*VLAN*) par adresse *MAC* est insuffisante pour garantir la sécurité du réseau.

Le technicien s'est rendu compte que l'adresse *MAC* de la carte réseau du poste concerné a été modifiée, afin que ce dernier appartienne au « *VLAN* » de la mairie, permettant ainsi l'impression.

#### **Question A1.4**

Proposer une nouvelle stratégie permettant de garantir le cloisonnement des ordinateurs de la médiathèque au sein du réseau local virtuel (*VLAN*) approprié, sans ajouter de matériel d'interconnexion ou de service supplémentaire.

## **Mission A2 – Vérification de l'infrastructure prévue en cas de crise**

Cette seconde mission vise à vérifier la validité de l'infrastructure et de l'organisation prévue en cas de défaillance majeure. Le réseau de la mairie ayant déjà été spécifiquement la cible d'attaques numériques, M. Hopada souhaite s'assurer de la résilience (capacité de résistance) de son système d'information.

Pour atteindre cet objectif, une infrastructure particulière a été mise en œuvre dans un local de la médiathèque afin de permettre la continuité des activités en cas de défaillance majeure.

L'utilité principale de ce « local de secours » est de garantir l'accès aux applications et aux données professionnelles définies comme critiques, c'est-à-dire nécessaires aux activités que doit assurer toute mairie en période de crise.

Ce local est bien entendu inaccessible au public et héberge deux serveurs de virtualisation (SRV-HYPERV3 et SRV-HYPERV4) ainsi qu'un réseau de stockage SAN (SAN-2).

En fonctionnement normal, les ressources du site de secours ne sont pas exploitées par les utilisateurs.

Les activités concernées sont la délivrance des états civils, l'établissement de mandats de paiement, la consultation du cadastre et les opérations de paie, répondant à une obligation légale du code des collectivités. La commune doit en toute circonstance être capable d'acheter du matériel en urgence, d'accéder aux plans cadastraux, de dresser des listes d'alerte aux citoyens, d'établir des actes de décès, etc.

Le plan de continuité d'activité reposant beaucoup sur la réplication, M. Hopada se demande si cette stratégie est suffisante.

### **Question A2.1**

Indiquer si la simple réplication des données garantit l'impossibilité de perte de données.  
*Justifier la réponse.*

Le plan de gestion de crise prévoit qu'en cas d'indisponibilité des postes utilisateurs du site principal de la mairie, les postes de la médiathèque normalement destinés au public soient utilisés pour accéder aux applications du site de secours.

M. Hopada vous demande de comparer cette solution avec l'utilisation de postes dédiés à cette tâche, préparés et stockés dans la salle technique du site de secours.

### **Question A2.2**

Comparer les deux solutions dans un tableau mettant en évidence les trois critères : (1) disponibilité des équipements et rapidité de mise en œuvre, (2) sécurité, (3) coût.

M. Hopada souhaite améliorer son plan de réplication, il vous demande d'en étudier la cohérence. Une attention particulière doit être portée aux applications et données incluses dans le plan, ainsi qu'aux fréquences de synchronisation.

### **Question A2.3**

Identifier au moins deux défauts du plan de réplication actuel, en précisant les problèmes potentiels que ces derniers peuvent engendrer.

Certaines applications de la mairie ont déjà fait l'objet d'une attaque. Des données ont alors été modifiées. Par chance, cet acte malveillant a été découvert trois jours après et une sauvegarde a pu être utilisée pour restaurer les données. M. Hopada s'interroge sur la durée d'historisation des sauvegardes.

### **Question A2.4**

Indiquer si la fréquence d'historisation est adaptée aux usages de la mairie. Le cas échéant, en proposer une nouvelle.  
*Justifier la réponse.*

M. Hopada est aussi soucieux des possibles implications juridiques de ce vol de données.

**Question A2.5**

Identifier les obligations légales qui s'imposent à la mairie, en matière d'archivage et de protection des données des administrés.

Dans le plan actuel, le lieu de sauvegarde est unique. Dans le cas d'une éventuelle attaque simultanée sur le site principal et sur le site de secours, le système d'information serait donc exposé à un risque de perte de données.

**Question A2.6**

Proposer une solution de stockage complémentaire qui permettrait d'améliorer la conservation des données en cas de défaillance majeure.

Durant le mois d'avril de cette année, un individu a tenté de saboter une borne technique située sur la voie publique. Cette borne contient, entre autres, les câbles de connexion entre le site principal et le site de secours. Cet élément a été physiquement sécurisé depuis, mais l'incident a permis de mettre en évidence deux défauts de l'infrastructure :

- l'unicité du lien entre les sites et sa criticité,
- l'impossibilité de disposer d'une connexion internet sur le site de secours en cas de défaillance de ce lien.

**Question A2.7**

Préconiser une solution permettant de résoudre les deux défauts constatés précédemment (lien inter-site unique et absence de connexion internet).

*Justifier la réponse.*

**Mission A3 – Amélioration de la disponibilité des liaisons externes**

Cette mission se concentre sur un autre point sensible du réseau. Tout le trafic des connexions FAI (fournisseurs d'accès à internet) emprunte le routeur pare-feu FW-SEC. Une défaillance matérielle ou une attaque ciblée sur celui-ci rendrait indisponible l'ensemble des connectivités externes. Un projet de mise en œuvre d'une haute disponibilité des pare-feux est à l'étude. M. Alatur, le collaborateur chargé de sa mise en œuvre, est peu au fait des questions de sécurité et vous demande de l'aider dans sa tâche.

M. Alatur s'interroge sur le fait que les pare-feux soient une contre-mesure pleinement efficace contre le déni de service distribué (DDoS), dont il maîtrise peu les problématiques.

**Question A3.1**

- Rappeler l'objectif et le principe de fonctionnement d'une attaque par déni de service distribué.
- Argumenter sur la capacité des pare-feux à résister à une attaque de type DDoS.

Quoi qu'il en soit, le projet de haute disponibilité des pare-feux sera mis en œuvre, car la tolérance de panne s'avère obligatoire. M. Alatur souhaiterait cependant savoir comment réagirait cette partie de l'infrastructure en cas d'attaque, il vous demande donc d'effectuer un test réel en réalisant une simulation d'attaque complète et concrète.

**Question A3.2**

Proposer une procédure de test permettant de vérifier la résilience de la grappe de haute disponibilité des pare-feux face à une attaque de type DDoS.

## Dossier B – Amélioration de la sécurité du réseau

### **Mission B1 – Protection contre les logiciels rançonneurs (rançongiciels ou ransomware)**

La mairie a été par deux fois la cible de logiciels malveillants de type rançongiciel.

Le processus de chaque attaque a été identique : une fois l'intrusion dans le réseau effectuée, les logiciels ont chiffré les fichiers présents dans le système informatique de la mairie. Une clé de déchiffrement a ensuite été proposée par courrier électronique au maire en échange d'une forte somme d'argent. L'administration a bien entendu refusé de payer conformément aux recommandations du CERT (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) et de l'ANSSI (agence nationale de la sécurité des systèmes d'information).

À chaque fois les rançongiciels ont été rapidement découverts, les ressources infectées isolées et les données restaurées à partir d'une sauvegarde préalable, au prix d'une longue période d'indisponibilité de certaines applications et données, allant jusqu'à une semaine pour la seconde attaque.

Le maire ne souhaite plus que cette situation se reproduise. M. Hopada demande d'étudier des moyens de sécurisation permettant d'éviter une nouvelle attaque de ce type.

#### **Question B1.1**

Lister les types d'équipements de la mairie qui peuvent faire l'objet d'une infection par rançongiciel.

#### **Question B1.2**

Citer les impacts directs, pour les différentes catégories d'utilisateurs, de la compromission du réseau par un rançongiciel.

Le premier rançongiciel à avoir sévi est Dharma. Selon l'ANSSI, il est responsable en France de plusieurs incidents connus depuis 2017, majoritairement dans le secteur de la santé.

La mairie n'était pas ciblée spécifiquement. L'infection initiale a été causée par l'utilisation d'une clé USB provenant de l'extérieur. Elle comprenait le rançongiciel qui a été exécuté à l'ouverture d'un document.

Un membre du personnel de la police avait en effet suivi une formation à l'hôpital régional ; il avait récupéré les supports numériques de la formation et voulu les montrer à ses collègues à son retour au sein des locaux de la police municipale. Dès lors, Dharma a commencé à chiffrer les fichiers présents sur la machine ainsi que sur les emplacements réseaux partagés.

#### **Question B1.3**

Proposer au moins deux solutions permettant d'empêcher l'infection du rançongiciel par clé USB.

Le second rançongiciel Clop est intervenu la semaine dernière. Cette fois-ci, il ciblait spécifiquement la mairie. La compromission initiale a eu lieu par l'ouverture d'un courriel malveillant. Le lien piégé contenu dans ce courriel a permis à l'attaquant de déployer des outils de reconnaissance. Les manipulations de l'attaquant ont abouti au déploiement du rançongiciel dans la nuit du samedi au dimanche, chiffrant des données hébergées sur plusieurs serveurs du parc informatique. Selon le mode opératoire classique de ce type d'attaque, le pirate a certainement utilisé des logiciels spécialisés comme *CobaltStrike*, *Metasploit*, *Mimikatz* ou *SDBBot*.

#### **Question B1.4**

Citer aux moins deux moyens permettant de restreindre la propagation de rançongiciel par lien piégé.

Les journaux du routeur indiquent qu'il y a eu une forte activité sortante, laissant supposer une exfiltration de données personnelles. La mairie doit certainement communiquer sur l'attaque.

#### Question B1.5

- a) Rappeler, au niveau juridique, le processus de notification prévu par le RGPD (règlement général sur la protection des données) en cas de faille de sécurité dans le système d'information de la mairie.
- b) Présenter l'objectif de cette procédure pour chaque partie prenante.

L'usage d'internet étant indispensable aux différents services de la mairie, vous devez trouver une solution permettant de limiter la consultation aux sites considérés comme sûrs.

#### Question B1.6

Donner au moins un moyen de restreindre concrètement la navigation à certains sites en expliquant le principe de fonctionnement de ces restrictions.

### Mission B2 – Sécurisation des liaisons avec les sites distants

Suite à une présentation commerciale, M. Hopada souhaite mettre en place un réseau privé virtuel (VPN) site à site entre le site principal de la mairie et le site de secours notamment dans le but de maintenir une réplication des services « *Hyper-V* » et « *Active Directory* » en cas de défaillance de la liaison principale.

#### Question B2.1

Rappeler les objectifs de sécurité garantis par un réseau privé virtuel (VPN) pouvant aider M. Hopada dans la préparation d'un document officiel à destination des décideurs.

M. Hopada n'est pas un spécialiste des technologies VPN. Il a des compétences théoriques concernant les chiffrements symétrique et asymétrique mais ne comprend pas le fonctionnement du chiffrement des données décrit dans la phase 2 du document B1 - *Concepts et généralités VPN IPSec* : « [...] chaque extrémité possédera les deux clés symétriques : une pour chiffrer les données transmises et l'autre pour déchiffrer les données reçues... ».

#### Question B2.2

Représenter à l'aide d'un schéma détaillé l'utilisation des deux clés symétriques, nommées et citées en phase 2 dans le document B1, en indiquant le processus de chiffrement et de déchiffrement des données.

*Vous préciserez le rôle de chaque clé lors de l'envoi et de la réception des flux pour les deux équipements concernés.*

M. Hopada s'interroge sur l'utilisation d'un mécanisme d'IGC (infrastructure de gestion de clés ou PKI - *public key infrastructure*) plutôt que d'un mécanisme de clé pré-partagée (PSK - *pre-shared key*).

#### Question B.2.3

- a) Rappeler l'objectif d'une infrastructure à clé publique.
- b) Expliquer, à l'intention de M. Hopada, la nécessité d'opter pour un mécanisme d'IGC plutôt que pour un mécanisme de clé pré-partagée PSK.



### **Mission B3 – Mise en œuvre du télétravail**

L'équipe du service informatique a entrepris de mettre en place de nouveaux tunnels *VPN* pour clients nomades. Vous n'êtes pas encore totalement satisfait(e) en ce qui concerne la sécurité proposée.

Le logiciel libre *Nextcloud* a été installé sur un serveur de la zone démilitarisée (DMZ) afin de disposer d'un site d'hébergement de fichiers et d'une plateforme de collaboration rendant des services similaires aux services en ligne de *Microsoft OneDrive* et *Google Drive* tout en étant conforme au RGPD. Ce serveur a pour nom de domaine : [collab.saintjacques.fr](https://collab.saintjacques.fr).

Dans le cadre du développement du télétravail, la mairie souhaite offrir à ses collaborateurs un accès sécurisé au serveur de stockage et de partage de fichiers en ligne via un tunnel *VPN* pour client nomade.

Vous disposez d'un extrait des règles de filtrage du pare-feu de la mairie que vous jugez trop permissives.

Vous souhaitez que les utilisateurs Denis Barbier et Bruno Paillard ne puissent accéder au travers du tunnel qu'au site <https://collab.saintjacques.fr>.

#### **Question B3.1**

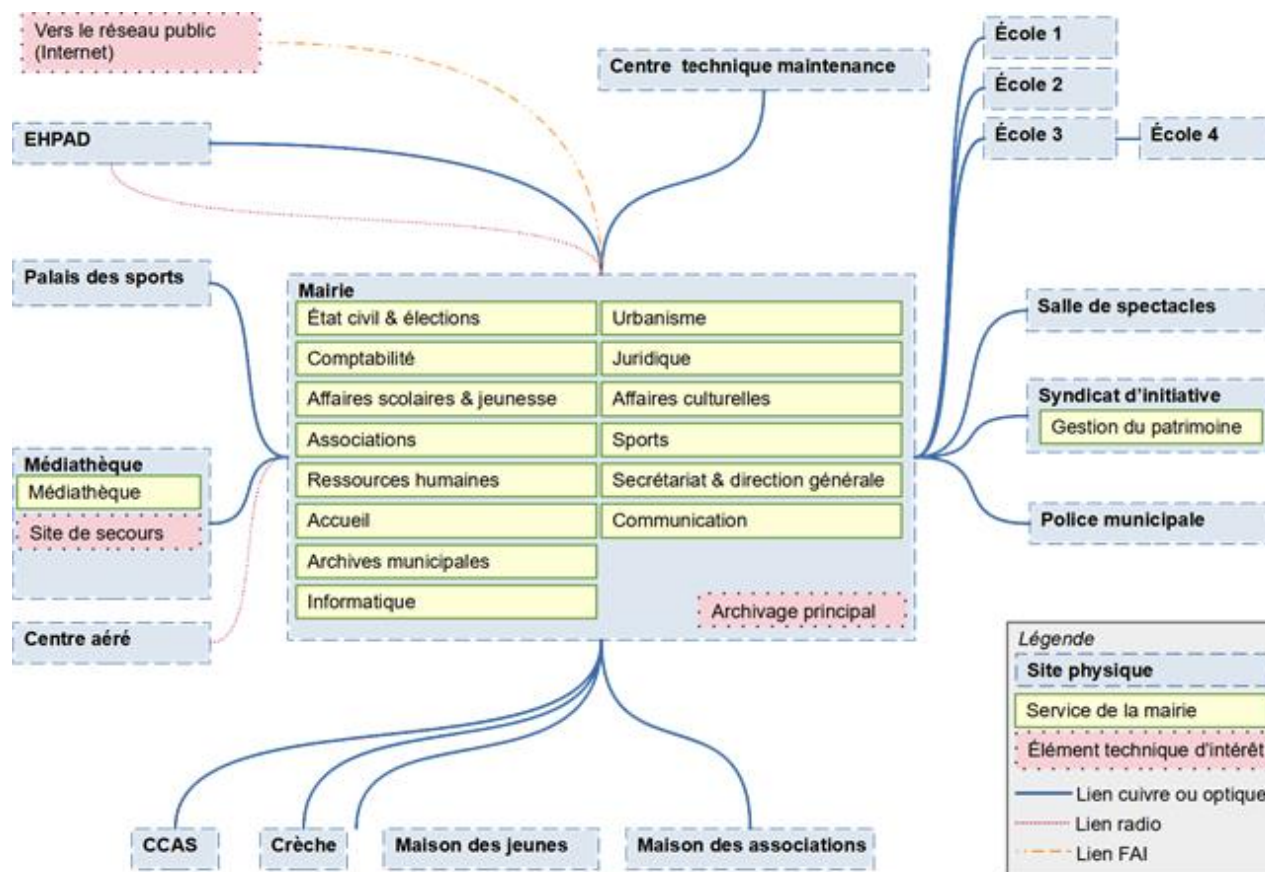
Proposer une modification à apporter aux règles de filtrage, concernant l'accès de ces utilisateurs.

Un ordinateur portable d'un collaborateur a été volé.

#### **Question B3.2**

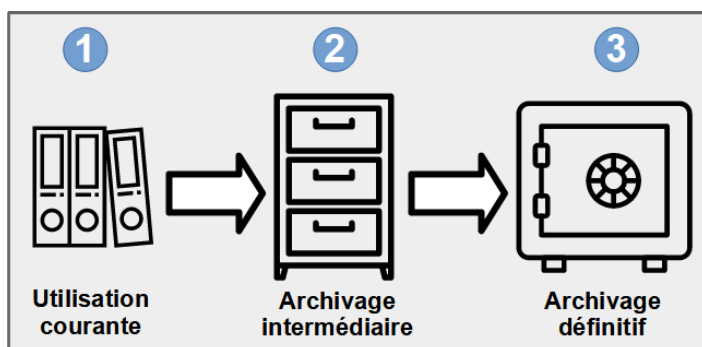
Donner, dans le cas d'un vol d'ordinateur, l'avantage fourni par la méthode d'authentification retenue, exploitant une infrastructure à clé publique (*PKI*).

## Document 1 : Organisation générale des services de la mairie



## Document 2 : Durées de conservation et archives

Les données à caractère personnel doivent être conservées pour la durée de leur utilité. Mais une même donnée peut avoir parfois plusieurs utilités successives ce qui implique donc des durées de conservation différentes.



Les différentes durées de conservation doivent être inscrites dans le registre du délégué à la protection des données pour chacun des traitements concernés.

Dans chacune des phases, le responsable du fichier doit prévoir des mesures techniques et organisationnelles pour protéger les données (destruction, perte, altération, diffusion ou accès non autorisés, etc.).

Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données considérées. Par exemple, les données des destinataires de la lettre d'information de la collectivité n'appellent pas les mêmes mesures que la gestion des prestations sociales octroyées par la collectivité ou le fichier de gestion des activités de la police municipale. Une personne qui exerce son droit d'accès doit obtenir la communication de l'intégralité des données qui la concernent, qu'elles soient stockées en base active ou archivées.

Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

Source : CNIL – Guide de sensibilisation au RGPD pour les collectivités territoriales.

### Document 3 : Applications mises à disposition via le réseau informatique

Service concerné	Application utilisée...	
	...pour un usage professionnel	...par le public
Pour chaque service	<ul style="list-style-type: none"> <li>• Navigation internet</li> <li>• Messagerie</li> <li>• Consultation de l'annuaire interne</li> <li>• Consultation des agendas du service</li> <li>• Demande d'intervention</li> </ul>	
Affaires culturelles	<ul style="list-style-type: none"> <li>• Réservations des salles de spectacle</li> <li>• Outils de planification</li> </ul>	<ul style="list-style-type: none"> <li>• Événements publics</li> </ul>
Affaires scolaires et jeunesse	<ul style="list-style-type: none"> <li>• Inscriptions scolaires et périscolaires</li> <li>• Suivi des présences périscolaire</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation des menus des cantines</li> <li>• Inscriptions et paiements du périscolaire</li> </ul>
Archives	<ul style="list-style-type: none"> <li>• Gestion électronique des documents</li> </ul>	
Associations	<ul style="list-style-type: none"> <li>• Gestion des demandes de subventions</li> </ul>	<ul style="list-style-type: none"> <li>• Demandes de subventions</li> </ul>
Centre technique	<ul style="list-style-type: none"> <li>• Gestion des plans techniques</li> <li>• Applications de maintenance spécialisées</li> </ul>	
Communication	<ul style="list-style-type: none"> <li>• Publications sur les réseaux sociaux</li> <li>• Outils de PAO</li> <li>• Outils de relations avec la presse</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation de l'agenda public</li> <li>• Consultation de l'annuaire public</li> <li>• Consultation du guide pratique</li> <li>• Consultation du Bulletin municipal</li> </ul>
Comptabilité / finances	<ul style="list-style-type: none"> <li>• <b>Mandats de paiement</b></li> <li>• Achats</li> <li>• Encaissements</li> <li>• Télédéclarations comptables</li> </ul>	
État civil et élections	<ul style="list-style-type: none"> <li>• <b>Délivrance des états civils</b></li> <li>• Recensement de la population</li> <li>• Recensement militaire</li> <li>• Élections</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation des résultats publics des élections</li> </ul>
Gestion patrimoine	<ul style="list-style-type: none"> <li>• Gestion des fichiers du patrimoine</li> </ul>	
Informatique	<ul style="list-style-type: none"> <li>• Administration &amp; Supervision</li> <li>• Gestion du patrimoine informatique</li> </ul>	
Juridique	<ul style="list-style-type: none"> <li>• Consultation de sites spécialisés</li> <li>• Publication d'annonces légales</li> <li>• Gestion des marchés publics</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation des annonces légales, loi et règlements</li> </ul>
Médiathèque	<ul style="list-style-type: none"> <li>• Gestion des prêts</li> </ul>	<ul style="list-style-type: none"> <li>• Recherches documentaires</li> </ul>
Police municipale	<ul style="list-style-type: none"> <li>• Accès aux fichiers de police</li> <li>• Accès aux fichiers centralisés de gestion des immatriculations</li> <li>• Accès à la vidéosurveillance</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation des informations de sûreté (Vigipirate, mise en sécurité...)</li> </ul>
Ressources humaines	<ul style="list-style-type: none"> <li>• <b>Paie</b></li> <li>• Gestion des carrières des agents</li> <li>• Gestion des effectifs</li> </ul>	<ul style="list-style-type: none"> <li>• Consultation des offres d'emploi</li> </ul>
Secrétariat du maire et administration générale	<ul style="list-style-type: none"> <li>• Consultation et prise de rendez-vous (tous services)</li> </ul>	
Sports	<ul style="list-style-type: none"> <li>• Réservation des équipements sportifs</li> <li>• Outils de planification</li> </ul>	
Urbanisme	<ul style="list-style-type: none"> <li>• <b>Propriété foncière / Cadastre</b></li> <li>• Autorisations d'urbanisme</li> <li>• Consultation droits des sols</li> <li>• Police de l'urbanisme et contentieux</li> </ul>	

**Applications critiques** : Délivrance des états civils, mandats de paiement, cadastre, paie

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 11 sur 19

**Document 4 : Matériel utilisateur de chaque service**

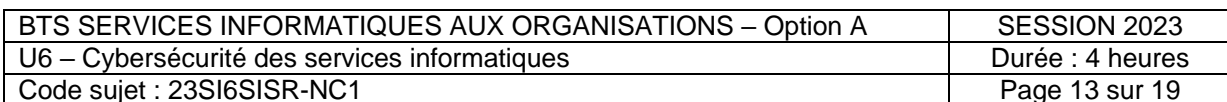
Service de la mairie ou lieu	Nombre de postes de travail		Service de la mairie ou lieu	Nombre de postes de travail	
	Mairie	Public		Mairie	Public
Accueil	1		Ressources humaines	1	
Affaires scolaires et jeunesse	2		Secrétariat du maire et administration générale	1	
Affaires culturelles	2		Sports	1	
Archives	1		Urbanisme	1	
CCAS (Centre Communal d'Action Sociale)		2	Écoles (toutes écoles confondues)	4	82
Centre technique	2		Associations	1	
Communication	3		Centre aéré	1	
Comptabilité	2		Crèche	1	
État civil et élections	2		EHPAD	1	2
Gestion du patrimoine	1		Maison des associations		1
Informatique	4		Maison de la jeunesse		1
Juridique	1		Palais des sports	1	
Médiathèque	3	4	Salle de spectacles	3	
Police municipale	3		Syndicat d'initiative	1	1

**Document 5 : Description des liaisons**

Accès internet	Débits théoriques	Notes
Liaison spécialisée fibre optique	<ul style="list-style-type: none"> <li>300 Mb/s descendant</li> <li>300 Mb/s montant</li> </ul>	<ul style="list-style-type: none"> <li>Il s'agit du réseau de la communauté d'agglomération, partagé par plusieurs communes géographiquement proches.</li> <li>Ce réseau est assimilable à celui d'un fournisseur d'accès internet.</li> <li>Aucune sécurité particulière n'est assurée sur ce réseau, cette activité reste à la charge de chaque mairie.</li> <li>Une stratégie de qualité de service (non gérée par la mairie) garantit les débits théoriques pour 80 Mb/s descendant et 80 Mb/s montant.</li> </ul>
SDSL	<ul style="list-style-type: none"> <li>32 Mb/s descendant</li> <li>32 Mb/s montant</li> </ul>	<ul style="list-style-type: none"> <li>Les débits sont garantis pour 20 Mb/s descendant et 20 Mb/s montant, sauf cas de défaillance majeure</li> </ul>
ADSL	<ul style="list-style-type: none"> <li>64 Mb/s descendant</li> <li>8 Mb/s montant</li> </ul>	<ul style="list-style-type: none"> <li>Les débits ne sont pas garantis</li> <li>Fournisseur différent de la liaison SDSL</li> </ul>

Pour les liens entre sites	Pour les liens à l'intérieur d'un site
<ul style="list-style-type: none"> <li>20 Gb/s fibre optique ou cuivre selon les distances (2 liens 10 Gb/s agrégés pour la performance et la tolérance de panne) ;</li> <li>64 Mb/s radiofréquence entre la mairie et l'EHPAD (utilisé comme lien de secours) ;</li> <li>32 Mb/s radiofréquence entre la mairie et le centre aéré.</li> </ul>	<ul style="list-style-type: none"> <li>20 Gb/s (2 liens 10 Gb/s agrégés) entre le matériel d'interconnexion et le matériel de production (serveurs, SAN, NAS) ;</li> <li>1 Gb/s cuivre pour les équipements utilisateurs, les points d'accès sans fil, le matériel domotique.</li> </ul>

Notes : - les commutateurs utilisés dans l'infrastructure de la mairie sont de niveau 3.  
- Les points d'accès Wifi WF-SPEC et WF-MEDIAT sont ouverts au public.



## Document 7 : Stockage des données et applications du système d'information

Les **applications** sont installées :

- soit directement sur les postes de travail des utilisateurs de chaque service de la mairie. Il s'agit d'applications de type bureautique ou d'applications spécifiques utilisées localement (exemple : outils de conception assistée par ordinateur pour le centre de maintenance municipal) ;
- soit sur les serveurs de virtualisation. Il s'agit alors d'applications accessibles par le réseau, partagées par différents services (exemples : messagerie électronique, agenda commun, etc.) ou exploitées par un service particulier (exemple : application de mandats de paiement pour le service comptabilité).

Concernant les applications professionnelles utilisables en réseau, ces dernières sont stockées via des machines virtuelles dans les serveurs de virtualisation SRV-HYPERV1 et SRV-HYPERV2. La règle générale utilisée est qu'une application réseau correspond à une machine virtuelle.

Les machines virtuelles, et donc les applications, sont attribuées manuellement sur l'un ou l'autre des serveurs de virtualisation par les administrateurs réseau, qui tentent de répartir la charge de travail de manière à peu près équilibrée.

Il faut noter l'existence d'une machine virtuelle générale comportant un serveur « *Active Directory* », un serveur DHCP pour les accès publics, un serveur de fichiers, ainsi qu'un serveur de messagerie électronique interne.

Les **données** applicatives et les fichiers utilisateurs sont stockés comme suit :

- sur les postes de travail des utilisateurs pour les fichiers personnalisés, temporaires (niveau de l'information : utile, reproductible) ;
- sur les répertoires partagés du serveur de fichiers pour les modèles, documents finalisés (niveau de l'information : nécessaire ou critique).

Il existe quelques exceptions à cette organisation générale :

- les données des quatre écoles sont centralisées sur le serveur de stockage en réseau (NAS) dédié NAS-ECOLES ;
- les fichiers de capture issus des caméras de vidéosurveillance analogique de la commune sont stockés temporairement sur les deux serveurs de traitement vidéo au sein des locaux de la police municipale (le traitement consiste en la numérisation, l'encodage, l'ajout de métadonnées et l'indexation des vidéos). Les vidéos traitées sont stockées sur le serveur NAS dédié NAS-VIDEO afin de permettre la recherche et la consultation ultérieure ;
- certaines informations de l'EHPAD ne relèvent pas de la mairie (car médicales et confidentielles), le stockage et la conservation de ces données restent à la charge de l'EHPAD et du conseil départemental. Les données partageables avec la mairie sont en revanche stockées dans le dossier réseau du serveur de fichiers.

Les machines virtuelles des serveurs de virtualisation SRV-HYPERV1 et SRV-HYPERV2 exploitent diverses liaisons iSCSI vers le serveur de stockage SAN-1. L'ensemble des données, y compris celles du serveur de fichiers, sont donc stockées physiquement sur le serveur SAN-1.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 14 sur 19

## Documents associés au dossier A

### Document A1 : La continuité d'activité en cas de sinistre

En cas d'indisponibilité prolongée des serveurs suite à un événement climatique ou une attaque informatique sur le site principal de la mairie, les utilisateurs sont redirigés vers les applications et données du site de secours.

**Le plan de réplication** suivant a été mis en œuvre afin de garantir la continuation des activités :

- les machines virtuelles sont répliquées chaque dimanche :
  - le serveur SRV-HYPERV1 est répliqué sur le serveur SRV-HYPERV3,
  - le serveur SRV-HYPERV2 sur le serveur SRV-HYPERV4 ;
- le serveur SAN-1 est répliqué en temps réel sur le serveur SAN-2 ;
- les fichiers des écoles sont répliqués sur le serveur SAN-1 tous les semestres ;
- les fichiers de l'EHPAD partageables avec la mairie sont répliqués sur le serveur SAN-1 chaque soir ;
- les fichiers vidéo de la police municipale (NAS-VIDEO) ne sont pas répliqués ; ces fichiers sont importants en cas d'enquête diligentée par les autorités.

Le basculement du site principal vers le site de secours est réalisé manuellement par l'équipe informatique, qui reconfigure le réseau si besoin.

En cas d'indisponibilité des postes utilisateurs lors d'une crise, l'équipe informatique reconfigure les postes publics de la médiathèque afin de les intégrer au réseau local virtuel (VLAN) de la mairie.

Des vérifications sur l'exploitabilité des applications sont réalisées le premier mercredi de chaque mois pour les applications critiques.

**Un plan de sauvegarde** est lui aussi prévu.

Les utilisateurs des applications de la mairie ont pour consigne d'enregistrer leurs données dans les répertoires partagés du serveur de fichiers. Le contenu de ce dernier est inclus dans le plan de sauvegarde. Les données des applications réseau sont automatiquement stockées sur le serveur SAN-1.

Le contenu du serveur SAN-1 est sauvegardé chaque jour selon la stratégie suivante : une sauvegarde complète le dimanche, une sauvegarde incrémentielle chaque autre jour de la semaine. Les sauvegardes sont stockées sur le serveur SAN-2.

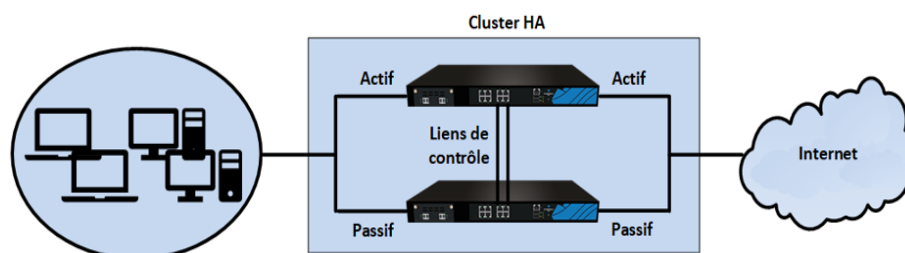
Une seule sauvegarde complète (la dernière) reste disponible sur le serveur SAN-2.

Afin de répondre à des contraintes légales, un archivage sur bande de la dernière sauvegarde est réalisé à la fin de chaque année civile. L'ensemble des bandes est conservé dans une armoire spécialisée située au service des archives de la mairie.

### Document A2 : Haute disponibilité des pare-feux

La fonctionnalité haute disponibilité (HA - *high availability*) permet d'assurer la continuité de service en cas de panne (réseau ou pare-feu) en mettant en œuvre une grappe de pare-feux (ou « *cluster de firewalls* »). Cette architecture nécessite la duplication des liens qui permettent de connecter le réseau local à internet.

Pour constituer la grappe en haute disponibilité, les deux pare-feux sont reliés avec un ou deux liens de contrôle (le deuxième lien est facultatif mais fortement recommandé) sur des interfaces dédiées.



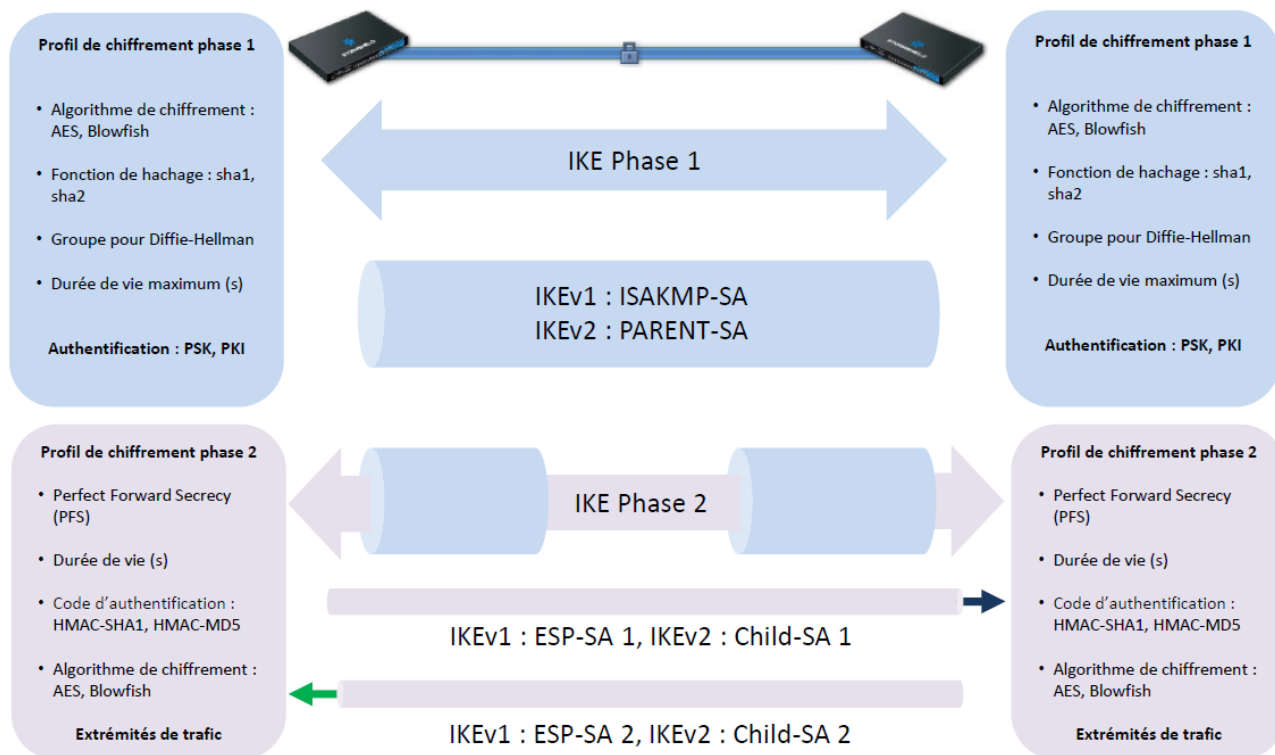
Les pare-feux d'une même grappe possèdent une configuration identique. Ils fonctionnent en mode actif / passif, ce qui signifie qu'un seul pare-feu est actif (fonctionnel) à un instant donné, et que seul ce pare-feu gère l'ensemble du trafic transitant entre les réseaux connectés à la grappe.

Source : documentation Stormshield SNS

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 15 sur 19



Document B1 : Concepts et généralités des réseaux privés virtuels de type VPN IPSec



La négociation avec le protocole IKE (*internet key exchange*) pour l'établissement d'un tunnel VPN IPSec se déroule en deux phases :

• **Phase 1** : durant cette phase, les deux extrémités de tunnel négocient un profil de chiffrement phase 1 qui contient les algorithmes de chiffrement/authentification. Durant cette phase également, les deux extrémités s'authentifient avec une clé pré-partagée ou avec des certificats. Dès que les deux extrémités se mettent d'accord, un dialogue d'application chiffré, nommé ISAKMP-SA (*internet security association key management protocol – security association*) dans le protocole IKEv1 ou PARENT-SA dans le protocole IKEv2, est établi entre les deux extrémités. Il permet la négociation de la phase 2 qui sera entièrement chiffrée grâce à la clé de phase 1.

• **Phase 2** : durant cette phase, les deux extrémités négocient le profil de chiffrement de phase 2 et les extrémités de trafic qui pourront communiquer via le tunnel VPN IPSec. Dès que les deux extrémités parviennent à faire concorder ces paramètres, deux canaux sont ouverts pour la transmission des données (un dans chaque direction). Chaque canal utilise sa propre clé de chiffrement. Elles sont appelées ESP-SA1 et ESP-SA2 selon le protocole IKEv1 et CHILD-SA1 et CHILD-SA2 selon le protocole IKEv2. Ainsi chaque extrémité possédera les deux clés symétriques : une pour chiffrer les données transmises et l'autre pour déchiffrer les données reçues.

Source : D'après le guide de formation Stormshield CSNA



## Document B2 : Certificats et infrastructure de gestion de clés (PKI)

Lorsqu'un équipement est impliqué dans un mécanisme d'authentification, ce dernier peut reposer sur des certificats issus d'une infrastructure de gestion de clés (IGC). La confiance placée dans cette IGC détermine alors la confiance du certificat utilisé et donc la fiabilité de l'authentification. En cas d'absence de solution externe de gestion des certificats, les pare-feux SNS (*Stormshield network security*) offrent la possibilité de générer une autorité de certification ainsi que des certificats signés par cette autorité.

Plusieurs cas d'usage impliquent l'utilisation de certificats par des équipements SNS, dont :

- la publication de l'interface d'administration *web* en mobilisant le protocole HTTPS ;
- l'authentification par certificat des administrateurs pour l'accès à l'interface *web* d'administration du pare-feu SNS ;
- l'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place de tunnels VPN IPSec ;
- l'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place d'un service de réseau privé virtuel VPN SSL/TLS ;
- la connexion à un annuaire externe au format LDAPS.

Source : ANSSI - Recommandations de sécurisation d'un pare-feu SNS

## Document B3 : Protocole IPSec et authentification des correspondants

L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (*PSK - pre-shared Key*), soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une infrastructure de gestion de clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes.

On privilégie généralement l'utilisation d'une IGC, ce qui permet de simplifier l'exploitation du système : l'ajout d'un nouvel hôte ou la révocation d'une clé compromise est aisé (il n'est pas nécessaire d'intervenir sur tous les équipements déjà en place). Il peut être délicat dans les autres modes de réagir avec la rapidité nécessaire à une compromission de clé, par exemple le vol d'un équipement.

Le mode *PSK* doit en principe être évité pour des systèmes en production et être cantonné à des systèmes de tests ou à des opérations de diagnostic. S'il était nécessaire d'y recourir exceptionnellement, une bonne pratique générale pour les secrets partagés est de prendre garde à ce que sa robustesse soit suffisante pour rendre difficile une attaque par recherche exhaustive. On se reportera à ce sujet au référentiel général de sécurité publié par l'ANSSI. Une longueur inférieure à 100 bits est considérée à la date de rédaction de ce document comme un choix risqué.

Il est fortement déconseillé dans le cas général d'utiliser la mise en place d'une clé manuelle ou clé pré-partagée (*PSK*) pour l'établissement d'un lien IPSec. Des mécanismes basés sur de la cryptographie asymétrique sont à privilégier. On favorisera en particulier les mécanismes d'IGC qui permettent la révocation rapide des clés compromises, en particulier en cas de perte d'un poste. Les dérogations à ces recommandations doivent avoir fait l'objet d'une étude de sécurité rigoureuse.

Source : ANSSI - Note technique - Recommandations de sécurité relatives à IPSec pour la protection des flux réseau-2015

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 17 sur 19

## Document B4 : Tunnel VPN IPsec nomade (pare-feu UTM SNS Stormshield mairie)

Un correspondant nomade mentionnant le profil de chiffrement de la phase 1 retenu a été créé avec les paramètres suivants :

### VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS   **CORRESPONDANTS**   IDENTIFICATION   PROFILS DE CHIFFREMENT

Chercher dans les corres...  Filtrer▼

+ Ajouter▼   × Supprimer   Renommer

Nom ▲

- nomade\_mairiea
- Site\_Fw\_B

Correspondant : nomade\_mairiea

Commentaire :

Passerelle distante : Any ▼

Configuration de secours : None ▼

Profil IKE : GoodEncryption ▼

Version IKE : IKEv2 ▼

Identification

Méthode d'authentification : Certificat ▼

Certificat : mairie-saintjacques ×

Local ID (Optionnel) : Saisir un identifiant

[Cliquer ici pour éditer la liste des PSK](#)

Un tunnel VPN IPsec nomade, mentionnant le profil de chiffrement de phase 2 retenu, a été configuré avec les paramètres suivants :

POLITIQUE DE CHIFFREMENT - TUNNELS

CORRESPONDANTS

IDENTIFICATION

PROFILS DE CHIFFREMENT

(1) IPsec 01

Activer cette politique

Editer

SITE À SITE (GATEWAY-GATEWAY)

ANONYME - UTILISATEURS NOMADES

Texte recherché

+ Ajouter

✕ Supprimer

↑ Monter

↓ Descendre


















































Couper

Copier

Coller

Ligne	Etat	Réseau local	Correspondant	Réseau nomade	Profil de chiffrement	Mode config
1	<div>on</div>	<div>Network_dmz1</div>	<div>nomade_mairiea</div>	<div>Net-IPSECVPN</div>	<div>GoodEncryption</div>	<div><div>on</div><div>Modifier</div></div>

Vous disposez d'un extrait des règles de filtrage spécifiques au réseau privé virtuel (VPN) *IPSec* nomade ainsi qu'au *VPN IPSec* site à site :

FILTRE		NAT					
Rechercher...		<a href="#">+ Nouvelle règle</a> <a href="#">X Supprimer</a> <a href="#">↑</a> <a href="#">↓</a> <a href="#">↕</a> <a href="#">↗</a> <a href="#">↘</a> <a href="#">Couper</a> <a href="#">Copier</a> <a href="#">Coller</a> <a href="#">Chercher dans les logs</a>					
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
20	 on	 passer	 Network_out	 Firewall_out	 ssh		
<div> <div></div> <div>Autoriser ISAKMP et protocole ESP (contient 2 règles, de 21 à 22)</div> </div>							
21	 on	 passer	 Any	 Firewall_out	 isakmp  isakmp_natt		
22	 on	 passer	 Any	 Firewall_out	 Any	vpn-esp	
<div> <div></div> <div>VPN IPSEC Nomade (contient 3 règles, de 23 à 25)</div> </div>							
23	 on	 passer	 bpaillard Auth. par :VPN IPsec via Tunnel VPN IPsec	 Network_dmz1	 Any		
24	 on	 passer	 dbarbier Auth. par :VPN IPsec via Tunnel VPN IPsec	 Network_dmz1	 Any		
25	 on	 passer	 vgrosjean Auth. par :VPN IPsec via Tunnel VPN IPsec	 Network_dmz1	 Any		
<div> <div></div> <div>VPN IPSEC site à site (contient 2 règles, de 26 à 27)</div> </div>							
26	 on	 passer	 NET_internals_B via Tunnel VPN IPsec	 srv_ftp_priv	 ftp		
27	 on	 passer	 NET_internals_B via Tunnel VPN IPsec	 srv_ftp_priv	 Any	icmp (requête Echo (Ping))	

Ces objets sont utilisés pour configurer les règles de façon plus parlante et succincte : cela permet de manipuler des noms d'objets, plus parlants que des valeurs et donc de simplifier la modification de ces valeurs.

- l'objet **http** désigne le port **TCP 80** ;
- l'objet **Network\_dmz1** désigne le **réseau IP** associé à la DMZ1 ;
- l'objet **srv\_ftp\_priv** désigne un hôte particulier (son **adresse IP**).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2023
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 23SI6SISR-NC1	Page 19 sur 19