

RÉSEAUX INFORMATIQUES

RÈGLES DE SÉCURITÉ

Référence	FT_SSI-RES_Réseaux informatiques_v1.5.docx
Clef GED	72633
Version	V1.5
Classification	Interne
Date	17/07/2020
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction Maitrise des Risques

Identification du document

Référence		Titre du document	
FT_SSI-RES_Réseaux informatiques_v1.5.docx		Réseaux informatiques	
Version		État du document	Auteurs
1.5		Final	Filière Sécurité des SI

Classification

Niveau	Diffusion
Interne	Le personnel de France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité,...)

Mises à jour

Version	Date	Nature de la modification
1.3	30 juillet 2018	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.4	05 juin 2020	Mises à jour dans le cadre de la directive NIS (conformité OSE)
1.5	20 février 2024	Mise à jour suite au changement marque PE→FT

Relectures et validations

Version	Relu par	Direction	Date	Statut
1.3	RSSI Sylvain Lambert	DGA-SI	13/07/2018	Validé
1.3	Mojdeh Hodjat-Panah-Daurelle	DGA-DMR	30/07/2018	Validé
1.4	RSSI Sylvain Lambert	DGA-SI	17/07/2020	Validé

Documents de référence

Référence	Titre du document
[1] Colibri 196557	Demande de dérogation
[2] Colibri 262372	Environnement de travail - Fixes
[3] Colibri 262373	Environnement de travail - Mobiles
[4] Colibri 262371	Environnement de travail - Bornes
[5] Colibri 262120	Environnement de travail – Supports Amovibles
[6] Colibri 268674	Charte d'engagement individuel de confidentialité
[7] Colibri 72649	Charte d'accès au SI par des tiers
[8] Colibri 72643	Classification et protection de l'information
[9] Colibri 72638	Plan de secours informatique
[10] Colibri 72634	Téléphonie

SOMMAIRE

1. PRÉAMBULE	4
1.1. Principes fondateurs de la Politique Générale de Sécurité des SI	4
1.2. Enjeux et objectifs du document.....	4
1.3. Champ d'application	4
2. CONCEPTS GÉNÉRAUX	5
3. RÔLES ET RESPONSABILITÉS.....	6
4. RÈGLES DE SÉCURITÉ.....	7
4.1. Périmètres de Protection	7
4.2. Règles relatives à l'architecture.....	8
4.2.1. Cloisonnement en domaines de confiance	8
4.2.2. Confidentialité des données	12
4.2.3. Accès au réseau interne.....	13
4.2.4. Accès aux ressources internes du SI	15
4.3. Règles relatives à l'exploitation et à la surveillance des réseaux	16
4.3.1. Qualité et continuité de service	16
4.3.2. Administration et supervision des réseaux.....	17
4.3.3. Exploitation des flux externes.....	20
5. ANNEXES.....	23
5.1. Glossaire	23
5.2. Liste des règles.....	27

Règles typographiques

Les termes écrits en vert et soulignés sont définis dans le glossaire de ce document.

Les règles de la thématique « Réseaux Informatiques » sont préfixées par le sigle « **RES-** » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

Définition de la règle

1. PRÉAMBULE

1.1. PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les systèmes d'information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que France Travail a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de France Travail.

1.2. ENJEUX ET OBJECTIFS DU DOCUMENT

Les Systèmes d'Information de France Travail sont confrontés à de nombreuses problématiques, liées au développement des interconnexions des réseaux avec ceux des **Tiers** et des partenaires, non maîtrisés, et avec Internet : ils constituent des vecteurs de risques potentiellement importants.

De ce fait, la sécurité des réseaux informatiques requiert des mesures de sécurité appropriées et adaptées aux environnements pour prévenir ces risques, notamment :

- L'intrusion à partir de points d'accès externes, et l'accès illicite aux ressources internes (attaque des services),
- Le vol ou l'atteinte à l'intégrité des informations en transit (écoute et interception),
- Le **déni de service**.

Ainsi, l'objet de ce document est de définir les règles visant à structurer et sécuriser la manière d'accéder aux informations et aux ressources de France Travail afin de :

- Limiter les risques de compromission des Systèmes d'Information,
- Rationaliser les accès externes,
- Protéger les actifs (patrimoine informationnel, logiciels, matériel et services),
- Préserver les performances des réseaux.

1.3. CHAMP D'APPLICATION

Ce document s'adresse aux personnels (agents) de France Travail et à l'ensemble des **tiers** ayant accès aux systèmes d'information de France Travail.

En cas de non applicabilité d'une des règles du présent document, une procédure de dérogation [1] doit être engagée. Cette demande de dérogation sera transmise au Responsable Sécurité des Systèmes d'Information.

Pour ce qui concerne les flux de téléphonie, le document thématique « Téléphonie » [10] peut compléter ce document pour les flux spécifiques voix.

2. CONCEPTS GÉNÉRAUX

Le présent document traite des points suivants :

Le présent document traite de la sécurité de l'ensemble des infrastructures réseau de France Travail, concernant notamment :

- Les réseaux locaux, métropolitains et d'interconnexion ainsi que les équipements actifs de ces réseaux,
- Les infrastructures de raccordement sécurisées des agents nomades, des partenaires, des tiers, des mainteneurs,...
- Les moyens de cloisonnement internes et externes aux réseaux,
- Les moyens d'accès et de contrôle permettant la connexion sans fil ou la connexion à distance aux réseaux,
- Les échanges opérés avec des tiers partenaires,
- Les équipements assurant l'interconnexion avec le réseau externe.

3. RÔLES ET RESPONSABILITÉS

Ce chapitre définit les **rôles fonctionnels** intervenant dans les processus d'application et de contrôle des règles énoncées dans le présent document, ainsi que les **responsabilités** associées à chacun de ces rôles :

- La Direction du Management des Risques et de la Sûreté (DMRS)
 - ▶ Valide les règles de sécurité relative aux réseaux informatiques.
 - ▶ Est informée des résultats des contrôles de conformité
 - ▶ Est informée des dérogations accordées par le département sécurité
- Le Département Sécurité
 - ▶ Définit les exigences fonctionnelles de sécurité,
 - ▶ Participe à la validation des dispositifs de sécurité,
 - ▶ Commandite des contrôles de conformité sur leur mise en place, afin de s'assurer de la cohérence entre ce qui est déployé et les exigences de sécurité,
 - ▶ Élabore les messages de sensibilisation à destination de l'ensemble des acteurs (Architecture, Maîtrise d'œuvre, Administration et Exploitation) en charge des infrastructures réseaux,
 - ▶ Gère les dérogations SSI et suit leur avancement.
- Le Département Architecture
 - ▶ Élabore et définit les architectures réseau et les standards applicables aux infrastructures réseaux et à leur sécurisation,
 - ▶ Contrôle les cahiers des charges des projets de refonte d'infrastructures réseau et télécoms,
 - ▶ S'assure de la cohérence entre ce qui est livré par la Maîtrise d'œuvre et les exigences de sécurité fonctionnelles exprimées par la Maîtrise d'Ouvrage Sécurité.
- La Maîtrise d'Œuvre
 - ▶ Traduit les exigences fonctionnelles de sécurité en objectifs et mesures techniques de sécurité adaptées aux infrastructures en place et aux standards internes en vigueur.
- L'Administration et l'Exploitation des infrastructures de communication réseau
 - ▶ Déploient, administrent, supervisent et maintiennent les infrastructures techniques réseaux et télécoms dans un état intègre, opérationnel et conforme aux engagements de service,
 - ▶ Assurent la mise en place des mesures et des moyens de sécurité relatifs à ces réseaux, conformément aux règles thématiques de sécurité établies.
- Les Utilisateurs & Métiers
 - ▶ S'engagent à respecter les règles de sécurité en vigueur et appliquer les bonnes pratiques en matière d'utilisation des réseaux informatiques et des Systèmes d'Information plus généralement.

4. RÈGLES DE SÉCURITÉ

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

Préconisations :

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

Recommandations :

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

Commentaires :

Des précisions sont apportées afin d'éclairer la règle énoncée.

4.1. PÉRIMÈTRES DE PROTECTION

RES-01 Interdiction des accès réseaux en dehors des points d'accès et de contrôle définis

Aucun accès réseau (entrant ou sortant) n'est autorisé en dehors des points d'accès et de contrôle mis en œuvre par la DSI de France Travail.

Néanmoins, par dérogation à la politique de sécurité, il est possible de créer un accès sortant Internet non contrôlé par la DSI de France Travail aux conditions suivantes :

- Le dispositif utilisé est isolé physiquement du réseau donnant accès au SI de France Travail,
- Un responsable de la navigation est identifié et porte la responsabilité des conséquences légales en cas de détournement d'usage de la solution,
- Une description du besoin justifiant le non-respect de la politique de sécurité est précisée dans la demande de dérogation.

Commentaires :

- En cas de dérogation, le responsable de la navigation doit notamment assurer l'identification des personnes navigant sur Internet.

4.2. RÈGLES RELATIVES À L'ARCHITECTURE

4.2.1. Cloisonnement en domaines de confiance

RES-02 Cloisonnement des réseaux en domaines de confiance

Les réseaux sont structurés en différents domaines de confiance, selon :

- Le niveau de sensibilité des ressources qu'ils hébergent
- Le niveau de risque que font peser les populations qui y accèdent

Ces domaines de confiance répondent à un principe de cloisonnement entre eux, visant à maîtriser les échanges et garantir le confinement de chacun des domaines communicants.

Commentaires :

- Le cloisonnement peut être logique et/ou physique.
- Traditionnellement, on oppose les réseaux de production informatiques des autres réseaux notamment, les réseaux internes utilisateurs, les réseaux de partenaires et les réseaux tiers (public comme Internet, semi-publics ou privés comme les réseaux d'opérateurs). Ce découpage dépend du contexte de l'entreprise.
- A titre d'illustration, les mécanismes de protection peuvent comprendre la translation des adresses (NAT), le filtrage réseau (commutateurs filtrants, routeurs, pare-feux), les réseaux virtuels (VLAN, VPN...), le filtrage applicatif (pare-feux applicatifs, relais), antispoofing, contrôle de conformité, 802.1x, IPS...

RES-03 Cloisonnement d'un système d'information essentiel

Chaque SIE est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes d'information de France Travail

Lorsqu'un SIE est lui-même constitué de sous-systèmes, ceux-ci sont cloisonnés entre eux physiquement ou logiquement.

Commentaires :

- Un sous-système peut être constitué pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIE ou encore pour isoler des ressources d'un SIE nécessitant un même besoin de sécurité.
- Seules les interconnexions strictement nécessaires au bon fonctionnement et à la sécurité d'un SIE sont mises en place entre le SIE et les autres systèmes ou entre les sous-systèmes du SIE.

RES-04 Mutualisation de services d'infrastructure entre domaines de confiance

Entre domaines de confiance présentant une certaine « adjacence » en termes de sensibilité, la mutualisation des services d'infrastructure est envisageable.

Pour les domaines présentant des risques importants (par exemple Internet), les services d'infrastructure doivent être spécialisés par domaine et leur contenu adapté aux besoins réels des zones concernées.

Une analyse de risques doit dans tous les cas être menée et un arbitrage rendu par le RSSI

Commentaires :

- Les services d'infrastructure concernés sont ceux essentiels au bon fonctionnement des réseaux (services DNS, DHCP, annuaires ...).

Préconisations :

- Ces services d'infrastructure doivent faire l'objet d'une sécurisation afin de garantir leur intégrité (restriction d'accès en modification...), et leur disponibilité (redondance des ressources délivrant les services...).

RES-05 Doublement des mécanismes filtrants entre domaines de confiance opposés

La communication entre 2 domaines de confiance opposés (interne/externe) requiert une architecture de cloisonnement à 2 niveaux au moyen d'équipements de sécurité filtrant de nature et de technologie différente.

Commentaires :

- Les communications entre l'Internet et le SI Interne doivent transiter au travers d'une double barrière filtrante : lorsque le 1er niveau est compromis, l'isolation des ressources internes est garantie par le 2ème niveau s'appuyant sur une solution d'un éditeur différent.

Préconisations :

- Une virtualisation des mécanismes filtrants permettrait de répondre à cette exigence pour les flux sortants directement en agence (en dehors du Datacenter) peut être envisagée.
- L'exposition de service (directement en agence, hors du Datacenter) nécessiterait la conduite d'une analyse de risque projet.

RES-06 Point d'Accès et de Contrôle

Tout accès logique aux réseaux de France Travail réclame l'application d'un contrôle d'accès. Selon les cas, le contrôle d'accès pourra être au choix :

- Restrictif : « *tout est interdit sauf ce qui est explicitement autorisé* »,
- Permissif : « *tout est autorisé sauf ce qui est explicitement interdit* ».

Ces contrôles sont conduits au niveau des **points d'accès et de contrôle** (cloisonnement) entre domaines de confiance.

Commentaires :

- Le contrôle d'accès restrictif est généralement conduit au moyen de « mécanismes filtrants » (routeur, pare-feux réseau...).
- Le contrôle d'accès permissif est conduit au moyen de « mécanismes préventifs » (IDS, IPS, antivirus...).
- L'application de l'une ou l'autre des approches dépendra des niveaux de sensibilité des domaines de confiance d'une part et de la complexité des réseaux (et des flux qu'ils véhiculent) d'autre part.

Préconisations :

- Il est recommandé d'appliquer un contrôle d'accès restrictif vis-à-vis de réseaux externes (accès Internet, accès de certains partenaires, accès nomades, accès WIFI...) et un contrôle d'accès permissif pour les réseaux internes (réseaux bureautiques, réseaux de production non sensibles). Certains réseaux internes peuvent néanmoins faire l'objet d'un contrôle d'accès restrictif si leur niveau de sécurité le réclame (réseaux d'administration des équipements de sécurité, par exemple).

RES-07 Point d'Accès et de Contrôle Externe

Tout flux transitant entre les réseaux interne et externe doit transiter par un **Point d'Accès et de contrôle Externe (PAE)**, conformément au principe de cloisonnement :

- Lorsque les flux externes sont issus de réseaux non sûrs, ils sont soumis à un contrôle d'accès restrictif et un principe de rebond doit être mis en place. Néanmoins, dans le cadre d'un partenariat et sur avis favorable du RSSI s'appuyant sur un audit de sécurité démontrant l'absence de risque pour le SI de PE, ces exigences pourraient être revues à la baisse.
- Lorsque les flux externes sont issus de réseaux sûrs, un contrôle d'accès permissif sur avis favorable du RSSI est conforme à la politique de sécurité.

La mise en place d'un **PAE** réclame l'accord du RSSI. Son nombre est limité au strict minimum.

La configuration d'un **PAE** doit permettre l'interruption sélective ou globale des flux acheminés, en cas de défaillance d'un équipement, de présomption d'intrusion ou d'infection virale.

Dans le cadre de multiplication de **PAE**, un même niveau de sécurité est exigé sur l'ensemble de ces équipements.

Commentaires :

Dans le cas de flux externes issus de réseaux non sûrs, et à chaque fois que cela est possible, un principe de rebond doit être mis en œuvre entre le **réseau non sûr** et le **réseau sûr**.

Préconisations :

- Dans le cadre d'échange de fichiers, seuls les clients du **réseau sûr** doivent être à l'initiative des accès aux données déposées sur le relais depuis le **réseau non sûr**. Les données déposées font l'objet de contrôles (codes malveillants...).
- Tout flux ne pouvant répondre pour des raisons techniques au principe de rebond doit faire l'objet d'une démarche dérogatoire. Par ailleurs, ce type de flux est régulièrement réexaminé afin de s'assurer qu'il puisse, compte tenu des évolutions, se conformer au principe de rebond ou, en revanche, qu'il soit remplacé par un flux plus adapté. Une fréquence *a minima* annuelle est recommandée.
- Les dispositifs de filtrage du **PAE** doivent :
 - Masquer et concentrer les ressources internes (utilisateurs) derrière un composant central concentrant les accès face à l'extérieur,
 - Limiter la visibilité des réseaux internes aux seules ressources autorisées à être accédées,
 - Détecter les usurpations d'adresses des accédants (**antispoofing**).

Au-delà des contrôles réseaux, les flux font l'objet :

- D'un contrôle d'accès logique, lorsqu'ils sont à destination de ressources non publiques,
- D'un filtrage de contenu pour bloquer les codes malveillants et les informations illicites ou non sollicitées, conformément aux exigences légales, réglementaires et internes.

RES-08 Interconnexion des SIE avec Internet

Lorsque le SIE requiert une interconnexion sur le réseau externe, tous les flux doivent transiter par un PAE (point d'accès externe), comme précisé à la règle "Point d'Accès et de Contrôle Externe", afin de respecter les principes de cloisonnement vis-à-vis des réseaux non sûr et bénéficier des mesures de protection en place conformément au principe de défense en profondeur.

Commentaires:

Les mesures de protections énoncées par l'ANSSI dans son document "« Recommandations relatives à l'interconnexion d'un système d'information à Internet »" sont couvertes par le Point d'Accès Extérieur (DMZ, filtrage, translation d'adresse, sonde de prévention d'intrusion, antispoofing, anti DDOS, lutte contre les logiciels malveillants,...etc.).

4.2.2. Confidentialité des données

RES-09 Confidentialité des échanges sur le réseau Interne

Les données d'authentification doivent transiter systématiquement dans un canal de communication sécurisé.

Pour tous autres types de données échangées, les mécanismes de sécurité doivent s'adapter selon la sensibilité des informations véhiculées et du niveau de confiance de la zone du réseau utilisée.

Commentaires :

En dehors des données d'authentification, toutes données personnelles échangées sont des données sensibles et doivent transiter dans un canal de communication sécurisé. Pour des données autres que personnelles, un besoin de sécurité sur le critère de la confidentialité pourra être exprimé dans le cadre d'un projet (expression de besoin, analyse de risque projet,...) pour lequel des mesures de sécurité devront répondre.

RES-10 Confidentialité des échanges depuis un réseau Externe

Les communications entrantes (authentification et échange de données) doivent transiter dans un canal de communication sécurisé assurant la confidentialité de toutes les données échangées.

Préconisations :

Les communications doivent s'effectuer selon un protocole chiffré et authentifié (utilisation de [TLS](#)) ou s'appuyer sur un chiffrement de type tunnel si le protocole ne permet pas le chiffrement de bout en bout. »

RES-11 Algorithme de chiffrement

L'algorithme de chiffrement utilisé pour assurer la confidentialité des données doit répondre aux exigences suivantes :

- Absence de vulnérabilités connues,
- Avoir une robustesse au déchiffrement supérieur à 12 mois avec une puissance de calcul actuellement mobilisable.

Préconisations :

A l'heure de la rédaction de ce document,

- Le mécanisme de hachage SHA-256 est conforme au Référentiel Général de Sécurité.
- L'algorithme de chiffrement [AES](#) par bloc est conforme au Référentiel Générale de Sécurité

4.2.3. Accès au réseau interne

4.2.3.1. Connexion au réseau IP filaire de l'entreprise

RES-12 Équipements autorisés

Seuls les équipements maîtrisés et labellisés PE sont autorisés à se connecter physiquement sur le réseau de l'entreprise.

Commentaires :

- La définition d'un équipement maîtrisé et labellisé est définie au sein de la thématique « *Environnement de travail fixe* » [2].
- La connexion d'un équipement sur le réseau Interne doit respecter les règles de sécurité décrites au sein des thématiques correspondantes suivantes :
 - EDT-Fixes [2]; EDT-Mobiles [3]; EDT-Bornes [4]; EDT-Supports amovibles [5]
 - Accès au SI de PE par des tiers [6].→ Toutes autres connexions au réseau IP filaire de l'entreprise sont interdites.

RES-13 Équipements connectés en zones publiques

Tout équipement présent en zone publique où sa connectivité filaire est accessible, requiert une authentification forte pour accéder au réseau IP de l'entreprise.

Commentaires :

- L'authentification de l'équipement est une mesure permettant de se prémunir contre les tentatives d'usurpations des connexions physiques par des matériels pirates.

Préconisations :

- Mise en œuvre d'une authentification [802.1x](#) autorisant la connectivité de l'équipement sur le réseau physique de l'entreprise.

4.2.3.2. Connexion au réseau IP sans fil de l'entreprise

RES-14 Point d'accès sans fil

Toute utilisation de réseaux sans fil n'est pas autorisée *a priori*, à l'exception des réseaux installés par la DSI. Des mécanismes de sécurité appropriés, conformes à l'état de l'art et à l'architecture définie dans les SI, sont mis en œuvre afin de garantir la confidentialité des données échangées.

Préconisations :

- En l'état actuel, l'usage de l'algorithme de chiffrement et de contrôle d'intégrité CCMP (utilisé par WPA2), basé sur l'algorithme de chiffrement par bloc AES est à privilégier.

RES-15 Authentification sur les Points d'accès sans fil de l'entreprise

La connexion sur le point d'accès sans fil permettant d'accéder aux ressources internes du SI est soumise à une authentification forte de l'accédant.

Néanmoins, le degré du niveau d'authentification pourra être inférieur dans les cas suivants :

- Pour l'accès d'un terminal mobile géré par une solution centralisée de type MDM (Mobile Device Management).
- Pour l'accès d'un terminal à un ensemble limité et identifié de ressources internes, pour lesquelles une analyse de risque doit être menée et fournie au RSSI.

Commentaires :

- Lorsque l'usage du point d'accès sans fil ne permet pas d'atteindre le SI interne de l'entreprise, l'authentification sur celui-ci n'est pas nécessaire. L'authentification sur les outils de communication utilisées, décrite au sein de la thématique Outils de Communication Électronique » reste néanmoins requise.

RES-16 Protection contre les attaques par émission de radiofréquences

Les points d'accès sans fil déployés doivent intégrer des mécanismes de sécurité permettant de lutter contre les attaques par émission de radiofréquences (ou attaque par « brouillage »).

Préconisation :

- Tout nouvel équipement doit être soumis à un droit de regard en termes d'utilisation de radio fréquence afin de préserver la continuité de service des équipements WiFi de France Travail.

4.2.4. Accès aux ressources internes du SI

RES-17 Population autorisée

L'accès aux ressources internes hébergées sur les systèmes d'information de France Travail n'est autorisé qu'aux agents de France Travail et à ses **tiers** ayant signé une charte de sécurité d'accès au SI et un engagement individuel de confidentialité.

Seules les ressources exposées en frontière du SI peuvent être accédées par tout autre utilisateur ou application interconnectée.

Commentaires :

- Charte d'engagement individuel de confidentialité [6]
- Charte de sécurité d'accès au SI de PE par des tiers [7].
- Les accès réseaux offerts aux invités ou à toutes personnes étrangères à France Travail, depuis les locaux de France Travail, pour accéder aux services exposés ou pour l'usage d'un outil de communication électronique ne doivent en aucun cas permettre d'accéder aux ressources du SI hébergées sur le réseau interne de l'entreprise.

Préconisations :

- L'étanchéité des ressources internes lors de l'utilisation du réseau IP par des personnes étrangères à France Travail peut être garantie par l'usage de VLAN (Virtual Area Network).

RES-18 Contrôle d'accès et de conformité depuis un réseau Externe

L'accès aux ressources internes de l'entreprise, par un agent de France Travail ou un **tiers** ayant signé la charte de sécurité d'accès au SI de FT, doit transiter par une solution sécurisée, labellisée, mise à disposition par la DSI, contrôlant le niveau de conformité de l'équipement accédant.

Les mises à jour de sécurité doivent pouvoir être diffusées et installées sur l'équipement. En cas de non-conformité, la demande de connexion est refusée.

Une authentification forte des utilisateurs accédant est requise, et sur la base de leur identité, un profil de connexion est appliqué afin de maîtriser les services accessibles et les flux autorisés.

La confidentialité des échanges nécessite l'établissement de communications sécurisées.

Commentaires :

Les profils de connexion suivants selon l'identité de l'accédant :

- Pour les utilisateurs externes (partenaires, mainteneurs, ...), des profils restreints dans le cadre desquels seules certaines applications non **sensibles** sont autorisées d'accès,
- Pour les utilisateurs internes de France Travail, un profil sans limitation. Dans ce cadre, l'utilisateur est connecté comme s'il était branché sur le réseau interne.

4.3. RÈGLES RELATIVES À L'EXPLOITATION ET À LA SURVEILLANCE DES RÉSEAUX

4.3.1. Qualité et continuité de service

RES-19 Engagements de service

Les engagements de niveau de service des réseaux, en termes de taux de disponibilité, délai de rétablissement, niveau de performance, sécurité, doivent être établis et documentés.

Dans le cadre de prestations délivrées par un tiers (opérateur télécoms, fournisseur d'accès Internet...), ces engagements sont formalisés explicitement dans les contrats.

Commentaires :

Les contrats de prestation établis avec les opérateurs pourront également prévoir des clauses de sécurité complémentaires :

- Engagement sur la confidentialité des informations délivrées par la DSI (structure des réseaux, emplacements de sites...) ainsi que sur la confidentialité et l'intégrité des informations véhiculées par leurs réseaux d'interconnexion.

RES-20 Qualité de service

Les services d'administration et d'exploitation réseau doivent garantir la qualité de service attendue par leurs clients, partenaires et collaborateurs. A cette fin, des moyens de surveillance permanents de l'état et de l'usage du réseau doivent être mis en œuvre pour permettre :

- Un traitement rapide des incidents, d'une part,
- Une planification des ressources et des capacités réseaux, d'autre part.

Les services d'administration et d'exploitation réseau doivent assurer un suivi historique et statistique des incidents d'exploitation survenant sur les réseaux. Ces éléments doivent être exprimés dans le cadre de tableaux de bord et doivent pouvoir être mis à la disposition du RSSI.

RES-21 Disponibilité des infrastructures réseaux

Des procédures doivent être mises en place pour permettre une reprise après une défaillance du réseau, sans atteinte à la sécurité.

Dans tous les cas, les moyens de secours doivent permettre de répondre aux exigences de continuité de service exprimées par les métiers conformément au document thématique « Plan de secours informatique » [9].

Préconisations :

Pour les réseaux supportant des flux particulièrement sensibles comme défini au sein de la thématique « Classification et protection de l'information » [8]), une redondance des infrastructures et des médias de communication est conseillée.

4.3.2. Administration et supervision des réseaux

RES-22 Formalisation et maintien des schémas d'interconnexion

L'architecture globale des infrastructures réseaux de France Travail – comprenant notamment les réseaux locaux, métropolitains et d'interconnexion, les réseaux WAN, les réseaux Ethernet -SAN, les moyens de raccordement, de cloisonnement et de sécurisation de ces réseaux – doit faire l'objet d'une formalisation (schémas d'architecture, schémas des réseaux d'interconnexion...).

Cette formalisation est réalisée et maintenue à jour par les responsables opérationnels des infrastructures réseau concernées.

RES-23 Documentation technique

Les informations consignait les règles de sécurité opérationnelles réseau (cloisonnement, mesures de protection, règles de filtrage et de routage...) et la cartographie de répartition des ressources sont documentées et les documents sont régulièrement mis à jour.

Ces documents sont classifiés de niveau « Confidentiel » et doivent être protégés conformément à leur niveau de classification.

Leur accès est restreint au seul personnel habilité.

RES-24 Plan d'adressage interne

Le plan d'adressage IPV4 interne est défini conformément à la RFC 1918, permettant que les adresses internes ne soient pas visibles depuis Internet.

Chaque identifiant réseau (adresse MAC, IP, etc..) doit être unique.

Tout document traitant du plan d'adressage interne est confidentiel et doit être protégé en conséquence.

Préconisations :

Les équipements doivent être configurés conformément aux règles d'adressage IP définies pour le réseau interne.

RES-25 Confidentialité des flux d'administration et de supervision

L'administration et la supervision des équipements de sécurité réseau doivent s'opérer au travers de communications sécurisées garantissant la confidentialité des données échangées.

La mise en place d'un LAN d'exploitation dédié à cet effet *a minima* pour les équipements positionnés en DMZ est requise.

Les flux d'administration doivent être chiffrés s'ils transitent sur des réseaux non dédiés à l'administration.

Commentaires :

Les flux d'administration et de supervision réclament un niveau élevé de confidentialité et nécessitent de transiter au travers de sessions sécurisées.

Préconisations :

- Les outils de supervision doivent être positionnés dans une zone de confiance.
- En cas de besoin de chiffrement, l'utilisation des protocoles sécurisés à l'état de l'art sera privilégiée.

RES-26 Usage des outils d'administration et de supervision

L'utilisation des outils d'administration, de supervision, de surveillance et de diagnostic réseau doit être limitée au seul personnel habilité et formé. Ces outils ne doivent pas être laissés sans surveillance.

L'accès à distance à ces interfaces doit requérir une authentification nominative, renforcée, se faire via des sessions protégées avec journalisation des accès.

Commentaires :

Seul le personnel en charge de l'exploitation et de la supervision du réseau de télécommunication est habilité à utiliser ces outils.

RES-27 Politique des flux du LAN d'exploitation

Une politique des flux, tenue à jour par les personnels et équipes habilités est mise en place sur le LAN d'exploitation garantissant l'intégrité des ressources hébergées en DMZ.

Commentaires :

Les communications d'une zone vers une autre zone sont autorisées après validation du RSSI.

RES-28 Raccordement d'équipements réseau

Seuls les équipements de communication réseau testés, validés et répertoriés par le personnel habilité peuvent être connectés au réseau interne.

L'utilisation de matériel réseau non agréé est interdite. Une procédure de contrôle doit être mise en œuvre et la découverte d'équipements de ce type doit faire l'objet d'un plan d'actions sécurité contenant des recommandations à mettre en œuvre.

RES-29 Double raccordement d'un équipement

Le raccordement d'un équipement simultanément au réseau interne et à tout autre réseau sans passer par les points d'accès de contrôle mis en place est interdit.

Commentaires :

L'interdiction du double raccordement d'un équipement en dehors des points d'accès et de contrôle concerne notamment :

- La télémaintenance via modem lorsque aucune autre alternative n'est possible,
- Les équipements multifonctions (scanner, imprimante, photocopieur intégrant des fonctionnalités d'échange électronique par mail...) potentiellement connectés à la fois au Réseau Interne et au RTC (Réseau Téléphonique Commuté).

RES-30 Journalisation des événements de sécurité

Des mécanismes et procédures de journalisation et d'archivage des journaux doivent être définis pour les équipements réseau.

Pour les points d'accès et de contrôle externes (PAE), les éléments suivants doivent être journalisés :

- Les événements liés à la gestion des équipements,
- Les événements liés à la gestion des flux,
- Les événements liés aux accès distants

Commentaires :

Concernant la gestion des équipements, les événements suivants peuvent être journalisés : tentatives de connexions, redémarrages, alertes de sécurité, anomalies, changements, modifications – en spécifiant l'auteur et le but de la modification...

Concernant la gestion des flux, les événements suivants doivent être journalisés : flux rejetés, flux autorisés dans des cas spécifiques qui le nécessitent à au moins un point de la chaîne de liaison.

Concernant les accès distants, les éléments suivants doivent être journalisés : identifiants de l'utilisateur, date/heure de connexion, durée de connexion...

La journalisation des événements sur le PAE doit couvrir a minima une période semestrielle.

Pour assurer une journalisation cohérente entre tous les équipements et faciliter une corrélation d'événements de sécurité, il est nécessaire d'assurer régulièrement la synchronisation des horloges sur un référent unique.

Les journaux enregistrant les événements générés par les ressources des systèmes d'information d'administration ne doivent contenir aucun mot de passe ou autre élément secret d'authentification en clair ou sous forme d'empreinte cryptographique

Recommandations :

Il est recommandé de mettre en place un système centralisé de gestion des journaux d'événements. Ainsi, l'exploitation des événements collectés et la détection d'incidents de sécurité seront facilitées.

RES-31 Contrôle

Un plan de contrôle doit être mis en place et les contrôles conduits conformément au plan de contrôle SSI.

Commentaires :

Les contrôles peuvent, porter sur les flux, les journaux d'évènements, les mises en production d'équipements réseaux, la continuité de service des liens externes et internes...

4.3.3. Exploitation des flux externes

RES-32 Demande d'ouverture de flux externe entrant ou sortant

Toute demande d'accès externe aux réseaux doit être soumise à une autorisation préalable délivrée par l'instance désignée par le RSSI : l'Administration et l'Exploitation des infrastructures de communication réseau.

Les autorisations de connexion sont fondées sur l'analyse des risques induits par les réseaux accédants et accédés.

Commentaires :

Les demandes d'accès externes doivent être formulées au moyen des formulaires et procédures d'ouverture de flux prévus à cet effet.

Ces procédures et formulaires sont maintenus et diffusés par l'instance désignée par le RSSI à tous les acteurs concernés.

Tout projet demandeur d'accès externes doit établir un dossier de spécification comportant les aspects sécurité (cahier des charges réseau) comprenant, notamment :

- Une description fonctionnelle de l'application souhaitant établir une communication entre les réseaux internes et les réseaux externes,
- Une description technique des flux et des moyens nécessaires,
- Une analyse des risques induits par le contexte de mise en œuvre des accès externes associés,
- Une présentation de l'architecture permettant de répondre aux risques identifiés,
- Un recensement des risques résiduels.

Ce dossier doit faire l'objet d'une validation formelle par l'instance désignée par le RSSI pour application (l'Administration et l'Exploitation des infrastructures de communication réseau).

RES-33 Ouverture de flux sensible

Toute ouverture de flux non encore référencée et classifié de « sensible » par l'instance désignée par le RSSI : l'Administration et l'Exploitation des infrastructures de communication réseau, nécessite une demande particulière adressée à la filière sécurité en joignant une analyse de risque correspondante pour aide à la décision.

Commentaires :

Une description du risque à autoriser l'ouverture du flux doit être transmise par l'entité en charge de l'administration et l'exploitation des infrastructures de communication réseau, au RSSI pour en obtenir son accord.

RES-34 Filtrage des flux sur contrôle d'accès restrictif

Il est nécessaire de mettre en place plusieurs niveaux de filtrage pour garantir l'acheminement des seuls flux autorisés. Des règles spécifiques seront mises en œuvre concernant leurs contrôles (émetteur, destinataire, flux), notamment :

- L'interdiction de symétrie (A est autorisé à accéder à B $\Rightarrow$ B n'est pas implicitement autorisé à accéder à A.),
- L'interdiction de transitivité (A est autorisé à accéder à B, B est autorisé à accéder à C $\Rightarrow$ A n'est pas implicitement autorisé à accéder à C.).

Les Projets doivent mentionner explicitement leurs besoins en termes d'ouverture et de fermeture de flux aux acteurs en charge des infrastructures réseaux et des moyens de cloisonnement associés.

Commentaires :

La granularité des filtrages (plages d'adresses, gammes des protocoles...) doit être proportionnée aux risques associés aux domaines de confiance et rester exploitable par les équipes en charge de leur gestion.

Le filtrage ne doit pas se substituer aux autres mécanismes de contrôle intervenant à un niveau autre que la couche réseau.

Les responsables des ressources ou services ont en charge de demander toute mise à jour ou suspension des filtrages exercés à destination de leurs ressources ou services (dans le respect des règles de sécurité).

RES-35 Filtrage des flux pour les SIE

Au sein d'un SIE, un mécanisme de filtrage doit être mis en place permettant de limiter la circulation des flux, aux seuls flux de données nécessaires à son fonctionnement et sa sécurité.

Les flux entrants et sortants des SIE ainsi que les flux entre sous-systèmes des SIE doivent être filtrés au niveau de leurs interconnexions.

Les flux non conformes doivent être bloqués par défaut.

Commentaires :

Des contrôles d'accès restrictif (tout est interdit sauf ce qui est explicitement autorisé doivent être définis au niveau des interconnexions des SIE afin de maîtriser la circulation des flux au sein des SIE.

Ces règles de filtrage comprennent notamment :

- Un filtrage sur les adresses réseau ;
- Un filtrage sur les protocoles ;
- Un filtrage sur les numéros de port ;
- Etc.

Une liste des règles de filtrage en place ou supprimées depuis moins d'un an doit être tenue et mise à jour. Cette liste doit indiquer pour chacune des règles :

- Le motif et la date de la mise en œuvre, de la modification ou de la suppression de la règle ;
- Les modalités techniques de mise en œuvre de la règle.

RES-36 Révision des contrôles d'accès restrictifs

Les contrôles d'accès restrictifs doivent être régulièrement mis à jour. Par ailleurs, ils doivent être systématiquement revus à l'occasion de livraisons de nouveaux services applicatifs ou à l'arrêt de services existants.

Préconisations :

Une fréquence semestrielle (voire trimestrielle) est préconisée pour la révision des contrôles d'accès restrictifs. Cette révision donne notamment lieu à l'identification des règles inutilisées, à leur examen avec les responsables des ressources ou services concernés et leur éventuelle révocation.

Commentaires :

Des examens ponctuels peuvent également être réclamés par les organes de contrôle/d'audit interne et externe.

5. ANNEXES

5.1. GLOSSAIRE

802.1x	Solution d'authentification mise en place par IEEE. Elle permet l'authentification avant l'accès à tout type de réseau 802, filaire ou non (Ethernet, WLAN...). 802.1x repose sur le protocole EAP (Extensible Authentication Protocol).
Adresse MAC	Media Acces Control (MAC). L'adresse MAC est l'adresse physique d'un équipement se connectant sur un réseau informatique. Elle est unique mondialement.
AES	Advanced Encryption Standard (AES). Il s'agit d'un algorithme de chiffrement symétrique par bloc de 128 bits.
Antispoofing	Mécanisme, dans un pare-feu par exemple, qui permet de détecter qu'un paquet IP a été spoofé. Le spoofing est une méthode qui permet d'envoyer des paquets IP avec une adresse usurpée pour faire croire qu'ils viennent d'une adresse autorisée.
ATM	ATM : Asynchronous Transfert Mode. Technologie réseau, apparue au début des années 1990, gérant le transport de la voix, de la vidéo aussi bien que celui des données en garantissant une qualité de service.
Authentification forte	Une authentification forte est définie comme requérant deux éléments : ■ Quelque chose que l'utilisateur possède (une carte à puce, un <i>token</i> qui génère un code automatique à durée de vie limitée), ■ Un secret que l'utilisateur connaît et qui n'est pas partagé par d'autres personnes (un mot de passe, un pin code, etc....).
CCMP	Counter-Mode/CBC-Mac protocol (CCMP). Il s'agit d'un protocole de chiffrement assurant la gestion des clés et l'intégrité des messages. Il est basé sur l'utilisation de l'algorithme de chiffrement AES.
Déni de Service	En anglais « Denial of Service » (DoS). C'est une attaque dirigée vers un système pour réduire ou bloquer entièrement le niveau de sécurité offert à ses utilisateurs. Les attaques par « Déni de service distribué » (DDoS) sont caractérisées par la participation de plusieurs systèmes attaquants.
DHCP	Dynamic Host Control Protocol (DHCP). Protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP/IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau.

	DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).
DMZ	En anglais, DMZ signifie Demilitarized Zone. Les DMZ permettent une séparation dans les échanges entre l'extérieur et le réseau interne. Ce sont des zones de communications par lesquelles des personnes extérieures au réseau interne sont autorisées à consulter des informations déposées par des entités internes et éventuellement déposer des informations qui seront récupérées par des agents de France Travail.
DNS	Domain Name System (DNS). Protocole Internet permettant d'établir la relation entre une adresse IP et le nom Internet associé.
Domaine de confiance	Un domaine de confiance est un domaine dans lequel est défini un niveau de sécurité spécifique de telle manière que les données et ressources y appartenant soient protégées durant tout leur cycle de vie.
HTTP	HyperText Transmission Protocol (HTTP). Protocole pour la transmission des pages Web depuis un serveur vers un navigateur client.
HTTPS	HyperText Transfert Protocol Secure (HTTPS) : Protocole de transfert de données sécurisées sur le web.
IDS	Intrusion Detection System (IDS). Système assurant le contrôle du trafic réseau et alertant les administrateurs des tentatives d'intrusion ou de l'existence d'un trafic suspect.
IP	L'Internet Protocol, généralement abrégé IP, est un protocole de communication de réseau informatique par commutation de paquets. IP est le protocole d'Internet. IP est un protocole de niveau 3 du modèle OSI et du modèle TCP/IP permettant un service d'adressage unique pour l'ensemble des terminaux connectés.
IPS	Intrusion Prevention System (IPS). C'est un système qui permet de réagir aux intrusions en coupant les attaques qu'il connaît.
IPv4	Internet Protocol version 4 (IPv4). Une adresse IPv4 est codée sur 32 bits.
LDAP	Lightweight Directory Access Protocol (LDAP). Protocole d'accès normalisé aux services d'un annuaire (base de données avec une structure spécifique arborescente).
Maîtrise d'Ouvrage (MOA)	Dans le cadre d'un projet, la maîtrise d'ouvrage est une entité cliente exprimant le besoin fonctionnel.
Maîtrise d'Œuvre (MOE)	Il s'agit d'une entité chargée de la réalisation d'un projet, pour le compte de la MOA et qui respecte l'expression des besoins réalisée par celle-ci.
NAT	Network Address Translation (NAT). Mécanisme implémenté sur des routeurs et pare-feu permettant d'établir une table de correspondance entre les adresses IP externes (visibles) et celles utilisées sur le réseau interne. Les adresses du réseau local sont masquées par translation.

PAE	Point d'Accès et de contrôle Externe (PAE).
Pare-feu	Un pare-feu est un élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité.
Réseau externe	Le réseau externe désigne tout réseau autre que les réseaux locaux des sites et que les réseaux privés d'interconnexion entre ces sites.
Réseau interne	Le réseau interne désigne l'ensemble des réseaux locaux et des réseaux privés d'interconnexion entre les sites internes. Tout autre réseau est dit externe.
Réseau non sûr	Tout réseau IP non géré par le personnel de France Travail (réseau d'un partenaire, réseau Internet,...).
Réseau sûr	Il s'agit d'un réseau IP supervisé et administré par le personnel de France Travail en charge de ce périmètre.
RFC 1918	Il s'agit d'une bonne pratique définissant les plages d'adressage pour les réseaux privés. Elles sont réutilisables d'un réseau privé à un autre mais ne sont pas routables sur Internet.
RSSI	Responsable de la Sécurité des Systèmes d'Information.
RTC	Réseau Téléphonique Commuté (RTC). Réseau de téléphonie traditionnel délivré par un opérateur télécoms.
SAN	Storage Area Network (SAN). Réseau desservant les baies de stockage de données auxquelles sont raccordés les serveurs de production. Le réseau SAN est un réseau bâti autour de la technologie Fiber Channer (FC) et constitué, comme les réseaux IP, de routeurs et de commutateurs. Le réseau SAN peut être raccordé à des réseaux IP, soit pour son administration, soit pour assurer le transport de trames iSCSI ou FCIP.
Sensibilité	La classification des informations repose sur la notion suivante : le propriétaire d'informations classe ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.
Sensibilité « Sensible »	Une information est dite de sensibilité sensible, si, lors de sa classification, le propriétaire de cette information mesure un impact limité en cas d'atteinte à cette information pour les critères DICP que ce soit en termes de pertes financières, juridiques, pertes de confiance ou d'image, ou de désorganisation interne.
SIE	Un SIE (Système d'information essentielle) est un système d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.
SNMP	Simple Network Management Protocol (traduire protocole simple de gestion de réseau). Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.
SSH	Secure Shell. Protocole qui permet de se connecter à une machine distante avec une liaison sécurisée. Les données sont

	cryptées entre machines.
Telnet	Utilitaire permettant l'utilisation de programmes sur des machines distantes, via un réseau de type Internet.
Tiers	Le terme « Tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires employés à titre individuel par France Travail ; ces personnels sont amenés à travailler, de manière permanente ou occasionnelle, sur les Systèmes d'Information de France Travail et, de ce fait, à avoir accès à des informations ou à des ressources de France Travail.
TLS	Transport Layer Security (TLS). C'est un protocole utilisé pour sécuriser les échanges sur Internet. Il sécurise la couche Transport du modèle OSI (Open Systems Interconnection).
VLAN	Virtual Local Area Network (VLAN). Technologie réseau dont l'objectif est de scinder l'ensemble des composants réseaux en « sous-réseaux » selon des critères logiques (fonction, partage de ressources, appartenance à un département...), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié....)
VPN	Virtual Private Network (VPN). Réseau virtuel privé qui permet d'accéder au réseau de l'entreprise et de faire transiter des données à travers des réseaux publics de manière sécurisée en intégrant des moyens de chiffrement et d'authentification.
WPA2	Wi-Fi Protected Access (WPA2). Il s'agit d'un mécanisme pour sécuriser les réseaux WiFi imposant l'utilisation du protocole de chiffrement CCMP et de l'algorithme de chiffrement AES.

5.2. LISTE DES RÈGLES

RES-01	Interdiction des accès réseaux en dehors des points d'accès et de contrôle définis...	7
RES-02	Cloisonnement des réseaux en domaines de confiance	8
RES-03	Cloisonnement d'un système d'information essentiel.....	8
RES-04	Mutualisation de services d'infrastructure entre domaines de confiance	8
RES-05	Doublement des mécanismes filtrants entre domaines de confiance opposés	9
RES-06	Point d'Accès et de Contrôle	9
RES-07	Point d'Accès et de Contrôle Externe	10
RES-08	Interconnexion des SIE avec Internet.....	10
RES-09	Confidentialité des échanges sur le réseau Interne	12
RES-10	Confidentialité des échanges depuis un réseau Externe	12
RES-11	Algorithme de chiffrement.....	12
RES-12	Équipements autorisés	13
RES-13	Équipements connectés en zones publiques	13
RES-14	Point d'accès sans fil	14
RES-15	Authentification sur les Points d'accès sans fil de l'entreprise	14
RES-16	Protection contre les attaques par émission de radiofréquences	14
RES-17	Population autorisée	15
RES-18	Contrôle d'accès et de conformité depuis un réseau Externe.....	15
RES-19	Engagements de service	16
RES-20	Qualité de service	16
RES-21	Disponibilité des infrastructures réseaux.....	16
RES-22	Formalisation et maintien des schémas d'interconnexion.....	17
RES-23	Documentation technique	17
RES-24	Plan d'adressage interne.....	17
RES-25	Confidentialité des flux d'administration et de supervision.....	18
RES-26	Usage des outils d'administration et de supervision	18
RES-27	Politique des flux du LAN d'exploitation	18
RES-28	Raccordement d'équipements réseau	18
RES-29	Double raccordement d'un équipement	19
RES-30	Journalisation des événements de sécurité	19
RES-31	Contrôle	19
RES-32	Demande d'ouverture de flux externe entrant ou sortant.....	20
RES-33	Ouverture de flux sensible	20
RES-34	Filtrage des flux sur contrôle d'accès restrictif	21
RES-35	Filtrage des flux pour les SIE.....	21
RES-36	Révision des contrôles d'accès restrictifs.....	22

(Fin de document)