



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'intérieur

PGSN – A06

Sécurité des réseaux

Version 1.0

NON PROTEGE

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'intérieur (PGSN-MI).

Les principes stratégiques de la PGSN-MI et les dispositions générales de l'instruction sont traduits au sein du présent document en objectifs à atteindre, reprenant la structure de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E).

Des règles techniques ou non techniques permettant de contribuer à la réalisation de chaque objectif sont énoncées au sein du présent document :

- Les mesures préfixées par « PSSI-E », suivies de la nomenclature seule, sont des règles inchangées de la PSSI-E de 2014. Des modifications peuvent néanmoins y être effectuées sur l'appellation de certaines fonctions propres au ministère.
- Les mesures préfixées « MI- » sont des mesures venant préciser la règle originale ou définir des règles propres au ministère de l'intérieur, formulées par le SHFD.

Toute dérogation à un objectif ou une règle du présent document, doit se faire en conformité avec la règle [MI-ORG-PGSN-DEROG] du document [PGSN-A01] du corpus de la sécurité numérique.

Dans la suite du document, le terme « DSI ministérielles » regroupe la direction du numérique et le service des technologies et des systèmes d'information de la sécurité intérieure.

Sécurité des réseaux

1. Sécurité des réseaux nationaux

Objectif A6-1 : usage sécurisé des réseaux nationaux. Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

PSSIE-RES-MAITRISE : systèmes autorisés sur le réseau. Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité.

MI-RES-INTERCO : interconnexion avec des réseaux externes. Les interconnexions avec Internet, ou d'autres SI étatiques ou privés, passent obligatoirement à travers les passerelles nationales, opérées par les DSI ministérielles, et homologuées. Ces passerelles mettent en œuvre des traitements visant à s'assurer de l'innocuité des flux et la protection des informations.

MI-RES-CLOIS-DMZ : cloisonner les SI en zones de sécurité. Le cloisonnement physique ou logique limite le risque de propagation latérale d'une attaque au sein du système d'information ministériel. Le principe de cloisonnement impose :

- La séparation physique des systèmes ou sous-systèmes de niveaux de sensibilité différents ;
- La séparation logique de systèmes ou de sous-systèmes distincts du même niveau de sensibilité ;
- La création d'une zone de sécurité (DMZ) séparant par des fonctions de filtrage et de protection adaptées une application ministérielle d'Internet ou des systèmes d'information des autres administrations.

Dans tous les cas, les fonctions de sécurité comme la fonction de filtrage doivent être assurées par des équipements dédiés.

PSSIE-RES-ENTSOR : mettre en place un filtrage réseau pour les flux sortants et entrants. Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.

PSSIE-RES-PROT : protection des informations cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes. Les accès à Internet passent obligatoirement à travers les passerelles nationales. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.

2. Sécurité des réseaux locaux

Objectif A6-2 : usage sécurisé des réseaux locaux. Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

PSSIE-RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes. Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

PSSIE-RES-INTERCOGEO : interconnexion des sites géographiques locaux d'une entité. L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et validées par le HFD.

PSSIE-RES-RESS : cloisonnement des ressources en cas de partage de locaux. Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le HFD.

MI-RES-CLOIS-DIFF : cloisonnement différent selon le niveau de sensibilité. Un cloisonnement logique par VLAN étanches doit être mis en œuvre sur les réseaux locaux. A minima, les sous-systèmes suivants doivent être séparés : postes dédiés à l'administration, postes clients, postes élections, postes téléphoniques IP, serveurs, zones d'impression.

MI-RES-CLOIS-VLAN : étanchéité des VLAN. La mise en œuvre de VLAN contribue au cloisonnement logique des différents sous-systèmes au sein d'un réseau local. Seules les fonctions de commutation de paquets doivent être activées. En aucun cas, les VLAN ne doivent assurer des fonctions de routage.

MI-RES-CLOIS-ROUT : routage inter-VLAN. Les fonctions de routages et de filtrage inter-VLAN doivent être assurées par des équipements de filtrage de type pare-feu. Des règles de filtrage précises doivent être configurées et de manière à n'autoriser que les flux explicitement répertoriés.

MI-RES-ZONE-FILT: Filtrage et détection entre zone de sécurité. Tout flux entre deux zones réseau de niveaux de maîtrise différents doit faire l'objet d'un filtrage, via un sas de sécurité de niveau adapté aux risques induit par cette connexion. Il doit être également équipé d'un dispositif de prévention et de détection d'intrusion via une sonde d'un niveau de sécurité adapté, éventuellement qualifié.

MI-RES-FLUX-VAL: validation des ouvertures de flux. Les ouvertures de flux ou la mise en place de nouveaux services réseaux doivent être encadrées par un processus de validation prévoyant un contrôle aux bonnes pratiques de sécurité numérique.

MI-RES-CLOIS-ADMN : cloisonnement des réseaux d'administration. Un réseau d'administration ne doit pas permettre un accès simultané au réseau bureautique et de production afin d'éviter que la compromission d'un réseau n'affecte le second par effet de rebond.

3. Accès spécifiques

Objectif A6-3 : accès spécifiques. Ne pas porter atteinte à la sécurité du SI par le déploiement d'accès non supervisés.

PSSIE-RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité. Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation.

MI-RES-ARCHI-INTERNET : passerelle Internet utilisateur. Les accès internet utilisateurs à vocations professionnelle et personnelle, permettant une navigation Web, sont uniquement autorisés au travers de la plate-forme Orion et celle équivalente de la Gendarmerie Nationale. Toute navigation hors de ces passerelles nationales homologuées est interdite. Seuls les cas particuliers, dans le cadre de programmes ministériels, peuvent être envisagés après autorisation exclusive du SHFD.

4. Sécurité des réseaux sans fil

Objectif A6-4 : usage sécurisé des réseaux sans fil. Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

MI-RES-SSFIL : mise en place de réseaux sans fil. Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le HFD, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis les technologies radio.

À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles ou Diffusion Restreinte est proscrit.

5. Sécurisation des mécanismes de commutation et de routage

Objectif A6-5 : sécurité des mécanismes de commutation et de routage. Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

PSSIE-RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses. Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.

PSSIE-RES-ROUTDYN : surveiller les annonces de routage. Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

PSSIE-RES-ROUTDYN-IGP : configurer le protocole IGP de manière sécurisée. Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

PSSIE-RES-ROUTDYN-EGP : sécuriser les sessions EGP. Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type message-digest-key.

MI-RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services. Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut. Les mécanismes d'authentification à double facteurs doivent être privilégiés.

PSSIE-RES-DURCI : durcir les configurations des équipements de réseaux. Les équipements de réseaux (par exemple : les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

6. Cartographie réseau

Objectif A6-6 : cartographie réseau. Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

MI-RES-CARTO : élaborer l'architecture technique et fonctionnelle. L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au système d'information. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des systèmes d'information.

Dans la mesure du possible, des solutions de cartographie et de supervision du réseau seront mises en œuvre afin d'obtenir une vision fidèle et en temps réel des réseaux.