BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°44 du 21 octobre 2011

PARTIE PERMANENTE
Administration Centrale

Texte n°3

DIRECTIVE N° 20/DEF/DGSIC
portant sur l'architecture des réseaux internet protocol.

Du *24 août 2011*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 20/DEF/DGSIC portant sur l'architecture des réseaux internet protocol.

Du 24 août 2011

NOR D E F E 1 1 5 1 7 4 4 X

Pièce(s) Jointe(s) :

Une annexe.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°44 du 21 octobre 2011, texte 3.

SOMMAIRE

2.1.3. Plan de gestion.

2.2. Règles organisationnelles.

2.3. Règles sémantiques.

ANNEXE(S)

ANNEXE. GLOSSAIRE ET ACRONYMES.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Objet du document.**

La présente directive définit les règles applicables au sein du ministère de la défense pour l'architecture des réseaux internet protocol (IP) de défense. Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

1.2. **Niveaux de préconisation.**

Les règles présentées dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'interopérabilité (RGI) et à la request for comments (RFC) 2119 :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Gestion du document.**

Ce document est maintenu et mis à jour par le sous-comité architecture et services du comité directeur des intranets. Les modifications sont soumises pour approbation au directeur général des systèmes d'information et de communication.

Ce document est disponible sur le site DGSIC.

1.4. **Modalités d'application.**

La présente directive s'applique à l'ensemble des réseaux IP de défense. Elle concerne les aspects techniques et organisationnels.

Ces règles définissent la cible et sont applicables à tout nouveau projet ou toute évolution majeure concernant les réseaux IP de défense.

Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics.

1.5. **Gestion des dérogations pour les projets.**

Les dérogations sont présentées par un expert de haut niveau ou un directeur de projet au sous-comité architecture et services (SC2) qui statue sur la demande.

La commission ministérielle technique des systèmes d'information et de communication (CMTSIC) peut également être saisie en dernier ressort. Ces dérogations font l'objet d'une approbation par le directeur général des systèmes d'information et de communication. Elles concernent :

- les circonstances et justifications du non respect d'une règle recommandée ;

- les circonstances et justifications du non respect d'une règle déconseillée ;

- les justifications des exceptions à toute règle absolue (obligatoire ou interdit). Dans ce dernier cas, une instruction préalable des services de la DGSIC est nécessaire.

1.6. **Cadre documentaire.**

1.6.1. ***Documents applicables.***

RGS : référentiel général de sécurité, version 1.0 publiée au *Journal officiel* le 18 mai 2010 (www.ssi.gouv.fr).

IGI1300 : instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 23 juillet 2010 (1), relative à la protection du secret de la défense nationale (www.ssi.gouv.fr).

QoS : répartition des flux IP pour une offre de services différenciés (communicable sur demande au ministère de la défense), guide S-CAT n° 16003, version 2.2. du 13 décembre 2004 (1).

ARCHI : recommandations pour l'évolution des architectures réseaux sécurisées (communicable sur demande au ministère de la défense), DGA n° 2010-115947/TEC/ACS/17M2008, version 1.01. du 5 octobre 2010 (1).

SLA : périmètre des contrats de services applicables au sein du ministère de la défense (MINDEF) (communicable sur demande au ministère de la défense), guide SCAT n° 16009 Ed 01 du 29 juin 2007 (1).

1.6.2. ***Normes et standards applicables.***

L'ensemble des RFC relatives aux protocoles mentionnés dans ce document, en particulier IPv4, IPv6 et IPSec, est applicable.

1.6.3. ***Autres documents et sites de référence.***

Site DGSIC : site intranet défense DGSIC (www.dgsic.defense.gouv.fr) ;

RGI : référentiel général d'interopérabilité, version 1.0. publiée au *Journal officiel* le 12 juin 2009 ;

RFC 2119 : request for comments relative aux mots clés pour les niveaux d'obligation (mars 1997).

1.7. **Domaine couvert et emploi.**

1.7.1. ***Services attendus.***

Cette directive a pour objectif de définir une architecture cible pour les réseaux IP au profit du ministère de la défense ainsi que les moyens pour la mettre en place.

Cette architecture permet d'améliorer l'efficacité globale du service d'acheminement des flux IP du ministère en offrant une connectivité IP de bout en bout basée sur des réseaux :

- interconnectés entre eux au niveau IP ;

- exploités de façon rationalisée ;

- tirant profit des capacités apportées par des moyens patrimoniaux et des moyens non patrimoniaux [par exemple : opérateurs civils, organismes (Organisation du traité de l'Atlantique Nord (OTAN)), etc.].

1.7.2. ***Principes et définitions.***

1.7.2.1. Architecture cible.

L'architecture cible de cette directive repose sur le principe de la mutualisation des réseaux de transit élémentaires pour constituer un transit global.

Pour atteindre le but recherché, à savoir une amélioration de l'efficacité du service d'acheminement IP, cette interconnexion doit se faire en évitant le recours à des passerelles de sécurité ou du « surchiffrement ».

Cette architecture met en œuvre 3 composantes : les enclaves, les transits élémentaires et le transit global.

Une enclave est un ensemble de moyens traitant d'informations d'un niveau de classification maximum donné. Une enclave constitue un domaine de sécurité. Une enclave peut aussi bien être une emprise importante (un site entier, un bâtiment), qu'être très réduite (une salle, un local area network (LAN) isolé voire un poste de travail, un combattant).

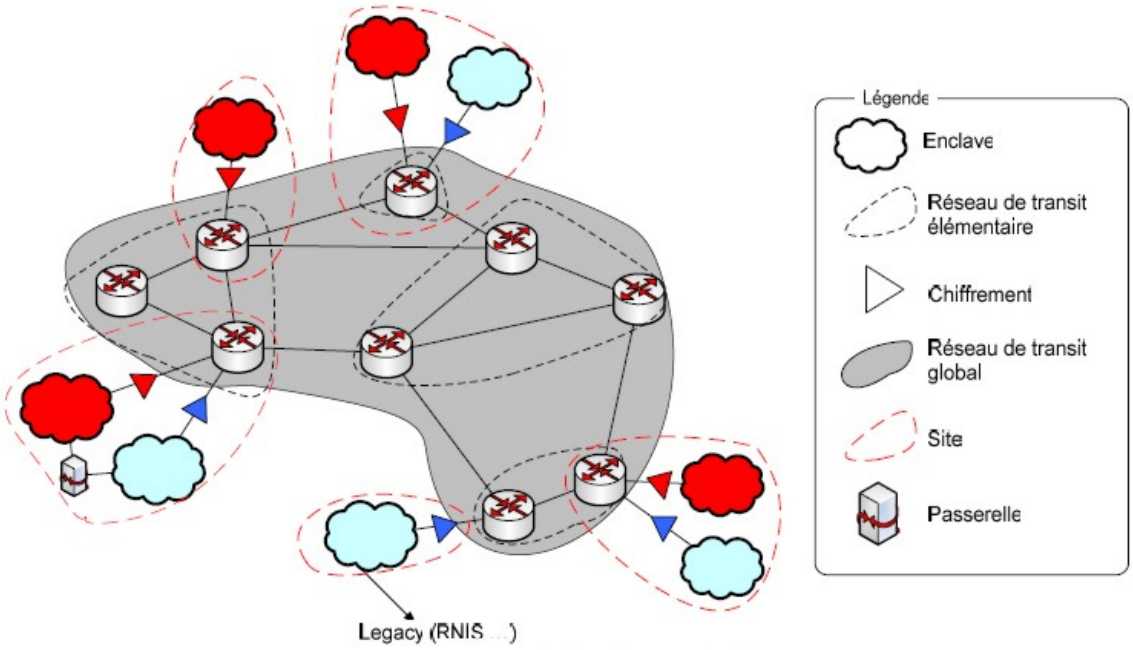
Un transit élémentaire est un ensemble de moyens (équipements, liaisons etc.) d'un même domaine de gestion, permettant l'acheminement de données entre différents points d'accès (enclave, point d'interconnexion). Les échanges aux points d'accès sont régis par des accords de service ; les réseaux de transit élémentaire (RTE) peuvent être des réseaux nationaux, des réseaux alliés ou des réseaux civils, de niveau stratégique, opératif ou tactique.

Le transit global est constitué de l'interconnexion de réseaux de transit élémentaires assurant le transport des paquets IP entre enclaves. Les relations entre transits élémentaires sont régies par des accords de service.

Afin que la mutualisation des réseaux de transit élémentaires n'induisent pas de risques supplémentaires, que ce soit pour la confidentialité des données transportées ou pour l'intégrité et disponibilité du réseau de transit global, l'architecture cible impose un chiffrement systématique des flux utilisateur ainsi qu'une sécurisation des réseaux de transit, tant aux interconnexions qu'en interne.

Les enclaves sont donc connectées aux réseaux de transit élémentaires par des moyens de chiffrement de niveau IP respectant la législation en vigueur. On constitue ainsi des réseaux privés virtuels (VPN) entre enclaves de même domaine de chiffrement.

Les passerelles ou *DeMilitarized Zone* (DMZ), utilisées pour interconnecter des domaines de sécurité différents, sont positionnées dans les enclaves qu'elles relient, et non en coupure des réseaux de transit.



Composantes de l'architecture cible

Le transit global est dit aconfidentiel, au sens où il ne véhicule que des flux utilisateur préalablement chiffrés au niveau IP [y compris pour le domaine non protégé (NP)] en sortie d'enclave (2). Ces flux ne sont donc plus porteurs d'aucun besoin de confidentialité.

Une telle architecture nécessitant le déploiement massif de moyens de chiffrement pour le niveau diffusion restreinte (DR), la définition de profils d'interopérabilité (chiffre et réseaux) pour ces moyens est recommandée afin de favoriser l'interopérabilité.

De même, l'adoption d'IPv6 favorise la construction d'un tel transit global, en garantissant une coordination native des plans d'adressage, évitant ainsi le recours à des mécanismes de traduction d'adresses IP (NAT).

Cette approche correspond aux orientations suivies par nos alliés (OTAN, etc.). Elle permet ainsi d'ouvrir des perspectives d'interopérabilité entre réseaux de différentes nations, en vue de la constitution de futurs réseaux IP de défense multinationaux, sans crainte pour la confidentialité des informations véhiculées par les différentes nations.

1.7.2.2. Accords de service.

Afin de formaliser les interactions entre réseaux de transit élémentaires d'une part et entre les utilisateurs et le transit global d'autre part, des accords de service de niveau réseau sont mis en œuvre pour :

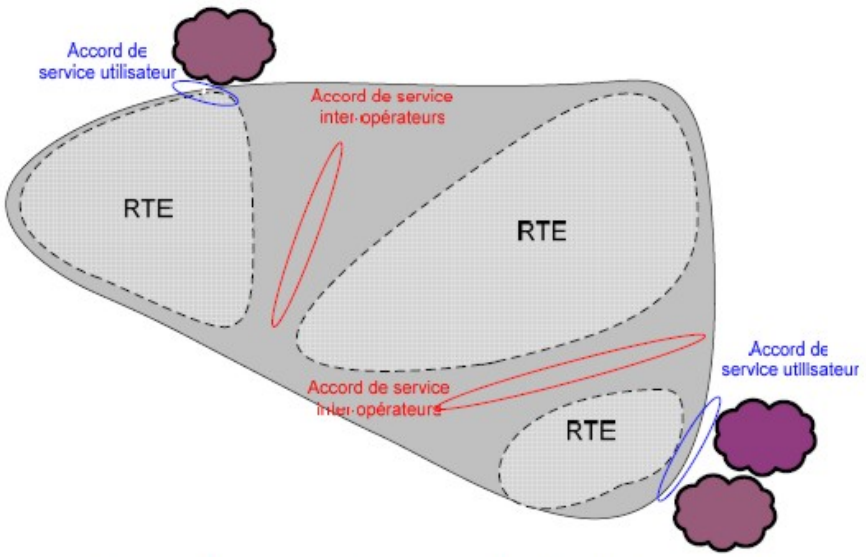
- clarifier les domaines de responsabilité ;

- expliciter les interfaces ;

- formaliser les caractéristiques du service attendu/fourni ;

- identifier les engagements sur la qualité du service : performance, disponibilité, moyens de soutien, sécurité etc.

L'accord de service définit en particulier la disponibilité attendue du réseau, dérivant de la disponibilité globale attendue des utilisateurs.



Position des contrats de service dans l'architecture cible

Les accords de service permettent de définir les flux pris en charge par les prestataires et leur coopération éventuelle en matière de signalisation (routage en particulier) et de gestion. Ces accords sont donc un maillon essentiel de la sécurité, car l'application d'une régulation conforme à ces accords permettra à un réseau de réduire sa surface d'exposition aux attaques.

1.7.2.3. Routage.

Pour assurer l'acheminement des paquets IP, le réseau de transit global réalise l'interconnexion de domaines de routage.

Un domaine de routage est constitué d'un ensemble d'équipements qui opèrent selon les mêmes procédures de routage. Il peut être divisé en sous domaines, permettant ainsi un routage hiérarchique facilitant le support de la mise à l'échelle.

Un même opérateur peut gérer plusieurs domaines de routage, mais un domaine de routage ne peut être géré que par un seul opérateur.

Ce découpage offre à chaque domaine de routage une certaine autonomie de gestion et de choix techniques.

La diffusion des routes entre domaines s'appuie sur un protocole de routage externe, dont les règles d'implémentation feront l'objet d'une directive.

1.7.3. ***Périmètres et limites.***

L'architecture cible, et donc les règles du point 2., ne concernent que la couche IP et ne présument ni des couches inférieures, c'est-à-dire des réseaux supports (radio, satellite, filaire, etc.), ni des couches supérieures, c'est-à-dire des protocoles de transport (TCP etc.) et des applications (voix, vidéo, etc.).

Les règles du point 2. portent principalement sur le réseau de transit global IP. L'architecture des enclaves ainsi que des passerelles ne relèvent pas du périmètre de la présente directive.

2. LES RÈGLES.

La mise en œuvre des principes décrits dans le paragraphe précédent nécessite de respecter un certain nombre de règles à la fois techniques et organisationnelles.

L'objectif de ces règles est de définir :

- des interfaces communes facilitant l'interopérabilité et la reconfigurabilité de l'ensemble ;

- les fonctions de sécurité nécessaires au maintien de l'intégrité du transit global.

Le cadre général défini par ces règles est ou sera complété par des directives plus spécifiques concernant la qualité de service, IPv6 ou le routage.

2.1. **Règles techniques.**

Les règles techniques sont présentées selon trois plans :

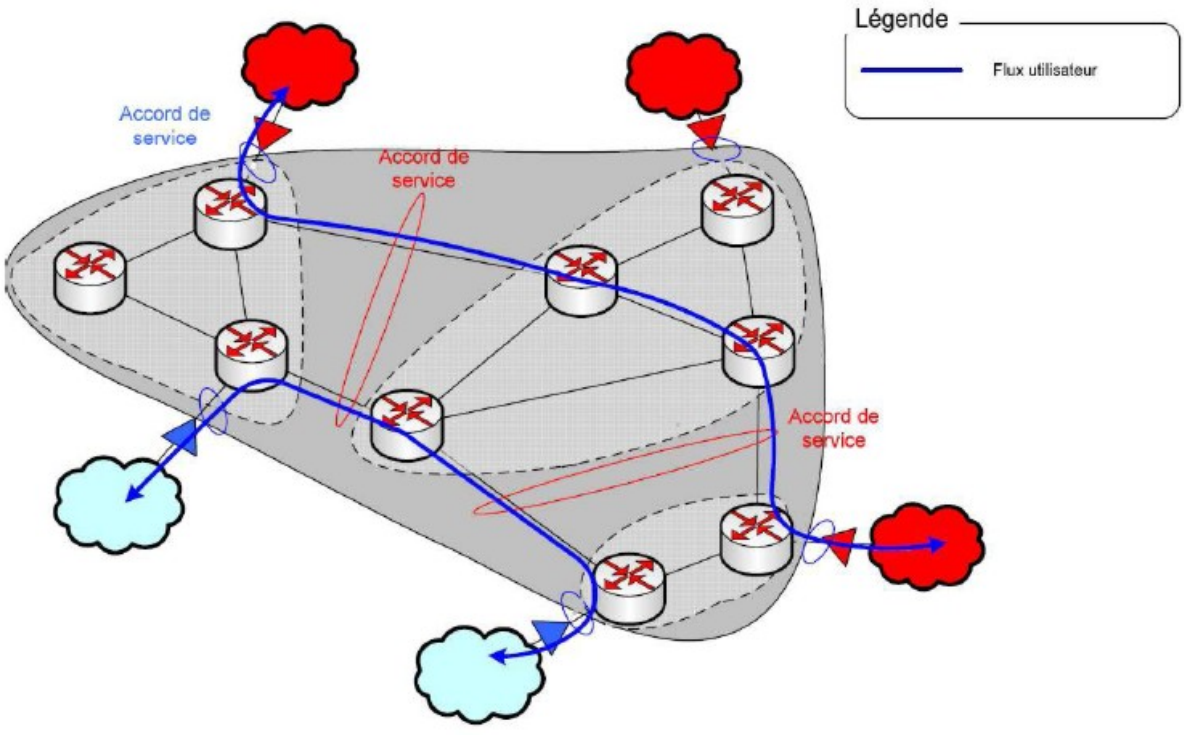
- le plan utilisateur, qui réalise le transit des informations entre enclaves, sous la forme de paquets IP ;

- le plan de contrôle, qui regroupe l'ensemble des échanges de signalisation entre équipements réseaux afin d'établir et de maintenir le service de transit (il s'agit des protocoles de routage, réservation de ressources, échange de clés etc.) ;

- le plan de gestion des réseaux, qui assure la supervision et l'administration du réseau depuis un ensemble de postes dédiés.

*2.1.1. **Plan utilisateur.***

La figure ci-dessous illustre le plan utilisateur pour l'architecture cible.



Plan utilisateur

RT 01 : il est obligatoire que les flux utilisateur soient chiffrés au niveau IP en sortie d'enclave.

Précision : même les flux utilisateur du domaine NP sont chiffrés entre enclaves du ministère de la défense : le respect de cette règle permet d'assurer la protection de l'infrastructure du réseau IP de transit vis à vis des trafics NP qui peuvent provenir d'internet.

Cette règle considère comme acquis que les enclaves disposent par ailleurs de mécanismes adaptés au niveau des informations manipulées dans les enclaves.

Les flux utilisateur étant chiffrés, le transit peut être considéré comme aconfidentiel.

RT 02 : il est obligatoire de filtrer et réguler (3) les flux utilisateur aux interfaces réseau de transit élémentaire (RTE)-RTE et RTE-Enclave en conformité avec les accords de service.

Précision : ceci doit également permettre de limiter l'efficacité d'attaques en déni de service en limitant les flux à acheminer.

RT 03 : il est obligatoire que le differentiated services code point (DSCP) des paquets IP soit marqué conformément à la directive (QoS).

RT 04 : il est recommandé que le DSCP des paquets IP ne soit pas modifié par les réseaux de transit traversés.

RT 05 : il est recommandé de ré-encapsuler les datagrammes IP dans un autre datagramme IP lors de la traversée d'un réseau modifiant le DSCP des paquets IP.

Précision : le datagramme initial peut ainsi être récupéré en sortie d'un réseau non conforme et poursuivre son acheminement, conformément au DSCP initial à travers les autres réseaux conformes traversés.

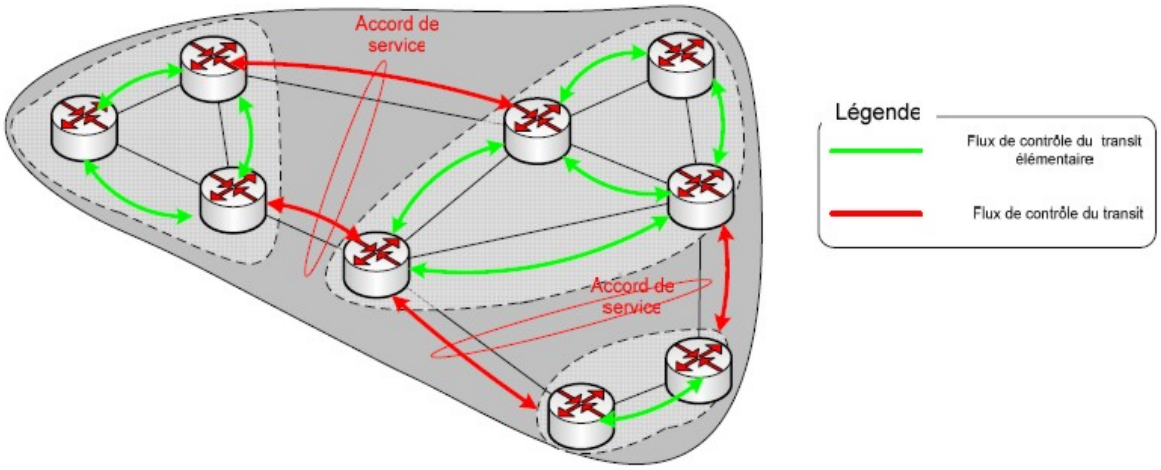
RT 06 : il est recommandé que le réseau de transit global ait un plan d'adressage assurant un maximum de cohérence entre les préfixes d'adresses et la topologie réseau (et par conséquent, les zones géographiques correspondantes).

Précision : dans le cas contraire, une forte incohérence entre les préfixes d'adresses et les zones géographiques correspondantes entraînerait une surcharge de signalisation de routage (diffusion de préfixes détaillés différents et donc non facilement agrégeables au sein du réseau pour desservir une même zone géographique) et une utilisation non optimale des ressources mémoire des routeurs.

RT 07 : il est déconseillé d'avoir recours à la traduction d'adresses network address translation (NAT).

2.1.2. ***Plan de contrôle.***

La figure ci-dessous illustre le plan de contrôle pour l'architecture cible.



Plan de contrôle

RT 08 : il est obligatoire que chaque réseau de transit élémentaire (RTE) filtre les routes diffusées et reçues aux interfaces RTE-RTE et RTE-Enclave en conformité avec les accords de service.

RT 09 : il est obligatoire que chaque réseau de transit élémentaire (RTE) assure une authentification mutuelle entre ses nœuds internes lorsque l'interconnexion de ces nœuds internes s'effectue dans un périmètre non maîtrisé.

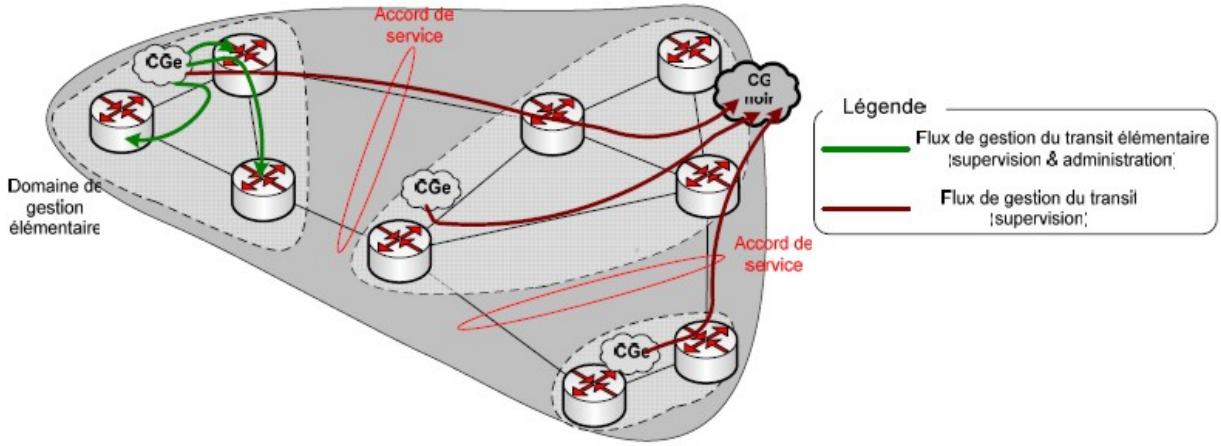
Précision : cette authentification s'effectue lorsque possible par IPSec. Les risques d'insertion d'un pair illégitime sont traités par des mesures organisationnelles et physiques dans le cas d'une interconnexion dans un périmètre maîtrisé.

RT 10 : il est recommandé que chaque réseau de transit élémentaire (RTE) assure une authentification mutuelle basée sur IPSec à l'interface entre RTE.

Précision : les paramètres de configuration d'IPSec (algorithme, longueurs de clés, mode, etc.) sont instanciés au cas par cas dans les accords de services.

2.1.3. ***Plan de gestion.***

La figure ci-dessous illustre le plan de gestion pour l'architecture cible.



Plan de gestion

Dans le plan de gestion, chaque RTE (réseau de transit élémentaire) représente un domaine de gestion élémentaire : un RTE dispose d'outils et de méthodes de gestion qui peuvent lui être propres pour superviser et administrer les équipements qui le composent. Chaque gestion de RTE est assurée depuis son CGe, centre de gestion élémentaire. Un ou plusieurs « CG noir », sont mis en place pour la supervision/hypervision du transit global.

Les RTE étant aconfidentiels, leur gestion peut également être considérée aconfidentielle. Cependant il est nécessaire de se prémunir des menaces, sans pour autant imposer un chiffrement gouvernemental et/ou le recours à un réseau de gestion dédié.

RT 11 : il est obligatoire de disposer d'une gestion dédiée au réseau de transit aconfidentiel distincte de la gestion des enclaves.

RT 12 : il est déconseillé de mettre en œuvre un réseau dédié à la gestion des RTE.

Précision : on vise ainsi une simplification des architectures de gestion permettant une réduction des coûts matériels et humains.

RT 13 : il est obligatoire d'utiliser des protocoles standards et sécurisés [hyperText transfer protocol secure (HTTPS), Simple network management Protocol v3 (SNMPv3), User-based Security Model (USM) & View-based access control model (VACM), Secure sHell (SSH...)] pour assurer le cloisonnement des flux de gestion et l'authentification mutuelle entre l'entité de gestion d'un RTE (CGe) et les équipements gérés.

RT 14 : il est obligatoire de garantir une bande passante minimum pour les flux de gestion.

Précision - en cas de congestion du réseau, il faut garantir l'acheminement des flux de gestion pour les éventuelles reconfigurations nécessaires.

RT 15 : il est obligatoire que chaque réseau de transit élémentaire (RTE) filtre les flux de gestion aux interfaces entre RTE conformément aux accords de service.

RT 16 : il est recommandé d'avoir la capacité d'échanger des données de supervision avec les autres réseaux de transit élémentaires (RTE).

2.2. **Règles organisationnelles.**

RO 01 : il est obligatoire d'organiser le réseau IP de transit global en domaines de routage correspondant à des zones géographiques distinctes :

- une « zone permanente » couvrant la métropole, l'outre-mer et l'ensemble des points de présence fixes en territoire étrangers ;

- une ou plusieurs « zones quasi permanentes » couvrant les bâtiments de la marine ;

- une « zone de théâtre » par théâtre d'opération géographique.

Précision : pour les opérations se déroulant en mer, il est possible de définir, soit une zone unique quasi-permanente pour l'ensemble des forces aéro-maritimes, soit une zone par regroupement de bâtiment (Task Force, groupe aéronaval etc.). Il n'a pas été identifié d'élément flagrant qui permette de trancher entre ces deux possibilités, sachant que le premier cas offre une plus grande simplicité de gestion globale, au détriment d'une gestion fine du contrôle des routes entre forces aéro navales (FAN), alors que le second cas permet une plus grande autonomie d'évolution et de contrôle par FAN, au détriment d'une gestion globale unique.

Concernant les opérations ne se déroulant pas en mer, une zone aéroterrestre par zone géographique est privilégiée.

RO 02 : il est obligatoire que les éventuelles règles de filtrage et de régulation aux interfaces RTE-RTE et RTE-Enclave soient définies *via* les accords de service.

Précision : ces règles dépendent de la confiance entre les opérateurs.

RO 03 : il est obligatoire de coordonner l'affectation des préfixes réseaux pour en garantir l'unicité.

Précision : cela permet d'éviter le recours à la traduction d'adresses (NAT).

2.3. **Règles sémantiques.**

Sans objet.

Pour le ministre de la défense et des anciens combattants et par délégation :

L'amiral,
directeur général des systèmes d'information et de communication,

Christian PÉNILLARD.

(1) n.i. BO.

(2) Le lecteur peut se référer aux documents (ARCHI) et (SLA) pour plus d'explications et de justifications pour les concepts introduits dans cette section.

(3) La régulation (ou shaping) désigne la mise en forme du trafic afin de satisfaire les critères de débit définis dans les accords de service.

ANNEXE.

GLOSSAIRE ET ACRONYMES.

ACRONYME.	DÉFINITION.
CG	Centre de gestion.
CMTSIC	Commission ministérielle technique des SIC.
DGSIC	Direction générale des systèmes d'information et de communication.
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information.
DMZ	DeMilitarized zone : zone de rupture de flux, déployée pour la protection, équipée de pare-feu et proxy.
DR	Diffusion restreinte.
DSCP	Differentiated services code point : champ des paquets IP (v4 et v6) utilisé pour signaler au réseau la qualité de service dont doit bénéficier le paquet.
FAN	Force aéro navale.
HTTPS	HyperText Transfer protocol secure.
IP	Internet protocol : - IPv4 est la version d'IP largement déployée aujourd'hui ; - IPv6 est la version déployée pour éviter la saturation d'adresses d'IPv4.
IPSec	Internet protocol security : sécurisation du protocole IP apportant notamment confidentialité et intégrité.
LAN	Local area network : réseau local.
NAT	Network address translation : traduction des adresses réseaux mise en œuvre pour l'interconnexion de réseaux ayant des plans d'adressage non cohérents.
NP	Non protégé.
OTAN	Organisation du traité de l'Atlantique Nord.
QoS	Quality of service : qualité de service.
RFC	Request for comment : documents officiels édités par l'Internet Engineering Task Force (IETF), décrivant les aspects techniques de l'internet.
RTE	Réseau de transit élémentaire.
SNMP	Simple network management Protocol : protocole de gestion réseau issu du monde internet ; nota : la version 3 offre un accès sécurisé aux équipements.
SSH	Secure sHell : protocole sécurisé pour la gestion des équipements.
TCP	Transmission control protocol : protocole pour le transport fiable des informations au dessus d'IP.
USM	User-based Security Model : modèle de sécurité pour l'authentification des utilisateurs pour le protocole SNMP.
VACM	View-based access control model : modèle de sécurité pour le contrôle d'accès aux informations de gestion pour le protocole SNMP.

TERME.	DÉFINITION.
Aconfidentiel.	Voir « réseau aconfidentiel »
Accord de service.	Un accord de service, ou « contrat de service », est un document contractuel établi entre un fournisseur et un client, répondant à l'obligation d'information sur le niveau de qualité des services offerts/attendus. L'accord de service est un outil de travail essentiel ; il fait apparaître notamment les mentions suivantes : - le délai de mise en service ; - le niveau de qualité minimum garanti pour chacune des caractéristiques techniques essentielles définies dans l'offre, telles que le débit, la capacité ou toute autre caractéristique susceptible d'être mesurée ; - le délai de rétablissement du service lorsque celui-ci est interrompu ; - le délai de réponse aux réclamations. Chaque information est fournie de façon précise et quantifiée dans l'unité appropriée. (Références : - périmètre des contrats de services applicables au sein du MINDEF, guide SCAT n° 16009 Ed 01 du 29 juin 2007 (n.i. BO) ; - arrêté du 16 mars 2006 (n.i. BO) relatif aux contrats de services de communications électroniques).
Domaine de sécurité.	Un domaine de sécurité est constitué d'un ensemble dénombrable de sujets et d'objets auxquels s'applique une même politique de sécurité. (Référence : politique d'interconnexion des réseaux IP de la défense, v3.0 de juin 2006, PIA n° 06-301.3, N° 1660/DEF/EMA/PI ; n.i. BO).
Enclave.	Une enclave est un ensemble de moyens traitant d'informations d'un niveau de classification maximum donné. Une enclave constitue un domaine de sécurité. (Référence : politique d'interconnexion des réseaux IP de la défense, v3.0 de Juin 2006, PIA n° 06-301.3, N° 1660/DEF/EMA/PI ; n.i. BO). Une enclave peut aussi bien être une emprise importante (un site entier, un bâtiment), qu'être très réduite (une salle, un LAN isolé, voire un poste de travail, un combattant). La notion d'enclave est distincte de la notion de SAD (Système Autonome de Desserte) qui porte sur le routage.
Politique de sécurité.	Une politique de sécurité désigne l'ensemble des règles et pratiques qui régissent la façon de gérer, protéger et diffuser les informations au sein d'une organisation.
Réseau aconfidentiel.	Un réseau est dit aconfidentiel, au sens où il ne véhicule que des flux utilisateur préalablement chiffrés au niveau IP (y compris pour les informations d'un domaine non protégé) en sortie d'enclave. Ces flux ne sont donc plus porteurs d'aucun besoin de confidentialité. (Référence : recommandations pour l'évolution des architectures réseaux IP sécurisées, DGA N° 2010-115947/TEC/ACS/17M2008, septembre 2010 ; n.i. BO).
Réseaux de transit élémentaire (RTE).	Un réseau de transit élémentaire est un ensemble de moyens (équipements, liaisons etc.) d'un même domaine de gestion, permettant l'acheminement de données entre différents points d'accès (enclave, point d'interconnexion). Les échanges aux points d'accès sont régis par des accords de service ; les réseaux de transit élémentaire (RTE) peuvent être des réseaux nationaux, des réseaux alliés ou des

	réseaux civils, de niveau stratégique, opératif ou tactique. (Référence : recommandations pour l'évolution des architectures réseaux sécurisées, DGA N° 2010-115947/TEC/ACS/17M2008, version 1.01 du 5 octobre 2010 ; n.i. BO).
Réseaux de transit global.	Un réseau de transit global est constitué de l'interconnexion de réseaux de transit élémentaires assurant le transport des paquets IP entre enclaves. Les relations entre transits élémentaires sont régies par des accords de service. (Référence : recommandations pour l'évolution des architectures réseaux sécurisées, DGA N° 2010-115947/TEC/ACS/17M2008, version 1.01 du 5 octobre 2010 ; n.i. BO).
Moyens de chiffrements IP.	Tous moyens, matériels ou logiciels, suffisant au chiffrement des flux IP, afin d'assurer la confidentialité et l'intégrité des données.
Profils d'interopérabilité des moyens de chiffrement.	Ensemble de protocoles et de paramètres à implémenter dans les moyens de chiffrement pour en garantir l'interopérabilité.
Domaine de gestion.	Un domaine de gestion est constitué d'un ensemble d'outils et de méthodes de gestion pour superviser et administrer les équipements qui le composent. Un domaine de gestion est géré par un seul opérateur.
Domaine de routage.	Un domaine de routage est constitué d'un ensemble d'équipements qui opèrent selon les mêmes procédures de routage. Il peut être divisé en sous domaines, permettant ainsi un routage hiérarchique facilitant le support de la mise à l'échelle. Un même opérateur peut gérer plusieurs domaines de routage, mais un domaine de routage ne peut être géré que par un seul opérateur.