Cible de sécurité CSPN

Produit IPdiva Secure 8

Catégorie « Identification, authentification et contrôle d'accès »

Référence : CSPN-ST-IPdiva Secure-2.02

Date : le 03/05/2016

Code interne : SYS002

Siège : 4 bis allée du Bâtiment ● 35000 Rennes ● France ● www.amossys.fr

SIRET : 493 348 890 00036 ● **NAF** : 6202 A ● RCS Rennes B 493 348 890 ● SAS au capital de 38.000 Euros

FICHE D'ÉVOLUTIONS

RÉVISION	DATE	DESCRIPTION	RÉDACTEUR
1.00	05/09/2014	Version initiale de la cible pour présentation à l'ANSSI	Jérôme LEBÈGUE
1.01	24/11/2014	Prise en compte des remarques ANSSI	Jérôme LEBÈGUE
1.02	17/02/2015	Ajout du serveur de Log et mise à jour de la cible de sécurité	Antoine COUTANT
1.03	30/03/2015	Mise à jour de la cible de sécurité avec l'ajout de la fonction de comparaison des hachés au démarrage de la solution	Antoine COUTANT
2.00	22/01/2016	Mise à jour de la version de la TOE et mise en forme de la cible de sécurité	Antoine COUTANT
2.01	04/02/2016	Précision apportée sur l'OS support	Antoine COUTANT
2.02	03/05/2016	Ajout de la référence du patch IPD-15934	Antoine COUTANT

Ce document est validé par Systancia.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], du produit « IPdiva Secure 8 » développé par la société Systancia.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de Systancia. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Editeur	Systancia Actipolis III 3, rue Paul Henri Spaak 68390 Sausheim - FRANCE
Lien vers l'organisation	http://www.systancia.com
Nom commercial du produit	IPdiva Secure 8
Numéro de la version évaluée	Composantes évaluées : - IPdiva Server 8 - IPdiva Gateway et Log 8 Version incluant le paquet `ipdiva-hostmanager-webserver` (patch référence IPD-15934)
Catégorie du produit	Identification, authentification et contrôle d'accès

1.3. RÉFÉRENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- Mécanismes cryptographiques Ipdiva, version 1.01 du 26/06/2015 ;
- Guide de l'utilisateur, référence MU-MEDV6 de 2012 ;
- Plateforme VPN SSL - IPdiva Anywhere Secure Access - Manuel d'administration, référence MA-MED- 6.0, version 3 de 2012 ;
- Pré-requis techniques IPdiva, version 1.4.

[1] Certification de Sécurité de Premier Niveau

[2] Agence nationale de la sécurité des systèmes d'information

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GÉNÉRALE

IPdiva Secure 8 permet la protection, le contrôle et la traçabilité de tous les accès externes aux ressources d'un système d'information.

S'appuyant sur le standard SSL et une plateforme de communication innovante (VPN SSL à topologie répartie [3]), IPdiva Secure 8 garantit un accès sélectif (« à la demande ») aux ressources internes d'une entreprise par Internet, en tout lieu et pour tout type de systèmes, à partir d'un simple navigateur web sans aucune interférence avec les infrastructures en place.

IPdiva Secure 8 présente de nombreux avantages dès lors qu'il s'agit d'adresser une variété d'utilisateurs, d'équipements d'accès, d'infrastructure support et de conditions d'usage des ressources mises à disposition.

En particulier, IPdiva Secure 8 permet :

- la sécurité et le contrôle des synchronisations smartphones/mobiles (mode ActiveSync) ;
- la sécurité des accès applicatifs et systèmes (mode portail VPN SSL) ;
- la sécurité des accès intranet (mode Reverse Proxy).

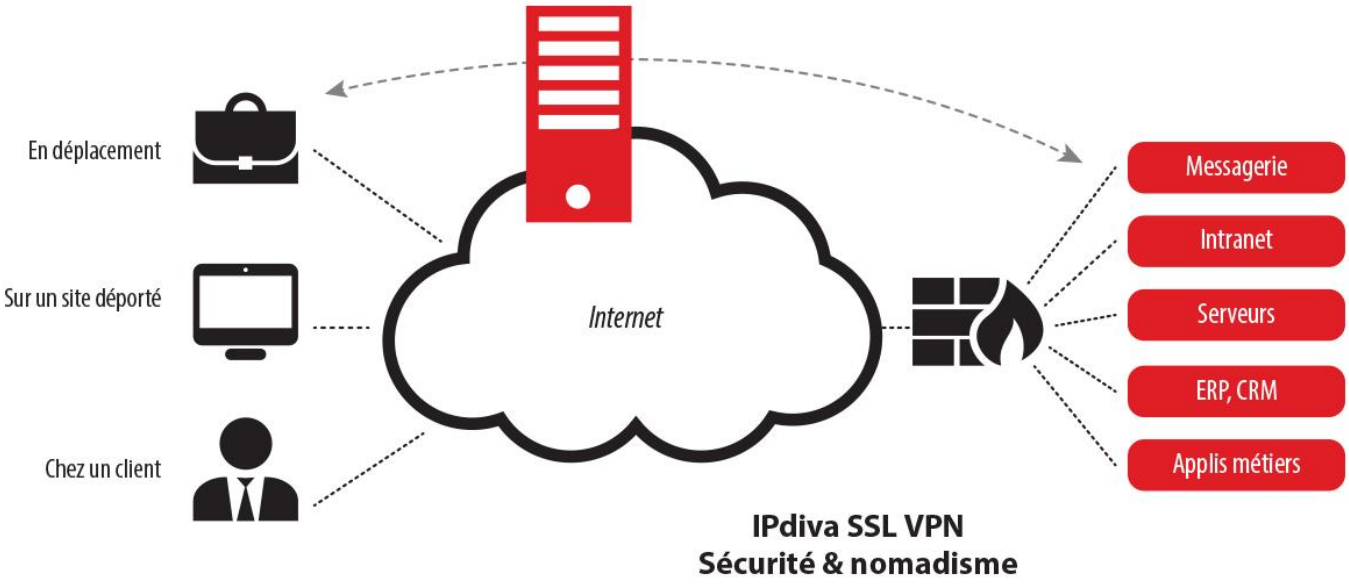

Figure 1 : Solution IPdiva Secure 8

Au démarrage de la solution IPdiva Secure 8, une fonctionnalité de comparaison de hachés permet de contrôler que les binaires utilisés par la cible d'évaluation sont intègres et donc qu'ils n'ont pas été modifiés.

[3] Les différents composants IPdiva peuvent être positionnés dans divers sites avec des flux transitant par des réseaux dont la sécurité n'est pas maitrisée, par exemple l'Internet. Les flux de communication de ces composants sont sécurisés par SSL. Chaque équipement possède son certificat propre. La construction des flux (lien TCP) est établie depuis les passerelles jusqu'au serveur de médiation. Le déploiement des passerelles est donc simplifié, celles-ci ne nécessitent pas d'ouverture de port depuis l'extérieur.

2.2. PRINCIPE DE FONCTIONNEMENT

IPdiva Secure 8 est une solution d'architecture à topologie répartie, avec une double « barrière d'entrée », qui permet un cloisonnement entre les serveurs applicatifs situés sur le réseau interne et le réseau externe. Les ressources internes ne sont jamais directement exposées sur Internet.

Comme illustré dans la figure ci-dessous, la solution s'appuie sur une séparation en deux composants : le serveur IPdiva (appelé aussi serveur de médiation) et la passerelle IPdiva.

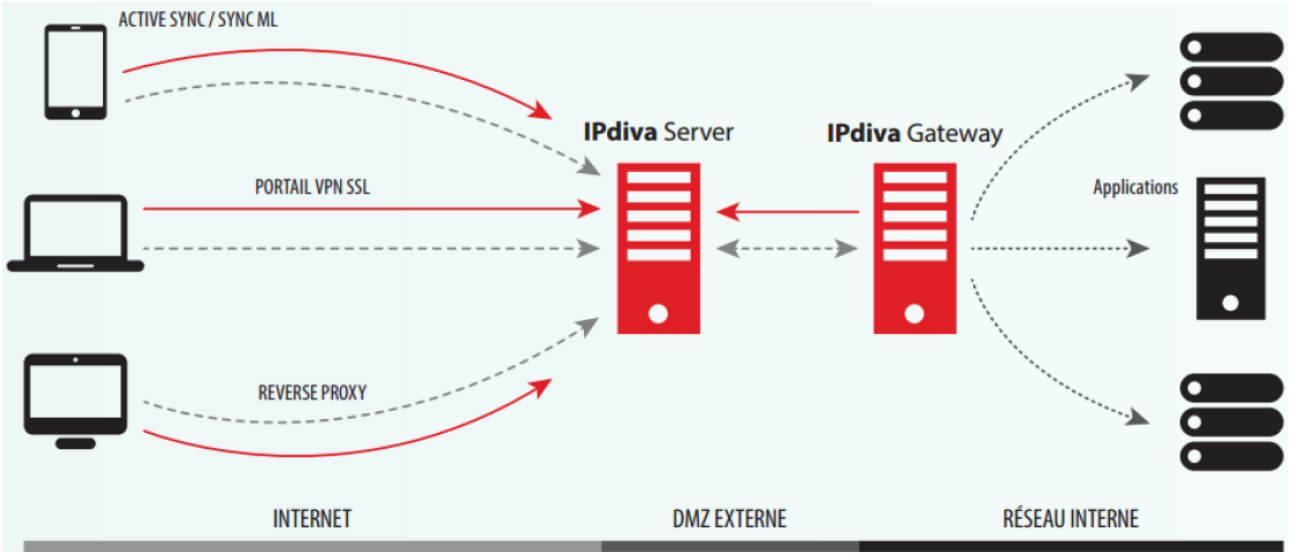

Figure 2 : Architecture d'un déploiement type de la solution

IPdiva Server agit comme portier d'accès centralisé pour les demandes d'accès externes :

- point d'entrée unique vers les sites hébergeant les systèmes à accéder ou les applications publiées ;
- mutualisation de l'authentification et du contrôle d'accès ;
- répertoire central pour toutes les traces des accès distants.

IPdiva Gateway est l'interface de relais entre IPdiva Server et les applications, les fichiers ou les systèmes devant être accessibles à distance. La communication est sécurisée entre IPdiva Server et IPdiva Gateway par un tunnel SSL sortant, sans intervention sur le firewall ou le routeur en place.

La solution peut être déployée selon plusieurs modes :

- « Mode Dual » : il s'agit du mode illustré dans la figure précédente, le serveur est déployé dans la DMZ du site hébergeant les ressources ;
- « Mode Cloud » : le composant IPdiva Server est déployé sur un serveur distant ;
- « Mode combo » : le serveur et la passerelle sont combinés sur un même serveur local.

À ces modes, s'ajoute la notion de sites. Un déploiement est appelé mono-site si toutes les ressources (au sens ressources protégées par la solution) sont sur le même réseau local. Un déploiement est multi-sites si les ressources sont distribuées sur plusieurs réseaux locaux, chacun disposant d'au moins une passerelle.

La solution permet l'authentification des utilisateurs selon plusieurs mécanismes :

- formulaire : page Web de saisie du couple identifiant/mot de passe ;

- boîte de dialogue navigateur : le navigateur affiche une boîte de dialogue standard d'identification (ce mode est déconseillé par le développeur car il permet de mémoriser le mot de passe dans les paramètres du navigateur) ;
- certificat : l'authentifiant de connexion est extraite du certificat (champ CN) ;
- certificat et formulaire : un mot de passe est requis suite à l'authentification par certificat.

Il est également possible d'ajouter des jetons d'authentifications type générateur d'OTP à l'authentification.

Une fois authentifié, l'utilisateur pourra avoir accès à différents types de ressources selon son (ou ses) groupe(s) d'appartenance métier. On peut citer, de manière non exhaustive :

- un/des accès Web (par exemple à un intranet) ;
- un accès distant de type SSH ou TSE ;
- un accès à ses emails ;
- etc.

2.3. DESCRIPTION DES DÉPENDANCES

La solution IPdiva est fournie soit sous forme de licences logicielles, soit sous forme d'un produit intégré (matériel et logiciel).

En tant que produit intégré (mode *appliance*), la TOE est autonome.

En mode logiciel, la TOE nécessite pour fonctionner correctement un certain nombre de composants sur les stations sur lesquels sont déployés ses composants constitutifs :

- système d'exploitation ;
- serveur SSH.

Les postes clients doivent disposer d'un navigateur prenant en charge ActiveX ou Java.

Un guide de sécurisation avancée est fourni par le développeur afin d'installer la solution dans des conditions optimales d'utilisation.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

La TOE (IPdiva Server, IPdiva Gateway et IPdiva Log) doit être installée sur des serveurs physiques distincts (sous environnement Linux). La virtualisation est possible mais, pour l'évaluation, les serveurs doivent être installés sur des équipements différents.

Pour l'évaluation CSPN, le système d'exploitation retenu pour l'évaluation CSPN est GNU Linux Debian 8.2 (architecture 64 bits). Cet OS sera utilisé pour installer IPdiva Server, IPdiva Gateway et IPdiva Log.

Les postes utilisateurs (administrateur et utilisateurs finaux) sont des postes Windows 7 Pro SP1 (architecture 64 bits).

Le navigateur utilisé est Internet Explorer 11.0.9600.17280 avec le support ActiveX.

2.5. PÉRIMÈTRE DE L'ÉVALUATION

2.5.1. Périmètre

Dans le cadre de l'évaluation CSPN du produit, les composants IPdiva Server et Gateway sont testés en utilisation reverse proxy avec authentification et comprenant le paquet `ipdiva-hostmanager-webserver` (patch référence IPD-15934).

La TOE n'est pas évaluée en tant que produit intégré (mode *appliance*) mais en mode logiciel.

Sont exclus du périmètre : le plugin navigateur utilisé (ActiveX ou Java), les systèmes d'exploitation des différents composants ainsi que les ressources exposées au travers de la TOE. Les fonctionnalités de SSO et d'authentification en cascade sont également hors du périmètre de cette cible.

Afin d'apporter à la cible d'évaluation une sécurité maximale sur l'intégrité des journaux des évènements, une passerelle IPdiva Log est rajoutée. Son objectif est le stockage d'une copie des journaux externalisés autre que le serveur de médiation ainsi que la vérification de l'intégrité des binaires des composants IPdiva Server et Gateway au démarrage de la solution (avec retour d'intégrité correcte ou pas sur la console de l'administrateur ayant démarré le service). La communication entre le serveur de Log et le serveur de médiation est assurée par le service Gateway IPdiva, ainsi les données échangées sont parfaitement chiffrées.

Le composant IPdiva Log est situé en zone sécurisée et est une passerelle IPdiva Gateway dont l'usage est limité à la collecte, au stockage des journaux et à la vérification des empreintes.

2.5.2. Plateforme d'évaluation

La TOE est déployée en mode Dual mono-site. L'authentification se fait par l'intermédiaire d'un certificat et sans OTP. La TOE n'utilise pas d'annuaire autre que l'annuaire local, intégré, pour les comptes utilisateurs.

Le schéma ci-après présente les composants constitutifs de la cible évaluée (TOE) :

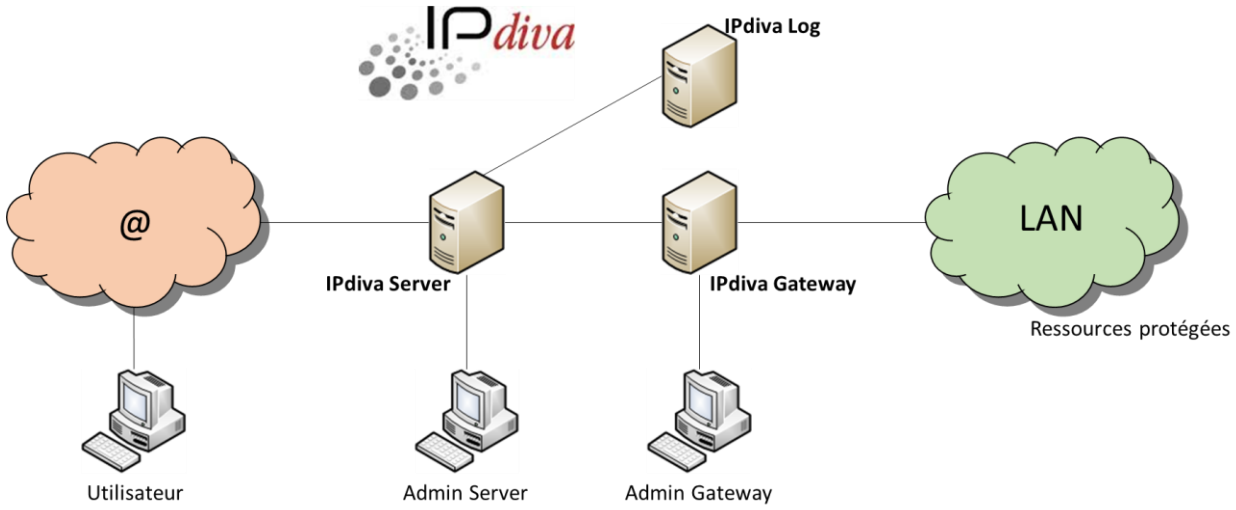

Figure 3 : Plateforme d'évaluation

3.PROBLÉMATIQUE DE SÉCURITÉ

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNÉS

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants seront pris en considération dans le cadre de l'analyse :

- **Utilisateur final**

  Il accède aux ressources via IPdiva Server en s'authentifiant sur la TOE. Il peut être amené à effectuer un certain nombre d'opérations sur la TOE si celle-ci est configurée dans ce sens (gestion de son mot de passe, de ses informations personnelles, etc.). Ses droits sont très restreints, il peut uniquement atteindre les ressources auxquelles un administrateur lui a donné accès.

- **Administrateur**

  Il accède à l'interface d'administration au travers d'un navigateur Web et réalise les opérations de gestion de la TOE (configuration, paramétrage, consultation des traces et des rapports d'audit).

  Il peut définir des profils, les droits et les comptes associés d'autres catégories d'utilisateurs autorisées à interagir avec la TOE : utilisateurs finaux, administrateurs délégués (rôle intermédiaire bénéficiant de droits d'administrations restreints), etc.

- **Super utilisateur**

  Ce rôle dispose des droits les plus étendus. En effet, il peut effectuer les opérations les plus sensibles, comme la configuration des certificats, des clés privées, la gestion des administrateurs de la plateforme, etc.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon trois critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité et confidentialité.

La fonctionnalité première de la TOE est de prendre en charge l'authentification et le contrôle d'accès des utilisateurs sur les ressources protégées d'un système d'information.

Pour cela, les biens sensibles à protéger sont les suivants :

- **B1.AUTHENTIFICATION**

  Données d'identification et d'authentification des utilisateurs sur la TOE, stockées par la TOE ou son environnement ainsi qu'échangées entre composants de la TOE ou avec les ressources informatiques de l'environnement. Selon la méthode d'authentification, ces données peuvent être hors TOE (exemple : authentification par carte à puce). Ce bien est sensible en confidentialité et en intégrité. La protection de ces données est réalisée au niveau du navigateur.

- **B2.JETON-SESSION**

  Données techniques permettant de prouver l'identité de l'utilisateur ainsi que le fait qu'il s'est déjà authentifié avec succès une première fois vis-à-vis de la TOE. Ces données sont échangées entre le poste de l'utilisateur et la TOE. Ce bien est sensible en confidentialité et en intégrité.

- **B3.FLUX-AUTHENTIFICATION**

  Flux impliqués dans la réalisation de l'authentification de l'utilisateur sur une ressource donnée, entre la TOE, la station de travail de l'utilisateur et la ressource concernée. Ces flux peuvent contenir les biens sensibles **B1.AUTHENTIFICATION** et **B2.JETON-SESSION**. Ils sont sensibles en intégrité et en confidentialité.

- **B4.CONTROLE-ACCES**

  Données permettant à la TOE de réaliser le contrôle des droits d'accès de l'utilisateur sur l'application qu'il souhaite accéder. Elles peuvent prendre la forme de règles métiers configurées par l'administrateur et de valeurs spécifiques aux utilisateurs ou aux applications. Ce bien est sensible en confidentialité et en intégrité.

- **B5.CLES-FRONTAL**

  Données gérées par la TOE et utilisées pour chiffrer / déchiffrer les échanges entre un utilisateur et IPdiva Server. Ces clés sont sensibles en confidentialité et en intégrité. La protection de ces clés est indiquée au §2.4.1 du document spécifique aux mécanismes cryptographiques.

- **B6.CLES-INTERNES**

  Données gérées par la TOE et utilisées pour chiffrer / déchiffrer les échanges entre IPdiva Server et IPdiva Gateway ainsi qu'entre IPdiva Server et IPdiva Log. Ces clés sont sensibles en confidentialité et en intégrité. La protection de ces clés est indiquée au §2.4.2 du document spécifique aux mécanismes cryptographiques.

- **B7.FLUX-METIER**

  Le flux métier désigne les flux entre l'utilisateur final et les services accédés via la TOE qui ne relèvent pas du fonctionnement de la TOE. Ces flux sont sensibles en confidentialité et intégrité.

- **B8.EMPREINTES_TOE**

  Empreintes stockées sur IPdiva Log des différents binaires des composants IPdiva Server et IPdiva Gateway. Ces données sont sensibles en disponibilité et intégrité.

Les besoins de sécurité de chacun de ces biens sont donnés ci-dessous :

Biens sensibles	Disponibilité	Intégrité	Confidentialité
B1.AUTHENTIFICATION		√	√
B2.JETON-SESSION		√	√

Biens sensibles	Disponibilité	Intégrité	Confidentialité
B3.FLUX-AUTHENTIFICATION		√	√
B4.CONTROLE-ACCES		√	√
B5.CLES-FRONTAL		√	√
B6.CLES-INTERNES		√	√
B7.FLUX-METIER		√	√
B8.EMPREINTES_TOE	√	√	

Tableau 1 - Besoins de sécurité des biens sensibles

3.3. DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

Les hypothèses sur l'environnement de la TOE sont les suivantes :

- **H1.LOCAUX**

  Les composants IPdiva Secure 8, ainsi que tous les supports contenant des biens sensibles (composants hors TOE tels que les annuaires LDAP des utilisateurs, papier, CDs, sauvegardes, etc.), se trouvent dans des locaux sécurisés dont l'accès est contrôlé nominativement et restreint aux administrateurs.

- **H2.ENVIRONNEMENT**

  Les composants IPdiva Secure 8 sont installés sur des systèmes sains (OS et navigateur), correctement mis à jour, en particulier concernant les correctifs liés à la sécurité. Les services et partages inutiles sont désactivés.

  Les composants hors TOE – en particulier les annuaires LDAP des utilisateurs – sont correctement sécurisés. En particulier, les accès logiques sont correctement paramétrés.

  Les composants sont installés dans un réseau de confiance et ne sont utilisés que pour les fonctions de sécurité de la TOE décrites au §3.5 de la présente cible de sécurité.

  L'initialisation et le renouvellement des clés de chiffrement, des certificats SSL ainsi que des comptes utilisateur à privilège sont réalisés conformément à la politique de sécurité conforme au Référentiel Général de Sécurité v2.0 de l'ANSSI[4].

  La TOE dispose des accès requis au réseau et aux ressources informatiques nécessaires à la bonne réalisation de ses fonctionnalités.

- **H3.POSTE-UTILISATEUR-SAIN**

  Les postes des utilisateurs finaux sont sains, correctement mis à jour et sécurisés :

  - ils sont protégés contre les virus ;

[4] http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/

- les échanges avec d'autres machines via un réseau ouvert sont contrôlés par un pare feu contrôlant et limitant les échanges ;
- l'accès aux fonctions d'administration est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur) ;
- l'installation et la mise à jour de logiciels sont réalisées sous le contrôle de l'administrateur.

- **H4.ADMINISTRATEUR**

  Les administrateurs et super utilisateurs sont considérés non hostiles.

  Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

  L'administrateur surveille régulièrement les évènements d'audit ainsi que les alarmes.

- **H5.POSTE-ADMINISTRATEUR-SAIN**

  Les postes des administrateurs sont sains, correctement mis à jour et sécurisés (cf. H3.POSTE-UTILISATEUR-SAIN).

- **H6.PROTECTION-FLUX**

  Les communications entre l'utilisateur final et le serveur IPdiva sont réalisés uniquement en TLS et en utilisant des suites cryptographiques conformes aux exigences de l'ANSSI (RGS[5]). Le serveur est authentifié sur la base d'un certificat émis par une AC[6] reconnue dans le navigateur Web de l'utilisateur final.

  En particulier, les échanges entre le serveur et la passerelle doivent être sécurisés et conformes aux recommandations de l'ANSSI du paragraphe 4 et ultérieur du DAT-NT-19/ANSSI/SDE/NP du 01/10/2014.

3.4. DESCRIPTION DES MENACES

3.4.1. Agents menaçants

Les agents menaçants considérés sont :

- un attaquant humain ou entité qui interagit avec la TOE mais ne disposant pas d'accès légitime à celle-ci ;
- un utilisateur final qui dispose d'un compte sur la TOE et qui va tenter d'élever ses privilèges.

Les administrateurs (positionnés sur les postes "Admin Server" et "Admin Gateway") ne sont pas considérés comme hostiles.

[5] Référentiel Général de Sécurité

[6] Autorité de Certification

Le positionnement des attaquants est indiqué sur la figure ci-dessous.

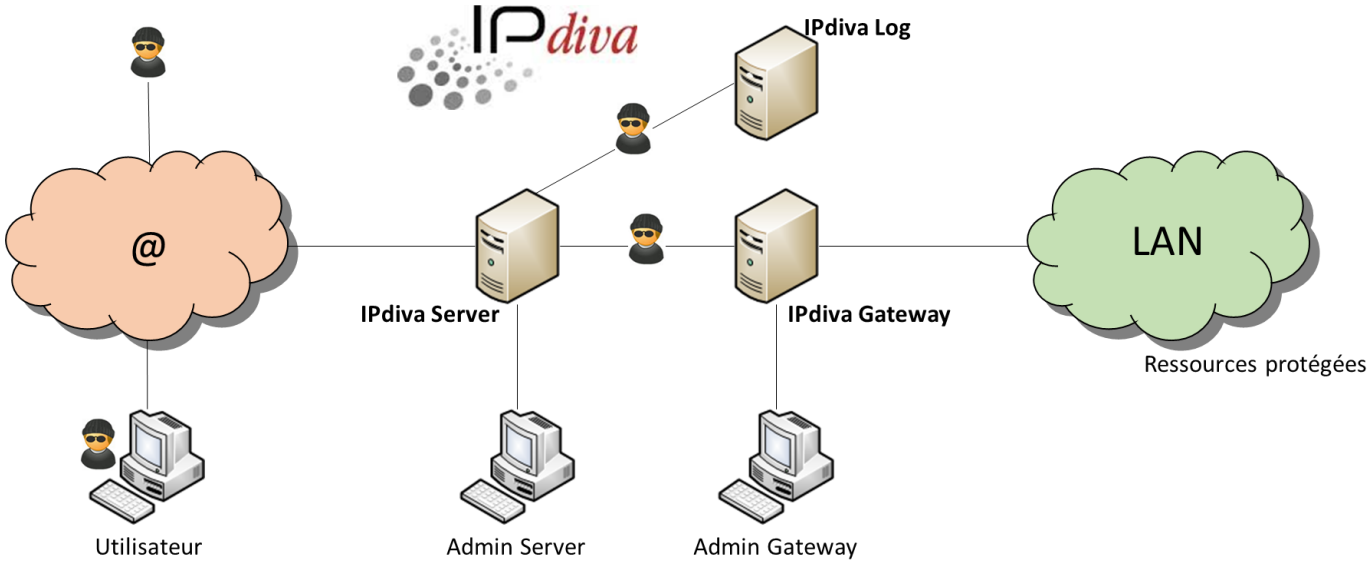

Figure 4 : Positionnement des attaquants

3.4.2. Menaces applicables à la TOE

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M1.ECOUTE-PASSIVE-EXTERNE**

  Un attaquant écoute les flux générés entre un poste utilisateur et IPdiva Server pour compromettre les données sensibles en confidentialité échangées.

- **M2.ECOUTE-PASSIVE-INTERNE**

  Un attaquant écoute les flux générés entre IPdiva Server et IPdiva Gateway (ou entre IPdiva Server et IPdiva Log) pour compromettre les données sensibles en confidentialité échangées.

- **M3.MAN-IN-THE-MIDDLE-EXTERNE**

  Un attaquant intercepte les flux générés entre un poste utilisateur et IPdiva Server. Il les modifie dans le but d'altérer les données sensibles en intégrité.

- **M4.MAN-IN-THE-MIDDLE-INTERNE**

  Un attaquant intercepte les flux générés entre IPdiva Server et IPdiva Gateway (ou entre IPdiva Server et IPdiva Log). Il les modifie dans le but d'altérer les données sensibles en intégrité.

- **M5.USURPATION-IDENTITE-USER**

  Un attaquant usurpe l'identité d'un utilisateur légitime et autorisé à accéder à une ressource interfacée avec la TOE.

- **M6.ELEVATION-PRIVILEGES**

  Un attaquant, utilisateur déclaré et légitime sur la TOE, parvient à élever ses privilèges (par exemple il parvient à passer d'utilisateur final à administrateur) ou à accéder à une ressource non disponible pour son profil.

- **M7.REJEU-FORGE**

  Un attaquant intercepte le jeton de session d'un utilisateur légitime et le fournit de nouveau à la TOE dans l'optique d'usurper l'identité de cet utilisateur. Il peut par ailleurs tenter de forger un vrai-faux jeton de session.

- **M8.SESSION-HIJACKING**

  La session d'un utilisateur légitime et authentifié sur la TOE est détournée et utilisée par un attaquant.

- **M9.USURPATION-IDENTITE-ADMIN**

  Un attaquant usurpe l'identité d'un administrateur légitime et autorisé à accéder à la TOE. Cette menace englobe également les scénarios dans lesquels un attaquant, dûment authentifié sur l'interface d'administration et avec un profil donné, essaie d'accéder à des informations qui ne sont normalement pas accessibles par ce profil et donc de mettre en défaut le cloisonnement.

- **M10.ALTERATION-FUITE**

  Un attaquant altère (modification ou suppression) des biens sensibles en intégrité de la TOE ou compromet des biens de la TOE sensibles en confidentialité.

- **M11.ALTERATION_BON_FONCTIONNEMENT**

  Un attaquant cherche à compromettre le démarrage de la solution. Cette menace peut prendre les formes suivantes :

  - altération (modification ou suppression) des empreintes échangées entre IPdiva Server et IPdiva Log ou entre IPdiva Gateway et IPdiva Log ;
  - altération (modification ou suppression) du retour de la comparaison réalisée par IPdiva Log.

3.5. DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- **F1.AUTHENT-CTRL-ACCES-TOE**

  La TOE permet d'identifier et d'authentifier nominativement les utilisateurs et de leur attribuer des droits sur la TOE en fonction de leur profil métier.

- **F2.AUDIT**

  La TOE trace en base les évènements relatifs à l'administration et la configuration de la TOE ainsi que les évènements métiers (authentifications des utilisateurs, authentifications et actions des administrateurs, accès à une ressource, etc.).

- **F3.COMMUNICATIONS-SECURISEES-EXTERNE**

  Les échanges électroniques entre un utilisateur et IPdiva Server sont protégés en confidentialité et en intégrité.

- **F4.COMMUNICATIONS-SECURISEES-INTERNE**

  Les échanges électroniques entre IPdiva Server et IPdiva Gateway ainsi qu'entre IPdiva Server et IPdiva Log sont protégés en confidentialité et en intégrité.

- **F5.CRYPTO**

  La TOE propose des mécanismes cryptographiques permettant en particulier de gérer et d'utiliser des clés cryptographiques conformément aux règles de l'ANSSI en matière de dimensionnement et de choix des mécanismes cryptographiques (annexe B1 du RGS).

- **F6.COMPARAISON_EMPREINTES**

  La TOE propose un mécanisme reposant sur la comparaison d'empreintes SHA-256 au démarrage de la solution IPdiva. En particulier, au démarrage de IPdiva Server (et IPdiva Gateway), un calcul d'empreintes est réalisé sur les composants puis le résultat est envoyé à IPdiva Log pour comparaison. En retour, IPdiva Log informe si la comparaison est un succès ou pas (avec blocage du démarrage en cas d'échec de la comparaison). Ceci permet ainsi de vérifier l'intégrité des composants lancés au démarrage sur la base des empreintes stockées en base sur IPdiva Log (base mise à jour à chaque déploiement d'une nouvelle mise à jour).

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles :

	B1.AUTHENTIFICATION	B2.JETON-SESSION	B3.FLUX-AUTHENTIFICATION	B4.CONTROLE-ACCES	B5.CLES-FRONTAL	B6.CLES-INTERNES	B7.FLUX-METIER	B8.EMPREINTES_TOE
M1.ECOUTE-PASSIVE-EXTERNE	**C**	**C**	**C**				**C**	
M2.ECOUTE-PASSIVE-INTERNE			**C**				**C**	
M3.MAN-IN-THE-MIDDLE-EXTERNE	**CI**	**CI**	**CI**				**CI**	
M4.MAN-IN-THE-MIDDLE-INTERNE			**CI**				**CI**	
M5.USURPATION-IDENTITE-USER				**C**				
M6.ELEVATION-PRIVILEGES				**CI**				
M7.REJEU-FORGE	**CI**	**CI**					**C**	
M8.SESSION-HIJACKING		**C**					**C**	
M9.USURPATION-IDENTITE-ADMIN				**I**	**CI**	**CI**		
M10.ALTERATION-FUITE	**CI**				**CI**	**CI**		
M11.ALTERATION_BON_FONCTIONNEMENT								**DI**

Tableau 2 - Couverture des biens sensibles

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F1.AUTHENT-CTRL-ACCES-TOE	F2.AUDIT	F3.COMMUNICATIONS-SECURISEES-EXTERNE	F4.COMMUNICATIONS-SECURISEES-INTERNE	F5.CRYPTO	F6.COMPARAISON_EMPREINTES
M1.ECOUTE-PASSIVE-EXTERNE			√		√	
M2.ECOUTE-PASSIVE-INTERNE				√	√	
M3.MAN-IN-THE-MIDDLE-EXTERNE			√		√	
M4.MAN-IN-THE-MIDDLE-INTERNE				√	√	
M5.USURPATION-IDENTITE-USER	√					
M6.ELEVATION-PRIVILEGES	√	√				
M7.REJEU-FORGE	√	√				
M8.SESSION-HIJACKING				√		
M9.USURPATION-IDENTITE-ADMIN	√	√				
M10.ALTERATION-FUITE		√				
M11.ALTERATION_BON_FONCTIONNEMENT		√		√	√	√

Tableau 3 - Couverture des menaces

Fin du document