TAPICS

Cible de Sécurité CSPN

TAPs gamme Cuivre

Version 1.3.10

Page intentionnellement laissée vide

Table des matières

Tableau de révision

Révision	Date	Auteur	Commentaires
0.1	13/11/2015	SERMA	Version Initiale
1.0	23/11/2015	SERMA	Première version à publier
1.1	11/12/2015	TAPICS	1ère prise en compte des remarques de l'ANSSI
1.2	16/12/2015	TAPICS	Ajout dans l'introduction de la précision « boitier » ou « équipement pour désigner » un TAP
1.3	21/12/2015	TAPICS / SERMA	§4 et §5 : 2nd prise en compte des remarques de l'ANSSI Prise en compte remarque de SERMA sur la limite de débit des TAPs Cuivre
1.3.1	7/1/2016	TAPICS	§6 ajout de la photographie du scellé
1.3.2	2/4/2016	TAPICS	Modifications suite à réunion ANSSI/SERMA/TAPICS du 13/4/2016
1.3.3	6/5/2016	TAPICS	Modifications suite à retour de SERMA
1.3.4	16/5/2016	TAPICS	Modifications suite à retour de SERMA
1.3.5	26/5/2016	SERMA	Dissociation des menaces M2 et M3 Suppression du commentaire page 4
1.3.6	24/6/2016	TAPICS	Modifications en §1.1, 2.1, 2.2, 2.3, 3, 4.1, 4.2 et 5 suite aux remarques écrites de l'ANSSI le 23/6/2016
1.3.7	27/6/2016	TAPICS	Supprimé le terme « réseau observé »
1.3.8	30/8/2016	TAPICS	§2.1 Précision sur la différence entre les TAPs 1 ligne et les TAPs 8 lignes §2.2 Ajout du schéma de connexion du TAP 8 lignes
1.3.9	9/9/2016	TAPICS	§2.1 page 5, précision des références de modèles dans le tableau
1.3.10	15/5/2017	TAPICS	§5 page 9, suppression de la fonction «Protection contre les rayonnements électromagnétiques» Annexe : - Ajout de la mention sur le microcontrôleur - Ajout de la mention sur la suppression du port USB

1 Introduction

1. 1 Identification de la Cible de Sécurité

Ce document décrit la Cible de Sécurité relative à l'ensemble des produits TAPs de la gamme Cuivre en vue de l'obtention d'une Certification de Sécurité de Premier Niveau (CSPN). Cette Cible de Sécurité prend en compte l'ensemble des produits de la gamme Cuivre dans leur version sécurisée sans dépendre des variantes de modèle (débit maximum, nombre de lignes, etc.).

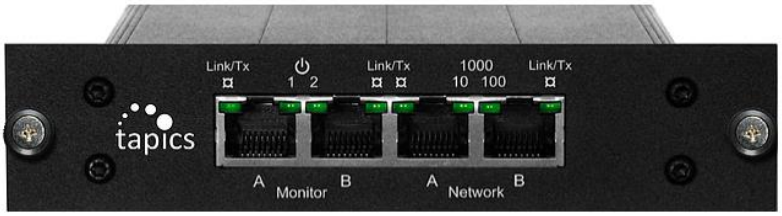
Les termes « boitier » et «équipement » désignent tous deux un TAP.

1. 2 Identification des produits

Société éditrice	TAPICS
Lien vers la société	www.tapics.fr
Nom commercial des produits	TAPs électriques
Références des produits évalués	TAPs de réplication passive : TACU1-1G-SEC (1 ligne réseau), TACU8-1G-SEC (8 lignes réseau)
Catégorie des produits	Matériel et logiciel embarqué

Ci-après, l'expression *le produit* renvoie à n'importe quel modèle de cette liste de références. On présente ci-dessous des vues des modèles cités :

TACU1-1G-SEC :



TACU8-1G-SEC :

2 Argumentaire du produit

2. 1 Description générale du produit

Le TAP (*Test Access Point*) est un équipement réseau passif inséré en ligne. L'objectif de ce dispositif est d'offrir sur les interfaces prévues à cet effet une copie du trafic réseau initial qui doit être la plus fidèle possible. Elle peut être utilisée à des fins diverses (sonde IDS, monitoring, etc.), et elle ne doit pas avoir d'effet sur le réseau.

Les TAPs de la gamme Cuivre, pour les réseaux Ethernet, possèdent des interfaces réseau RJ45 supportant des débits de 10Mbps jusqu'à 1Gbps.

Les TAPs Cuivre nécessitent une alimentation électrique externe pour alimenter le circuit électronique en charge de la recopie du lien réseau initial. En cas de perte d'alimentation, le lien réseau initial est conservé. Seul le lien réseau de monitoring est perdu.

Les TAPs de TAPICS concernés par cette cible n'intègrent aucune fonctionnalité logicielle embarquée ou pilotable :

- ils ne sont pas paramétrables,
- ils ne disposent d'aucune adresse IP,
- ils ne mémorisent pas le trafic.

Les deux modèles de TAPs cuivre proposés mettent en œuvre le même principe électronique interne, installé 1 ou 8 fois dans un boitier afin de répliquer le trafic d'une ou de huit lignes. Il n'y a donc aucune différence fonctionnelle ni de caractéristique entre les deux modèles, hormis le nombre de lignes en connexion, mais les circuits électroniques sont physiquement différents. Le tableau ci-dessous présente ces deux modèles :

Modèle référence TACU1-1G-SEC, TAP 1 ligne cuivre	**Modèle référence TACU8-1G-SEC, TAP 8 lignes cuivre**
Réplication du trafic d'une ligne	Réplication du trafic de 8 lignes
1 module électronique de réplication	8 modules électroniques de réplication
2 ports de réplication	16 ports de réplication

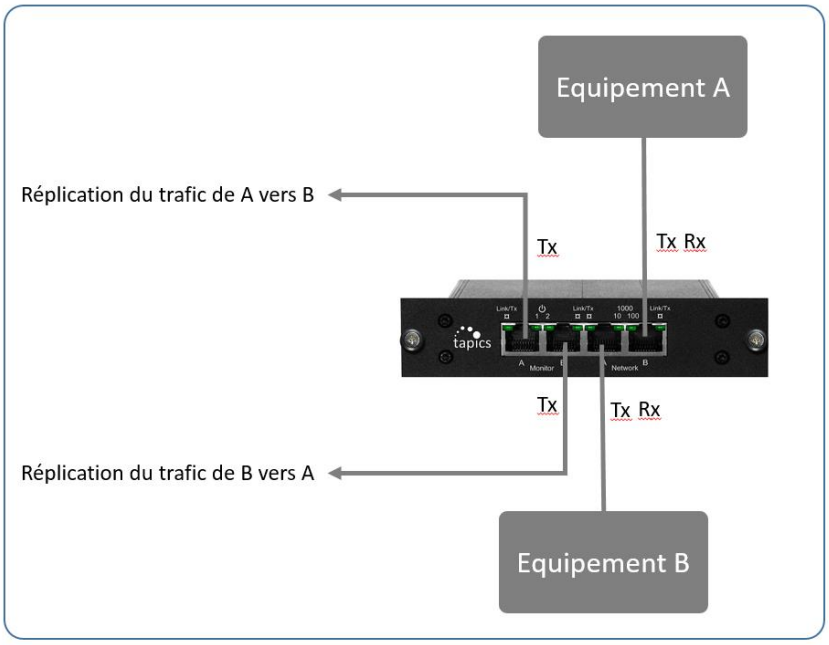
Les utilisateurs du produit sont les suivants :

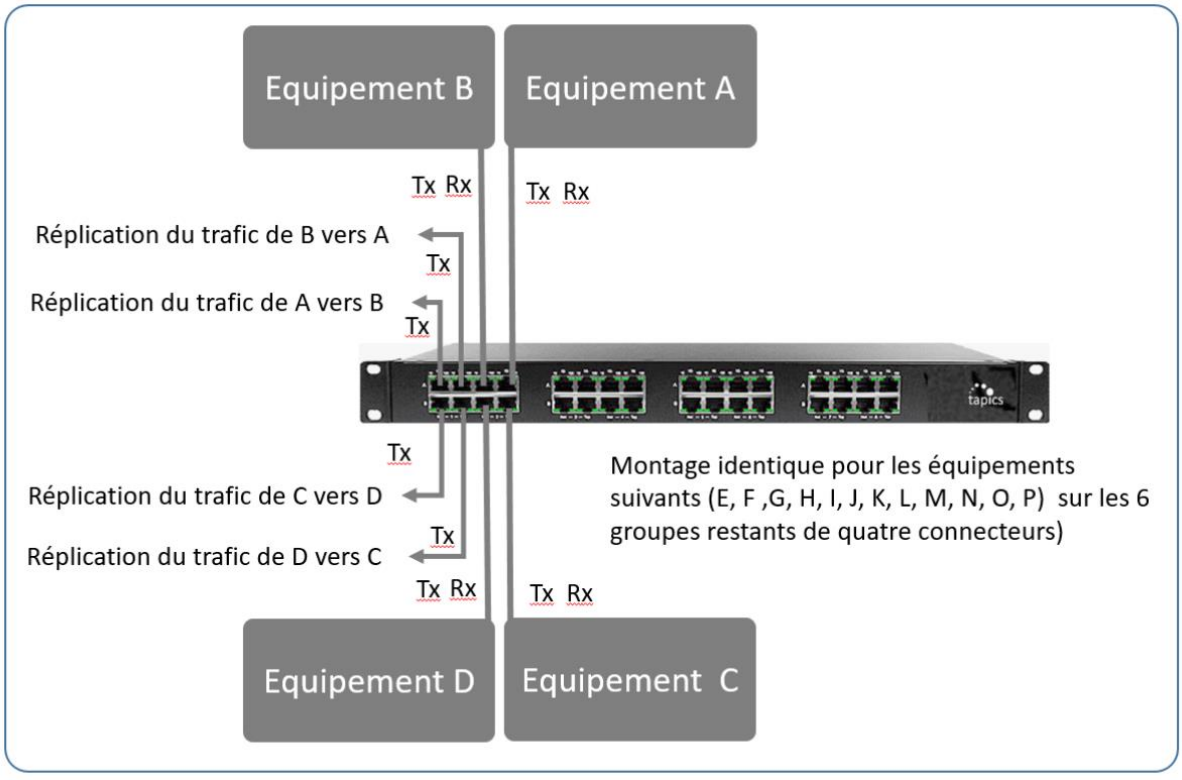
- Des personnels extérieurs qualifiés techniquement pour réaliser l'installation des équipements, employés d'entreprises d'intégration ou d'installation.
- Des techniciens en réseau et des administrateurs du système d'information, employés de l'utilisateur final des produits.

2. 2 Description de la manière d'utiliser le produit

Une fois que le lien réseau Ethernet est connecté, le TAP copie le trafic réseau vers les deux interfaces de monitoring.

Voici les schémas de connexion des TAPs 1 ligne et 8 lignes (l'alimentation électrique n'est pas figurée sur les vues) :





2. 3 Hypothèses sur l'environnement

H1. Environnement physique

On suppose que le TAP est installé dans des locaux sécurisés dont l'accès est limité aux personnels d'intégration autorisés, aux personnels en charge du réseau et aux administrateurs du système d'information, avec un processus adapté de surveillance.

H2. Organisation

Les administrateurs sont considérés comme des personnes de confiance sans intention de nuire.

H3. Alimentation

L'alimentation électrique est correctement fournie par le local informatique dans lequel le TAP est installé.

2. 4 Définition du périmètre de l'évaluation

L'évaluation concerne uniquement les équipements de la gamme Cuivre dans leur version sécurisée : c'est-à-dire la version possédant des scellés [Voir photo du scellé en annexe].

3 Biens sensibles

Les objectifs de sécurité sont les suivants :

B1. Trafic à répliquer

Le trafic que l'on souhaite répliquer doit demeurer disponible et intègre après l'installation du TAP.

B2. Trafic recopié

Le trafic répliqué par le TAP sur ses ports de monitoring doit être disponible, intègre et fidèle.

4 Description des menaces

4. 1 Profil des attaquants

Les différentes sources de menaces identifiées se résument à :

- Une personne interne ou externe ayant un accès aux interfaces de l'équipement.

4. 2 Types de menaces

Pour l'évaluation, les menaces suivantes ont été retenues :

M1. Altération du trafic à répliquer

- Un attaquant parvient à modifier ou supprimer le trafic entre l'entrée et la sortie du TAP, par exemple en modifiant la configuration du TAP ou en injectant du trafic depuis n'importe quelle interface, ou par rayonnement électromagnétiques...

M2. Altération du trafic recopié

- Un attaquant parvient à modifier ou supprimer le trafic recopié sur les interfaces de monitoring.

5 Description des fonctions de sécurité du produit

Les fonctions de sécurité du produit inclues dans le périmètre de l'évaluation sont les suivantes :

FS1. Transparence sur le trafic du réseau

- Le TAP garanti l'absence d'impact sur l'intégrité du trafic sur le réseau.

FS2. Fonction de réplication du trafic

- Le trafic en entrée est répliqué sur l'interface de monitoring de façon fidèle et intègre.

FS3. Anti-reflux (diode)

- Tout trafic venant du port de monitoring ne peut pas passer vers le réseau.