TAPICS

Cible de Sécurité CSPN

TAPs gamme Optique

Version 1.3.15

Page intentionnellement laissée vide

Table des matières

Tableau de révision

Révision	Date	Auteur	Commentaires
0.1	13/11/2015		Version Initiale
1.0	23/11/2015		Première version à publier
1.1	16/12/2015	TAPICS	1ère prise en compte des remarques de l'ANSSI
1.2	-	-	Non utilisée
1.3	21/12/2015	TAPICS	§2.3, §4 et §5 : 2nd prise en compte des remarques de l'ANSSI.
1.3.1	7/1/2016	TAPICS	Correction mineure de syntaxe suite à remarque . §6 ajout de la photographie du scellé.
1.3.2	17/5/2016	TAPICS	Modifications suite à réunion ANSSI/ /TAPICS du 13/4/2016
1.3.3	23/5/2016	TAPICS	Suppression de la table des références
1.3.4	24/5/2016	TAPICS	Modification de la catégorie des produits et correction d'erreurs mineures
1.3.5	26/5/2016		Ajout des profils utilisateurs en §2.1 Suppression doublon en dernière section
1.3.6			Non utilisée
1.3.7	27/6/2016	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
1.3.8	30/9/2016	TAPICS	Modification en §5
1.3.9	12/10/2016	TAPICS	Suppression du §6 sur les scellés
1.3.10	13/10/2016	TAPICS	Mise en cohérence des références de produits testés
1.3.11	19/10/2016	TAPICS	Ajout de la référence optique multimode Correction d'erreur dans la remarque du §1.2 §2.1 modification du second alinea sur les vitesses supportées Ajout d'une colonne dans le tableau en §2.1
1.3.12	14/11/2016	TAPICS	Précisions en FS3 page 8 sur diode optique, correction du tableau page 6
1.3.13	24/1/2017	TAPICS	Transmission à EDSI
1.3.14	19/5/2017	TAPICS	Mise à jour photos TAP multimode
1.3.15	29/5/2017	TAPICS	Suite à demande ANSSI du 29/5/2017 : en annexe, précisions sur les changements opérés et inclusion de la présentation technique du produit.

1 Introduction

1. 1 Identification de la Cible de Sécurité

Ce document décrit la Cible de Sécurité relative aux produits TAPs de la gamme Optique en vue de l'obtention d'une Certification de Sécurité de Premier Niveau (CSPN). Cette Cible de Sécurité prend en compte trois produits sécurisés de la gamme Optique sans dépendre des variantes de ratio (puissance transmise/puissance analysée).

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

1. 2 Identification des produits

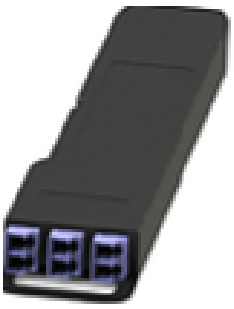
Société éditrice	TAPICS
Lien vers la société	www.tapics.fr
Nom commercial des produits	TAPs optiques
Références des produits évalués	TAMOD-OWL-1310-XX TAMOD-OWL-1550-XX TAMOD-OWL-850-XX
Catégorie des produits	Matériel et logiciel embarqué

Remarque : Dans les références listées ci-dessus, la variable XX est fonction des caractéristiques de ratio de transmission de l'équipement. Ces différences n'ont pas d'impact sur les fonctions de sécurité des produits. Il n'y a pas de différences fonctionnelles entre les TAP hormis leur adaptation à la longueur d'onde du lien réseau.

Ci-après, l'expression *le produit* renvoie à n'importe quel modèle de cette liste de références.

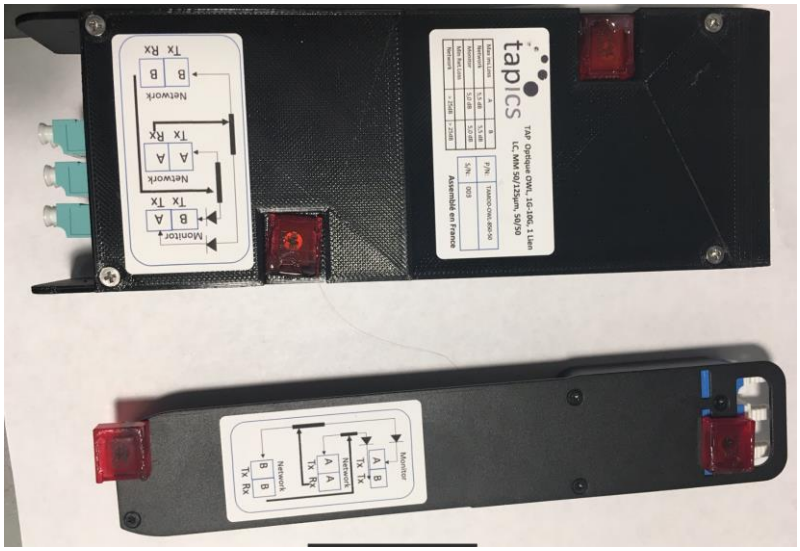
TAMOD-OWL-1310-XX (monomode)

TAMOD-OWL-1550-XX (monomode)



TAMOD-OWL-850-XX (multimode)

Vues comparées :



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.), elle ne doit pas avoir d'effet sur le réseau.

Les TAPs de la gamme Optique possèdent des interfaces optiques supportant des débits de 1Gbps jusqu'à 100Gbps.

Quel que soit le modèle, 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 modèles de TAPs optiques proposés mettent tous en œuvre le même module de couplage optique interne permettant de capter une partie de la puissance optique transmise sur le lien surveillé afin de l'aiguiller vers le port de monitoring. Il n'y a donc aucune différence fonctionnelle ni de caractéristique entre les deux modèles, hormis le nombre de lignes en connexion. Le tableau ci-dessous présente ces deux modèles :

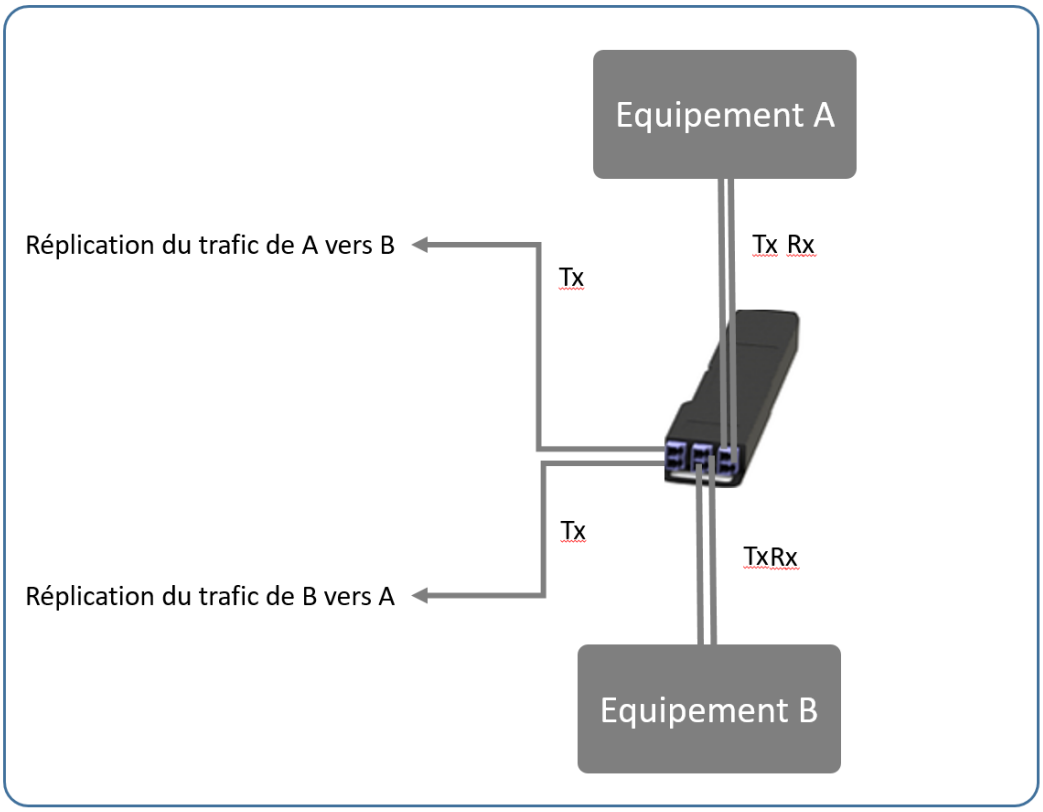
TAMOD-OWL-1310-XX	**TAMOD-OWL-1550-XX**	**TAMOD-OWL-850-XX**
Réplication du trafic d'une ligne optique fibre monomode avec longueur d'onde de 1310 nm, avec diode anti-retour	Réplication du trafic d'une ligne optique fibre monomode avec longueur d'onde de 1550 nm, avec diode anti-retour	Réplication du trafic d'une ligne optique fibre multimode avec longueur d'onde de 850 nm, avec diode anti-retour
Pour source de 1310 nm	Pour source de 1550 nm	Pour source de 850 nm
1 port de réplication	1 port de réplication	1 port 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 optiques de monitoring.


Equipement A
Réplication du trafic de A vers B
Tx
Tx Rx
Tx
TxRx
Réplication du trafic de B vers A
Equipement B

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.

Aucune alimentation électrique n'est nécessaire au fonctionnement de l'équipement.

H2. Organisation

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

2. 4 Définition du périmètre de l'évaluation

L'évaluation concerne uniquement les équipements de la gamme Optique 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 en entrée du trafic à répliquer ou de l'interface de monitoring ...

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 incluses 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 ni perturber le trafic du réseau. Le dispositif de diode ne peut pas être neutralisé. Il produit une atténuation de plus de -25 dB.