Documentation
GTap optique monomode
Modèle GTap O SM

ref.GTAP O1310 1P 5050

ref.GTAP O1310 1P 6040

ref.GTAP O1550 1P 5050

ref.GTAP O1550 1P 6040

Documentation version : V1

Date de création : Juillet, 2024

Dernière mise à jour : Juillet, 2024

Contents

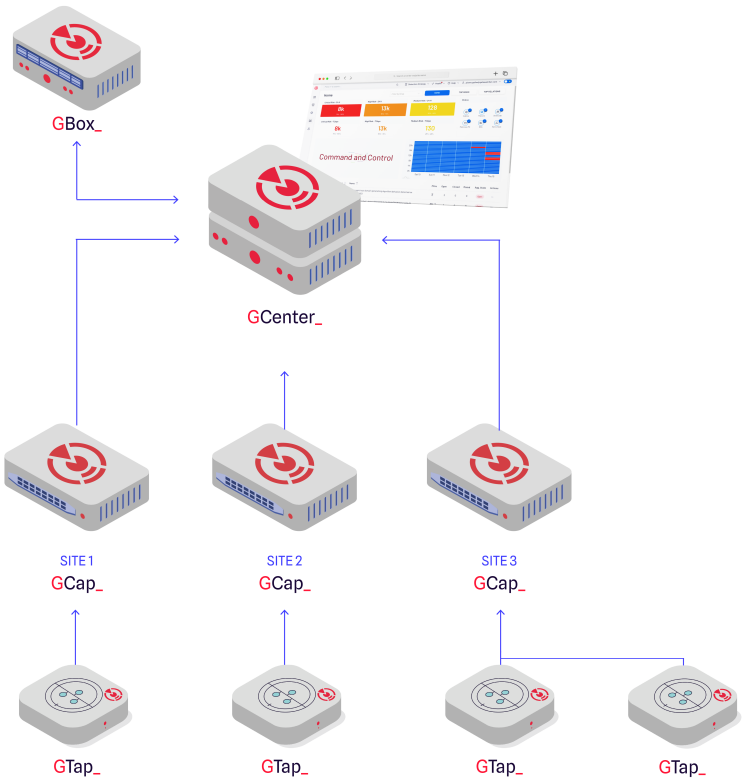
Chapter 1

Description

1.1 Introduction

La solution TRACKWATCH®/AIONIQ® est la plateforme de détection des intrusions informatiques – IDS (Intrusion Detection System) proposée par Gatewatcher®.
Elle comprend :

- un ou plusieurs GTap
- un ou plusieurs GCap
- un GCenter
- une GBox (optionnelle)



1.2 Présentation du GTap

Le GTap modèle GTAP_O_SM est composé d'un Tap permettant de dupliquer le flux réseau connecté sur les ports `A` et `B`.
Le GTAP_O_SM est identifié par quatre références distinctes :

- GTAP_O1310_1P_5050
- GTAP_O1310_1P_6040
- GTAP_O1550_1P_5050
- GTAP_O1550_1P_6040

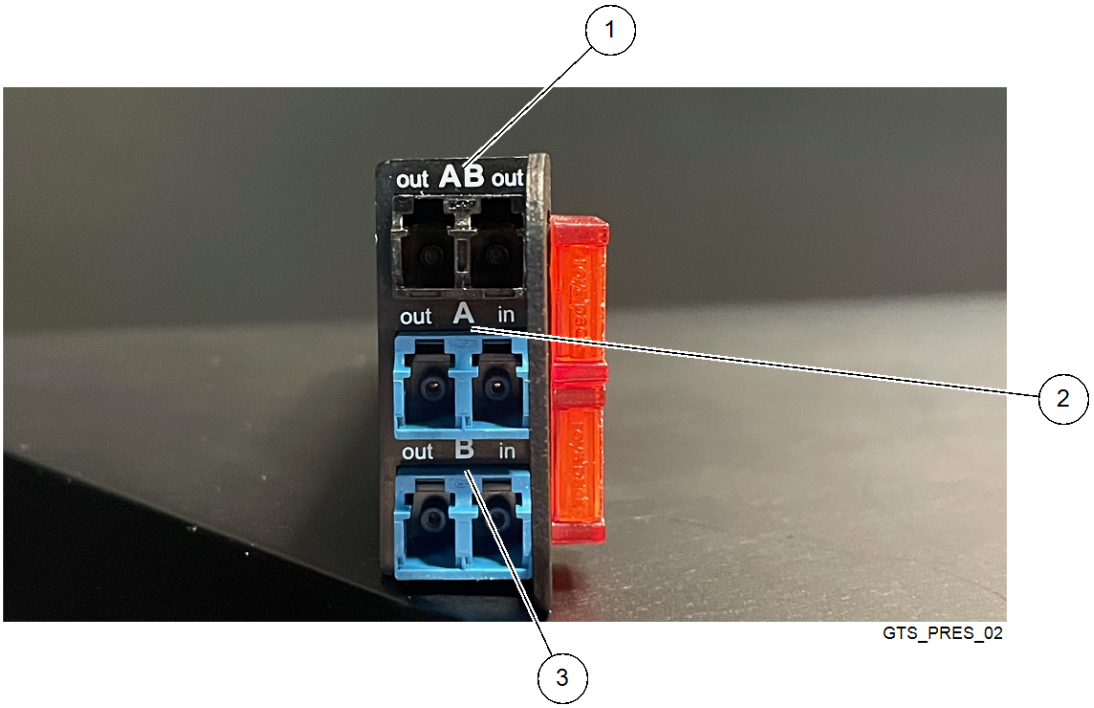
Le GTap se présente sous la forme suivante :

GTS_PRES_01

1.2.1 Liste des entrées / sorties du GTap

Le GTap_O_SM dispose d'un total de trois ports LC (Lucent Connector) duplex :

- les ports du réseau à surveiller : `A` et `B`
- le port à connecter à la sonde détection : `AB`



Repère	Description
1	AB : port de sortie du Tap connecté à la sonde de détection
2	A : port d'entrée du Tap connecté au réseau à surveiller
3	B : port d'entrée du Tap connecté au réseau à surveiller

Note:

Appliquer les bonnes pratiques pour l'insertion d'un Tap sur un réseau.
Si besoin, contacter le support Gatewatcher ou contacter votre interlocuteur Gatewatcher habituel.

1.2.2 Scellés de sécurité

Le GTap possède également trois scellés de sécurité, situés sur la face droite de l'équipement :

Repère	Description
1	Scellé n°1
2	Scellé n°2
3	Scellé n°3

1.2.3 Contenu du colis

Le colis comprend le GTap modèle GTAP_O_SM.

Chapter 2

Fonctionnement

2.1 Fonction du Tap

Le GTap empêche toute attaque ou perturbation potentielle en bloquant la lumière provenant des ports du moniteur.
Le GTap surveille les sept couches OSI.
Le GTap n'est pas configurable et donc ne possède pas d'interface de gestion/administration.
Le GTap ne mémorise pas le trafic.
Le GTap est non intrusif et donc ne perturbe pas le trafic à répliquer.

Selon le modèle, le GTap possède un ratio de répartition différent :

- GTAP_O1310_1P_5050: ratio de répartition de 50/50
- GTAP_O1310_1P_6040: ratio de répartition de 60/40
- GTAP_O1550_1P_5050: ratio de répartition de 50/50
- GTAP_O1550_1P_6040: ratio de répartition de 60/40

2.2 Connecteurs réseau LC

Les connecteurs réseau du GTap sont précisés dans la *Liste des entrées / sorties du GTap*.

2.3 Alimentation électrique

Le GTap ne possède pas d'alimentation électrique.

Chapter 3

Caractéristiques

Référence	Type de fibre (µm)	Longueur d'ondes (nm)	Ratio de répartition	Perte d'insertion maximale (dB) NET / TAP	Dimensions (mm)	Poids (g)
GTAP_O1310_1P_5050	Monomode 9	1310	50/50	3,6 / 4,4	41 x 17 x 217	76
GTAP_O1310_1P_6040	Monomode 9	1310	60/40	2,7 / 5,5	41 x 17 x 217	76
GTAP_O1550_1P_5050	Monomode 9	1550	50/50	3,6 / 4,4	41 x 17 x 217	76
GTAP_O1550_1P_6040	Monomode 9	1550	60/40	2,7 / 5,5	41 x 17 x 217	76

Chapter 4

Cas d'utilisation

4.1 Procédure de contrôle de la livraison

4.1.1 Introduction

Le GTap est livré avec trois scellés de sécurité personnalisés ayant une identification unique qui assure la traçabilité tout au long de la chaîne d'approvisionnement.
Ces scellés de sécurité ont été photographiés avant leur expédition afin de hausser le niveau de sécurité qu'ils offrent.
Nous vous demandons de prendre une photo de chaque scellé de sécurité et de les télécharger sur le disque partagé.
Nous les comparerons et confirmerons l'intégrité de votre équipement.

Pendant la durée de la procédure, l'équipement doit être stocké dans une installation sécurisée.
Cette installation :

- doit avoir un accès strictement limité au personnel autorisé et
- doit faire l'objet d'un processus de surveillance approprié.

Note:

Le dispositif est livré avec des étiquettes de sécurité personnalisées ainsi qu'avec une identification unique qui assure la traçabilité tout au long de la chaîne d'approvisionnement.
Merci de bien vouloir vérifier l'intégrité des scellés et des étiquettes ainsi que la correspondance de l'identifiant.

4.1.2 Procédure préliminaire

Note:

L'accès au disque partagé est fourni par le biais d'un ticket ouvert par notre équipe de support sur votre compte TAC.

- Vérifier la présence d'un lien vers le disque partagé sur votre compte TAC.
  Si ce lien n'a pas été reçu, solliciter le support de Gatewatcher afin de l'obtenir.
  Si besoin, contacter le support Gatewatcher ou contacter votre interlocuteur Gatewatcher habituel.

4.1.3 Procédure

- Ouvrir le colis.
- Vérifier la présence des scellés de sécurité.
- Prendre une photo en haute définition de chaque scellé de sécurité, comme illustré dans les exemples ci-dessous. Le GTap en possède trois, soit deux photos au total.

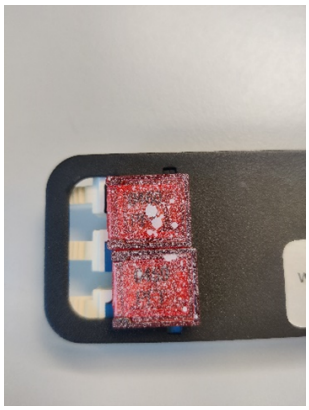


Figure1: exemple 1

Figure2: exemple 2

- Cliquer sur le lien vers le disque partagé.
- Télécharger toutes les photos sur le disque partagé vers le répertoire défini ci-dessous.

Le nom du répertoire est la référence de la commande et à l'intérieur, vous trouverez un répertoire pour chaque GTap (référencé par le numéro de série).
Merci de bien vouloir télécharger les photos dans le répertoire correspondant à chaque GTap.

- Répondre au ticket du TAC pour confirmer le téléchargement des photos.
  Une fois le contrôle effectué par nos soins, nous vous communiquerons l'état de l'intégrité de votre équipement.
- Si l'intégrité est correcte, utiliser le GTap.
  Sinon, veuillez le renvoyer.

4.2 Procédure d'installation

4.2.1 Procédure préliminaire

Important:

Avant l'installation, veiller à contrôler l'intégrité de l'équipement en suivant la *Procédure de contrôle de la livraison*.

Note:

Pour capturer le flux du réseau à surveiller, insérer le GTap dans le réseau existant.
Ceci peut se faire soit :

- en remplaçant une jarretière optique LC duplex multimode par deux jarretières de même type
- en utilisant les ports mirroring du commutateur si celui-ci en est équipé

- Appliquer les bonnes pratiques pour l'insertion d'un Tap sur un réseau.
  Si besoin, contacter le support Gatewatcher ou contacter votre interlocuteur Gatewatcher habituel.
- Procédure pour installer les GTap dans un rack :
  - Insérer les GTap dans le rack jusqu'à entendre le clic indiquant qu'ils sont fixés dans les rails internes.
  - Si les GTap s'insèrent difficilement dans le rack, vérifier que les rails internes sont situés au bas de ce dernier et que les GTap sont alignés sur les rails internes, le texte de la face avant à la verticale.

  Note:

  Un rack de 19 pouces peut contenir jusqu'à 16 GTap_O_SM.

- Si besoin, monter le rack dans une baie et le fixer.

  Note:

  La hauteur du rack de GTap est de 1U.

Important:

La propreté de la fibre optique est primordiale pour une bonne transmission du signal car la poussière et d'autres particules microscopiques peuvent perturber ou bloquer le signal.

Il est recommandé de conserver les capuchons anti-poussière sur les connecteurs non utilisés afin de réduire le risque de contamination.

En cas de signal faible ou d'absence de signal, la première mesure à prendre est de nettoyer les câbles et les connecteurs.

Avant de les connecter, il est recommandé de nettoyer les jarretières optiques et les connecteurs à l'aide d'un équipement de nettoyage des fibres optiques approprié.

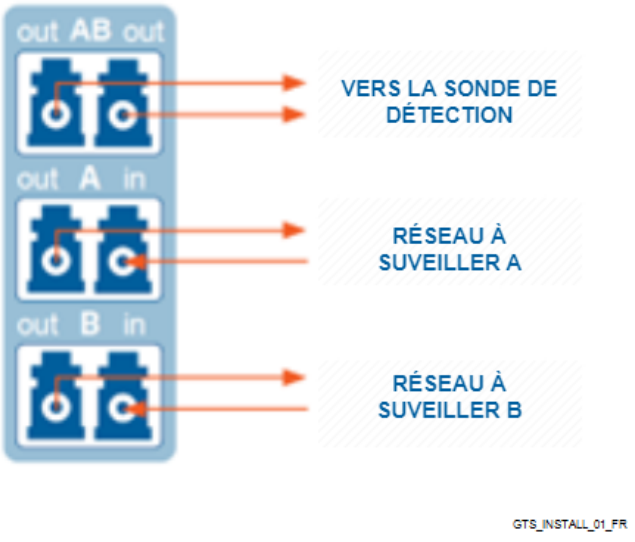
4.2.2 Procédure

- Connexion au réseau à surveiller :
  - Connecter la jarretière optique LC duplex multimode du réseau à surveiller sur le port `A`.
  - Connecter la jarretière optique LC duplex multimode du réseau à surveiller sur le port `B`.

Note:

Pour chaque jarretière, enlever les caches protégeant les fibres et connecter la jarretière.

- Connexion à la sonde de détection :
  - Connecter le port `AB` à la sonde de détection à l'aide d'une jarretière optique LC duplex multimode.
  - Connecter les jarretières comme sur le schéma ci-dessous :



Chapter 5

Annexes

5.1 Informations juridiques

5.1.1 Clause de non-responsabilité

Le fabricant ne fait aucune déclaration ni ne donne aucune garantie concernant le contenu du présent document et rejette toute garantie implicite de qualité marchande ou de conformité à un usage particulier.
Le fabricant se réserve le droit de réviser cette publication et d'en modifier le contenu sans obligation de notifier à qui que ce soit une telle révision ou modification.

5.1.2 Copyright

5.1.3 Marques déposées

Les marques déposées mentionnées dans ce manuel sont la propriété exclusive de Gatewatcher :

- TRACKWATCH®/AIONIQ®
- Gatewatcher®

5.2 LPM

5.2.1 Rappels réglementaires

Quelques rappels sur les grands principes de la LPM française :

- Loi de Programmation Militaire (loi n°2013-1168 du 18 décembre 2013)
- Article 22 : mise en application supervisée par l'ANSSI auprès des OIV
  - Imposer des mesures de sécurité
  - Imposer des contrôles sur les systèmes d'information les plus critiques
  - Rendre obligatoire la déclaration des incidents constatés par les OIV sur leurs systèmes d'information
- Article L. 1332-6-1 du Code de la Défense modifié par LOI n°2015-917 du 28 juillet 2015 - art. 27
  - Instaurer des mesures organisationnelles et techniques
  - Définir des modalités d'identification et de notification des incidents de sécurité affectant les SIIV

5.2.2 Rappels des objectifs

Les objectifs sont de :

- protéger les infrastructures vitales nationales contre les attaques informatiques,
- réduire l'exposition aux risques et
- optimiser la qualité des services fournis par les organisations.

5.2.3 Rappels des exigences

Des exigences pour les OIV et les acteurs PDIS sont à prendre en compte sur les équipements :

- mettre en place une politique de sécurité des systèmes d'information
- conduire une homologation de sécurité
- communiquer les éléments sur le SIIV mis en place par l'opérateur à l'ANSSI
- observer les alertes de sécurité et réagir à celles-ci
- limiter les accès
- cloisonner les réseaux
- sélectionner les technologies qualifiées

5.2.4 LPM appliquée au GTap

Le GTap modèle GTAP_O_SM est conforme avec la Loi de Programmation Militaire et est qualifié par l'ANSSI.

Chapter 6

Glossaire

GBox
: La GBox est un équipement pouvant fonctionner de manière autonome ou conjointement avec le GCenter. Elle dispose de quatre moteurs d'analyse complémentaires et d'un moteur pour détecter des noms de domaines ayant été générés par des DGA.

GCap
: Le GCap est la sonde de détection de la solution Trackwatch/Aioniq. Elle récupère le flux réseau du GTap et reconstitue les fichiers qu'elle envoie au GCenter.

GCenter
: Le GCenter est le composant qui administre le GCap et effectue l'analyse des fichiers envoyés par le GCap.

GTap
: Le GTap est un dispositif passif qui duplique le flux d'un réseau et le recopie intégralement, sans le mémoriser ni l'impacter.

IDS
: Les systèmes de détection d'intrusion sont des systèmes logiciels ou matériels conçus pour automatiser la surveillance des événements se produisant dans un réseau ou sur une machine particulière, et pour pouvoir faire rapport à l'administrateur système, toute trace d'activité anormale sur ce dernier ou sur la machine surveillée.

OSI
: Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel qui définit comment les systèmes réseau communiquent et envoient des données d'un expéditeur à un destinataire. Il contient sept couches qui s'empilent conceptuellement de bas en haut.

TAC
: Le TAC (Technical Assistance Center) est la plateforme de support de Gatewatcher.

Index