Documentation
GTap cuivre 8 liens Gigabit
Modèle GTap CU 8P

Documentation version : V2

Date de création : Juin, 2024

Dernière mise à jour : Juillet, 2024

Contents

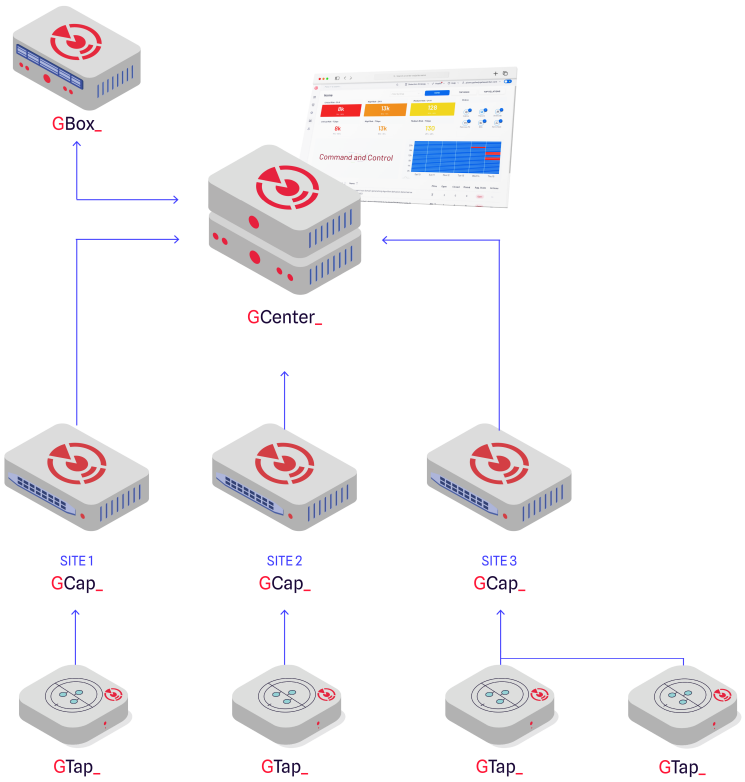
Chapter 1

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

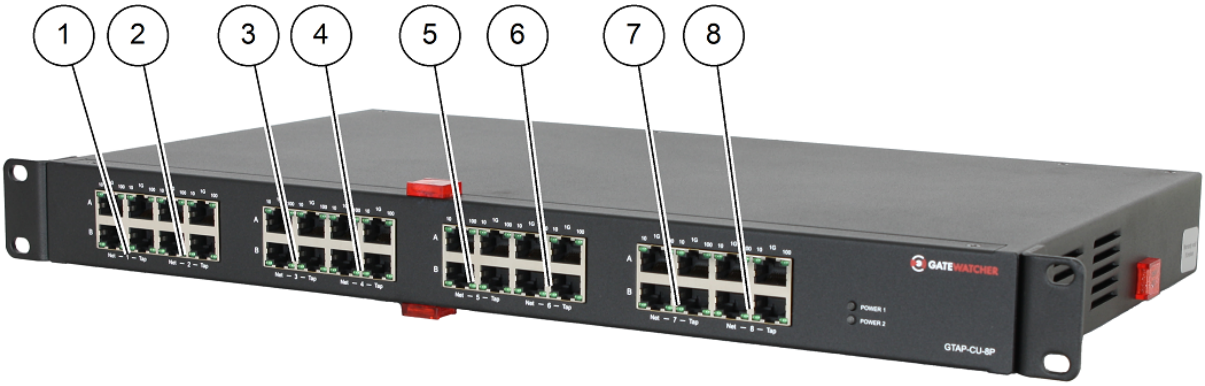
Le GTap modèle GTAP_CU_8P est composé de :

- huit Tap unitaires indépendants permettant chacun de dupliquer le flux réseau connecté sur les ports `Net`
- un châssis mécanique (1U/19 pouces) pour être fixé dans une baie
- deux alimentations redondantes

Le GTap se présente sous la forme suivante :

1.2.1 Liste des entrées / sorties du GTap

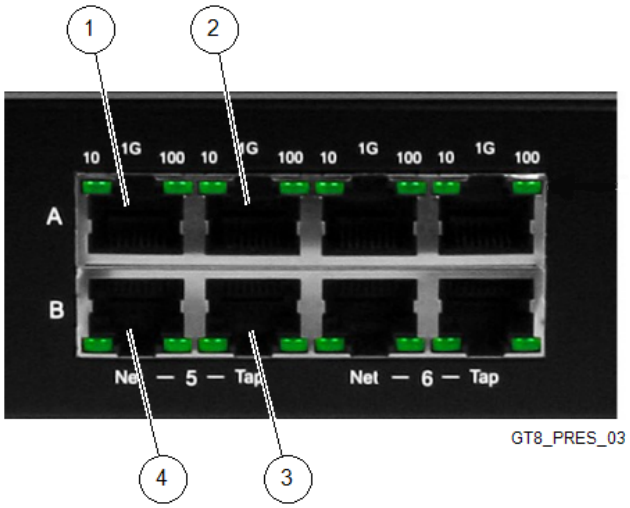
Le **GTap** possède huit Taps unitaires numérotés de 1 à 8 :



GT8_PRES_02

Repère	Description
1	Tap unitaire n°1
2	Tap unitaire n°2
3	Tap unitaire n°3
4	Tap unitaire n°4
5	Tap unitaire n°5
6	Tap unitaire n°6
7	Tap unitaire n°7
8	Tap unitaire n°8

Ces Tap unitaires possèdent chacun quatre ports :



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

En face arrière, les deux connecteurs d'alimentation C14 sont nommés <POWER 1> et <POWER 2>.

1.2.2 Scellés de sécurité

Le GTap possède également six scellés de sécurité, ils sont repérés de la façon suivante :

Repère	Description
1	Scellé n°1
2	Scellé n°2
3	Scellé n°3
4	Scellé n°4
5	Scellé n°5
6	Scellé n°6

1.2.3 Contenu du colis

Le colis comprend :

- le GTap modèle GTAP_CU_8P
- deux cordons d'alimentation Fiche mâle de type E (CEE 7/7) / prise C13

Chapter 2

Fonctionnement

2.1 Fonction du Tap

Chaque Tap unitaire recopie fidèlement l'ensemble du trafic entrant dans les ports RJ45 (Net A et Net B) en gardant le même débit réseau (10/100/1000 BASE-T).
Le Tap surveille les sept couches OSI et duplique :

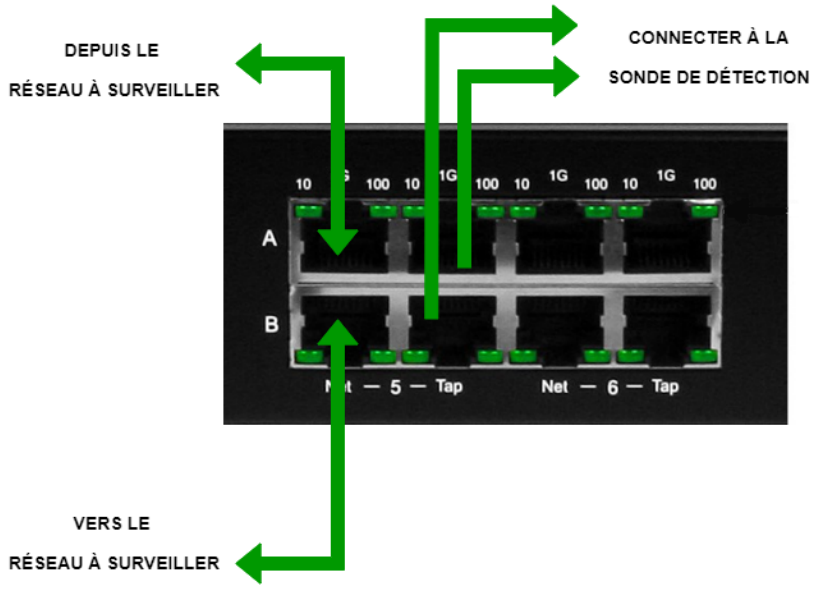
- les paquets de toutes tailles et de tous types
- les erreurs de bas niveau et le trafic VLAN

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.
Le GTap n'a pas d'adresse IP et isole le réseau à surveiller du dispositif de surveillance.
Une fois en place, le GTap permet de connecter et de déconnecter à volonté les dispositifs de surveillance, sans impact sur la liaison du réseau à surveiller.

2.2 Connecteurs réseau RJ45

Le GTap_CU_8P dispose d'un total de 32 ports RJ45, pour huit Tap unitaires (numérotés de 1 à 8).
Chaque Tap unitaire est composé de quatre ports :

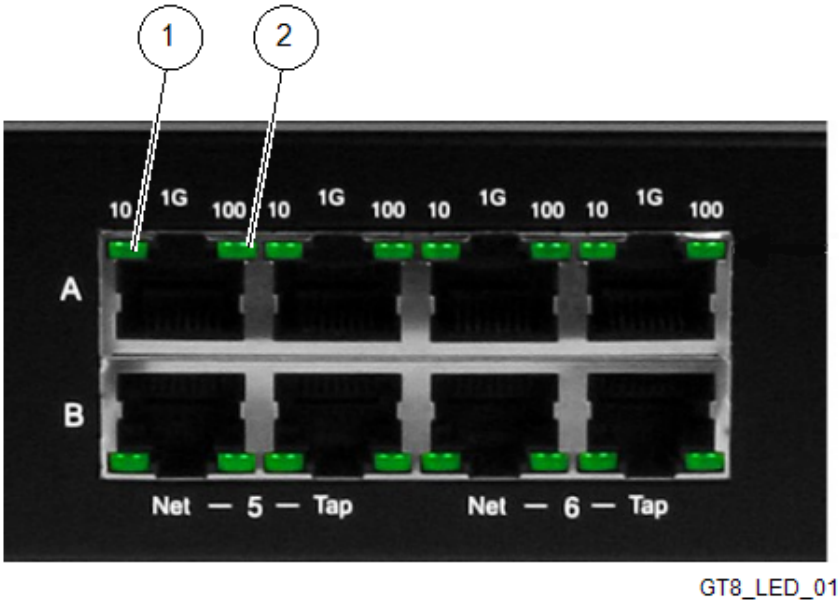
- les ports du réseau à surveiller : `` `Net A` `` et `` `Net B` ``
- les ports à connecter à la sonde détection : `` `Tap A` `` et `` `Tap B` ``



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.

2.3 LED 10 et LED 100



GT8_LED_01

Repère	Description
1	LED 10 Mb/s
2	LED 100 Mb/s

Après négociation sur les ports réseau actifs et connectés, l'allumage fixe des LED indique la vitesse du réseau :

- LED 10 (1) est allumée fixe pour une connexion à 10 Mb/s
- LED 100 (2) est allumée fixe pour une connexion à 100 Mb/s
- Les deux LED sont allumées fixe pour une connexion à 1 Gb/s

Le clignotement signifie qu'un signal est détecté et qu'un seul câble réseau est connecté.

2.4 Alimentation électrique

Le GTap est doté de deux alimentations électriques redondantes.

La présence de l'alimentation est indiquée par les LED <POWER 1> et <POWER 2>.

En cas de panne d'une alimentation (extinction d'une des deux LED), contacter le support Gatewatcher.

En cas de coupure de courant totale, le GTap passe instantanément en mode totalement passif pour que la liaison réseau surveillée reste opérationnelle.

Chapter 3

Caractéristiques

	CARACTÉRISTIQUES
Connecteurs	8 Tap unitaires (4 ports RJ45 par Tap), plaqués or
LED	2 LED 10/100 par port RJ45 (Speed, Link, Activity) 1 LED POWER par alimentation (présence tension)
Alimentation électrique	2 x 100-240VAC stabilisé, 50-60Hz, 50W
Consommation électrique	50W
MTBF (temps moyen entre pannes)	150 000 heures
Structure	Acier et aluminium, peinture noire
Dimensions (H x L x P)	44 x 440 x 260 mm (1U/19 pouces)
Poids	3,6 kg
Température d'utilisation	0 °C à 50 °C
Température de stockage	-20 °C à 70 °C
Humidité	10 à 90 %, sans condensation
Certifications	RoHS — CE — FCC classe A IEEE 802.3 — UL 62368-1

Chapter 4

Cas d'utilisation

4.1 Procédure de contrôle de la livraison

4.1.1 Introduction

Le GTap est livré avec six scellés de sécurité personnalisés, chacun 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 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 de chaque scellé de sécurité.
- Prendre des photos en haute définition de chaque scellé de sécurité (le GTap CU_8P en possède six, soit six photos au total).
  - Prendre les photos comme suit :

Figure1: Exemple1

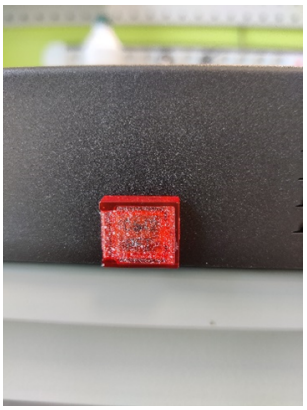


Figure2: Exemple2

- 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 un câble réseau existant par deux câbles de dérivation vers le Tap
- 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.
- Ne pas mettre le GTap sous tension.
- Si besoin, monter le GTap dans une baie (19 pouces) et le fixer.

Note:

La hauteur du GTap est de 1U sans les scellés de sécurité.

4.2.2 Procédure

- Connexion des câbles d'alimentation du GTap :

Note:

Recommandation : connecter les alimentations du GTap sur deux nourrices différentes, elles-mêmes connectées à des lignes d'alimentation séparées avec des disjonctions différentes.

  - connecter le premier cordon d'alimentation C13 fourni :
    * d'un coté au connecteur <POWER 1> (type C14) du GTap
    * de l'autre coté à la première nourrice de la baie

Important:

N'utiliser que des cordons d'alimentation et des nourrices correctement reliés à la terre.
Les nourrices doivent rester facilement accessibles après l'installation.

  - connecter le deuxième cordon d'alimentation C13 fourni :
    * d'un coté au connecteur <POWER 2> (type C14) du GTap
    * de l'autre coté à la deuxième nourrice de la baie
- Vérification de l'alimentation électrique du GTap :
  - Vérifier que les LED <POWER 1> et <POWER 2> sont bien allumées.

    Si ce n'est pas le cas, vérifier que les câbles soient correctement enfoncés dans les prises et que les nourrices de la baie soient bien alimentées.
- Connexion au réseau à surveiller :
  - connecter les câbles du réseau à surveiller sur les connecteurs `Net A` et `Net B`.
    * Utiliser des câbles RJ45 UTP de catégorie 5e ou supérieure.

      Dans le cas d'un équipement réseau 10/100 MB ne prenant pas en charge l'auto-crossover :
      · utiliser deux câbles droits si les périphériques réseau sont de type différent (un DTE et un DCE)
      · utiliser un câble droit et un câble croisé si les deux périphériques réseau sont du même type (tous deux DTE ou tous deux DCE)
- Vérification du flux réseau à surveiller avec les LED :

  Après négociation sur les ports réseau actifs et connectés, l'allumage fixe des LED indique la vitesse du réseau :
  - LED 10 (1) est allumée fixe pour une connexion à 10 Mb/s
  - LED 100 (2) est allumée fixe pour une connexion à 100 Mb/s
  - Les deux LED sont allumées fixe pour une connexion à 1 Gb/s

  Le clignotement signifie qu'un signal est détecté et qu'un seul câble réseau est connecté.
  - Vérifier que les LED `Net A` et `Net B` des Tap unitaires utilisés soient allumées de façon fixe.

    Si les LED d'un Tap unitaire clignotent, vérifier ses câbles et ses connexions.
  - Vérifier l'activité du réseau à surveiller.

    Pour cela, vérifier que les LED des `Net A` et `Net B` des Tap unitaires utilisés clignotent rapidement.
- Connexion vers la sonde de détection :
  - connecter les ports `Tap A` et `Tap B` de chaque Tap unitaire à sa sonde de détection, à l'aide de câbles RJ45 UTP, droits ou croisés, de catégorie 5e ou supérieure.

    Note:

    Un Tap alimenté corrigera toujours une mauvaise configuration de câble.
    Le trafic réseau reçu sur le port `Net A` est dupliqué sur le port `Tap A` et le trafic réseau reçu sur le port `Net B` est dupliqué sur le port `Tap B`.
    La distance maximale entre les dispositifs connectés est de 100 mètres.

- Vérification du flux réseau à surveiller avec les LED :

  Note:

  Les ports surveillés `Tap` fonctionnent à la même vitesse que les ports d'entrés réseau `Net`.

  - Vérification de la vitesse des liens `Tap` :
    * vérifier que les LED (10 et 100) de chaque port `Tap` et `Net` utilisés soient allumées de façon identique.
  - Vérification de l'activité du réseau à surveiller :
    * vérifier que les LED des `Tap A` et `Tap B` utilisés clignotent rapidement.

Chapter 5

Annexes

5.1 Consignes de sécurité

Cet équipement n'est pas adapté à une utilisation dans des lieux où des enfants sont susceptibles d'être présents.
Ce dispositif comporte plusieurs alimentations électriques.

- Débrancher TOUS les cordons d'alimentation lors de la dépose/repose.
- Ne pas pousser ou forcer d'objets à travers quelconque ouverture du cadre du châssis, cela pourrait provoquer un choc électrique ou un départ d'incendie.
- Éviter de renverser du liquide sur l'équipement, cela pourrait provoquer des décharges électriques ou endommager l'équipement.

5.2 Informations juridiques

5.2.1 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.

5.2.2 Copyright

5.2.3 Marques déposées

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

- TRACKWATCH®/AIONIQ®
- Gatewatcher®

5.3 LPM

5.3.1 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

5.3.2 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.

5.3.3 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

5.3.4 LPM appliquée au GTap

Le GTap modèle GTAP_CU_8P 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 TAP 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.

PSU
: Le PSU (Power Supply Unit) est l'unité d'alimentation électrique.

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

Index