Documentation
GTap CU_1P

Documentation version : V1

Date de création : Juillet, 2024

Dernière mise à jour : Juillet, 2024

Contents

Contents i

1 Description 1
- 1.1 Introduction . . . 1
- 1.2 Présentation du GTap . . . 2
  - 1.2.1 Liste des entrées / sorties du GTap . . . 2
  - 1.2.2 Scellés de sécurité . . . 3
  - 1.2.3 Étiquettes de sécurité . . . 4
  - 1.2.4 Contenu du colis . . . 4

2 Fonctionnement 6
- 2.1 Fonction du Tap . . . 6
  - 2.1.1 Propagation des défaillances de liaison (LFP) . . . 6
- 2.2 Connecteurs réseau RJ45 . . . 7
- 2.3 LED . . . 7
- 2.4 Alimentation électrique . . . 8
  - 2.4.1 Fast Failover . . . 8

3 Caractéristiques 9

4 Cas d'utilisation 10
- 4.1 Procédure de contrôle de la livraison . . . 10
  - 4.1.1 Introduction . . . 10
  - 4.1.2 Procédure préliminaire . . . 11
  - 4.1.3 Procédure . . . 11
- 4.2 Procédure d'installation . . . 12
  - 4.2.1 Procédure préliminaire . . . 12
  - 4.2.2 Procédure . . . 13

5 Annexes 15
- 5.1 Consignes de sécurité . . . 15
- 5.2 Informations juridiques . . . 15
  - 5.2.1 Clause de non-responsabilité . . . 15
  - 5.2.2 Copyright . . . 15
  - 5.2.3 Marques déposées . . . 16

6 Glossaire 17

Index 18

Index 18

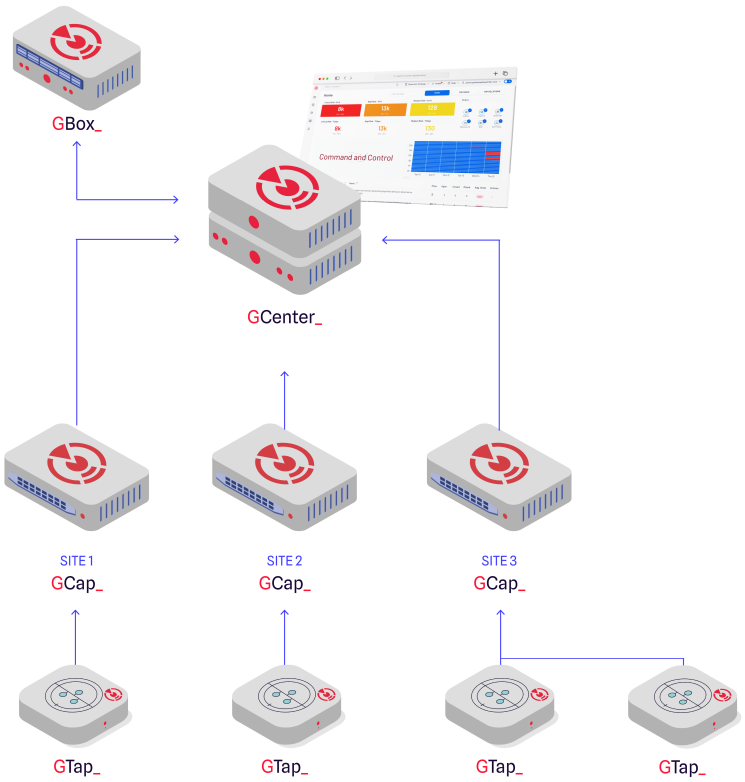
Chapter 1

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_1P est composé de :

- un Tap permettant de dupliquer le flux réseau connecté sur les ports `Network`
- une alimentation externe

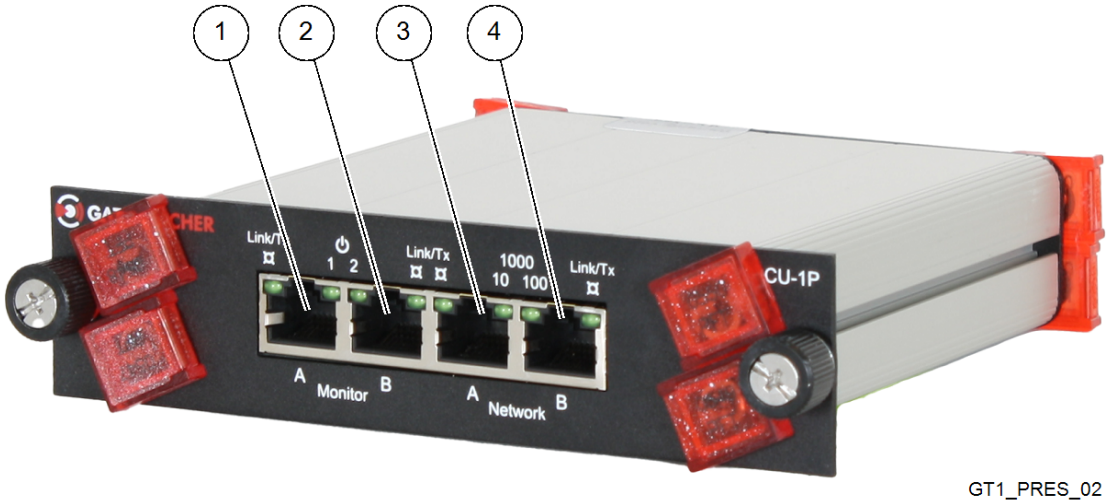
Le GTap se présente sous la forme suivante :

GT1_PRES_01

Note:

Le GTAP_CU_1P est vendu individuellement mais un rack de trois est disponible en option pour une installation en baie.
Si besoin, contacter le support Gatewatcher ou contacter votre interlocuteur Gatewatcher habituel.

1.2.1 Liste des entrées / sorties du GTap



GT1_PRES_02

Le **GTap** possède quatre ports :

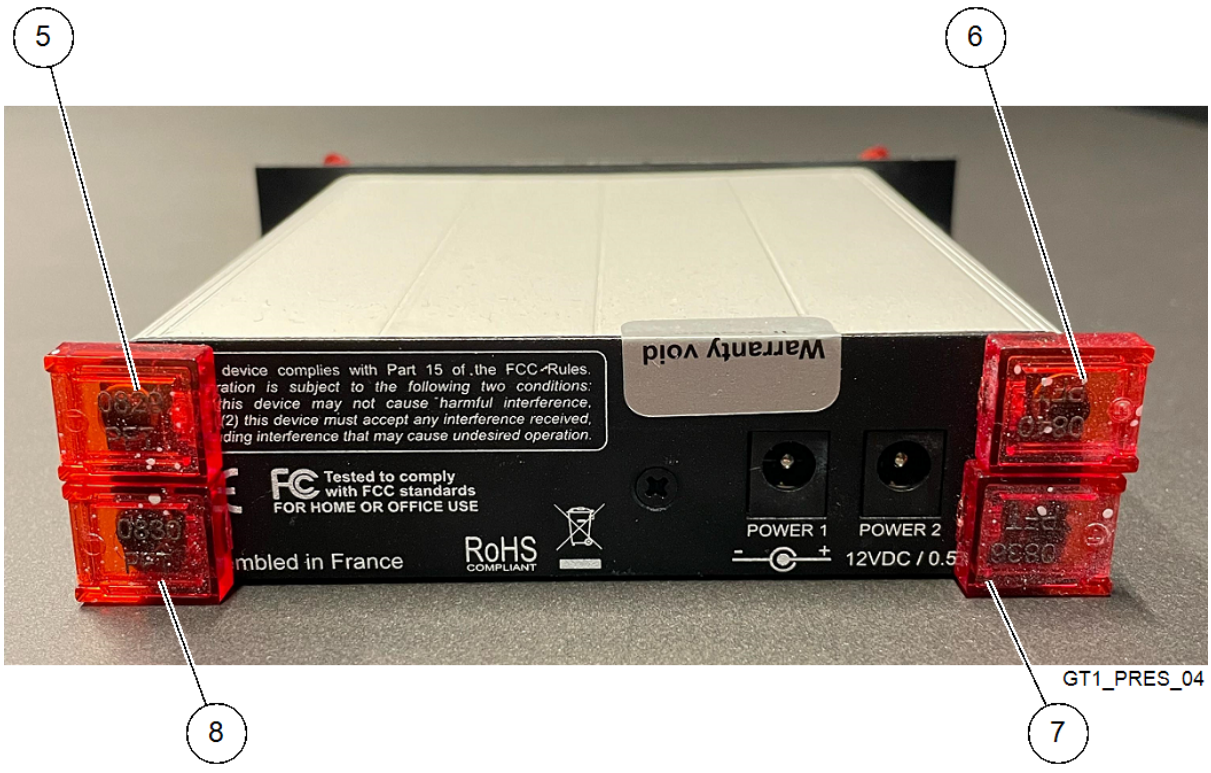
Repère	Description
1	Monitor A : port de sortie du Tap connecté à la sonde de détection
2	Monitor B : port de sortie du Tap connecté à la sonde de détection
3	Network A : port d'entrée du Tap connecté au réseau à surveiller
4	Network B : port d'entrée du Tap connecté au réseau à surveiller

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

1.2.2 Scellés de sécurité

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

GT1_PRES_03



GT1_PRES_04

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
7	Scellé n°7
8	Scellé n°8

1.2.3 Étiquettes de sécurité

Le GTap possède une étiquette de sécurité argentée, située à l'arrière de l'équipement, qui se présente sous la forme suivante :

GT1_PRES_05

L'alimentation électrique fournie avec le GTap possède également deux étiquettes de sécurité argentées, qui se présentent sous la forme suivante :

1.2.4 Contenu du colis

Le colis comprend :

- le GTap modèle GTAP_CU_1P
- une alimentation 100-240VAC / 12VDC 1,5A / prise C14
- une deuxième alimentation 100-240VAC / 12VDC 1,5A / prise C14 (option lors de la commande)

GT1_PRES_06

Figure1: Vue côté gauche

GT1_PRES_07

Figure2: Vue côté droit

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.

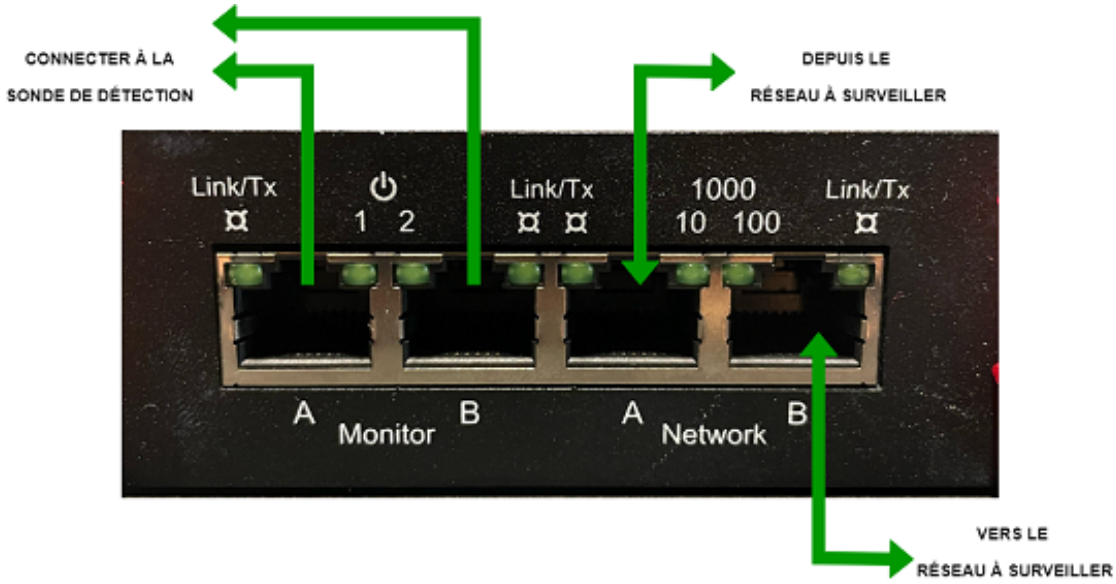
2.1.1 Propagation des défaillances de liaison (LFP)

Le GTap transmet automatiquement les erreurs de défaillance de liaison entre les ports, ce qui permet au réseau d'activer un chemin redondant, tandis que le Tap reste disponible pour l'autonégociation.
Le LFP permet de réduire les temps d'arrêt et est essentiel pour les réseaux à haute disponibilité.

2.2 Connecteurs réseau RJ45

Le GTap_CU_1P dispose d'un total de quatre ports RJ45 :

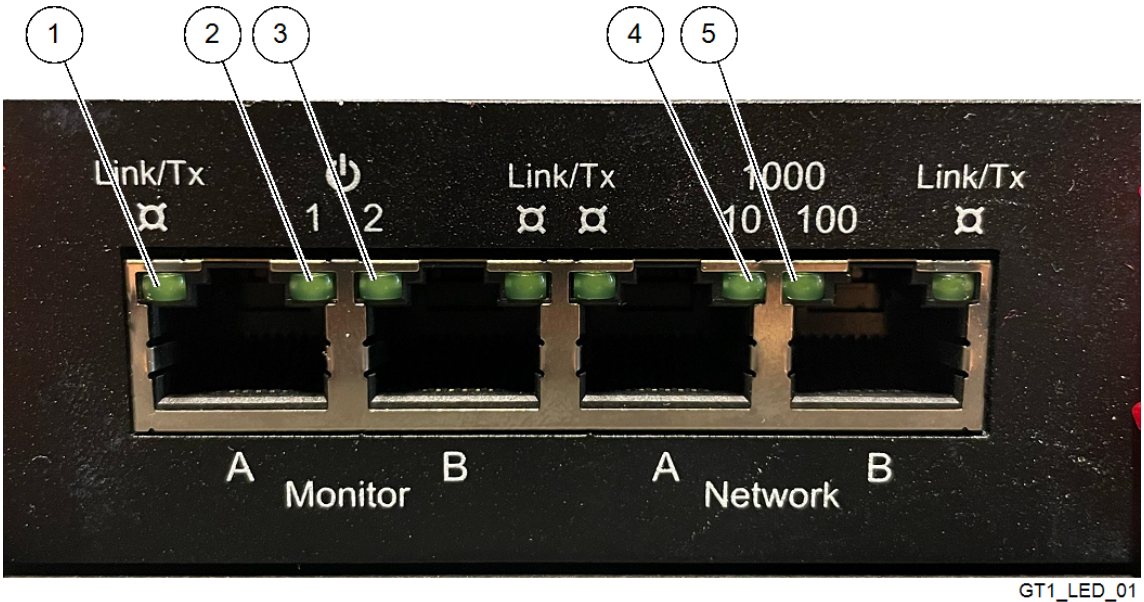
- les ports du réseau à surveiller : `Network A` et `Network B`
- les ports à connecter à la sonde de détection : `Monitor A` et `Monitor B`



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



GT1_LED_01

Repère	Description
1	LED Link/Activity
2	LED <POWER 1>
3	LED <POWER 2>
4	LED 10 Mb/s
5	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 (LED Link/Activity)

2.4 Alimentation électrique

Le GTap est doté d'une alimentation électrique (ou de deux alimentations électriques redondantes si présence de la deuxième).

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 active ses circuits de dérivation et connecte les ports `` `Network A` `` et `` `Network B` `` ensemble. Les ports `` `Monitor` `` sont désactivés lorsque le Tap n'est pas alimenté.

Note:

La deuxième alimentation électrique est une option lors de la commande du GTap.

L'achat de cette alimentation à l'unité reste possible après avoir passé commande.

Si besoin, contacter le support Gatewatcher ou contacter votre interlocuteur Gatewatcher habituel.

2.4.1 Fast Failover

Lorsqu'un changement d'alimentation se produit, les appareils du réseau renégocient la liaison.

Cette opération peut prendre jusqu'à 5 secondes en fonction de la configuration du réseau et peut entraîner une reconfiguration de la topologie du réseau.

La fonction Fast Failover permet de réduire ce temps en essayant de maintenir la liaison sans renégociation pendant le changement d'alimentation.

Avec le Fast Failover, l'indisponibilité du chemin réseau dure entre 30 et 300 ms.

Chapter 3

Caractéristiques

	CARACTÉRISTIQUES
Connecteurs	4 ports RJ45, plaqués or
LED	2 LED 10/100 par port Net (Speed) 1 LED Link/Activity par port RJ45 2 LED POWER
Alimentation électrique	2 x 12 VDC (1 nécessaire pour le fonctionnement, 2 pour la redondance)
Consommation électrique	4W
MTBF (temps moyen entre pannes)	250 000 heures
Dimensions (H x L x P)	30 x 113 x 128 mm
Dimensions de la face avant (H x L)	143 x 35 mm
Accessoire	1 x 90-240 VAC PSU
Température d'utilisation	0 °C à 50 °C
Température de stockage	-22 °C à 70 °C
Humidité	10 à 90 %, sans condensation
Certifications	RoHS — CE — FCC classe A — IEEE 802.3

Chapter 4

Cas d'utilisation

4.1 Procédure de contrôle de la livraison

4.1.1 Introduction

Le GTap est livré avec 8 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.
L'alimentation électrique externe fournie avec le GTap possède deux étiquettes de sécurité argentées.
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 de chaque scellé de sécurité.
- Prendre des photos en haute définition de chaque scellé de sécurité, en photographiant deux scellés par photo, comme illustré dans les exemples ci-dessous. Le GTap CU_1P en possède huit, soit quatre photos au total.

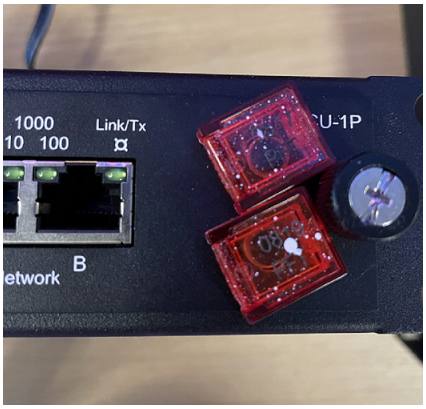


Figure1: exemple 1

Figure2: exemple 2

- Prendre des photos en haute définition de chaque face de l'alimentation électrique, comme illustré dans les exemples ci-dessous. Chaque alimentation en possède six, soit six photos au total.

- Cliquer sur le lien vers le disque partagé.

Figure3: exemple 1

Figure4: exemple 2

- 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, installer le rack de trois GTap dans une baie (19 pouces) et le fixer.
  - Pour installer un rack, visser les GTap dans un châssis pour obtenir le résultat suivant :

Figure5: Rack de trois GTap

Note:

La hauteur du rack de trois GTap est de 1U.

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 la première alimentation :
    - d'un coté au connecteur <POWER 1> du GTap
    - de l'autre coté à la première nourrice

    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 la deuxième alimentation si elle est présente :
    - d'un coté au connecteur <POWER 2> du GTap
    - de l'autre coté à la deuxième nourrice
- 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, en cas de mise en baie, les nourrices de la baie soient bien alimentées.

Note:

La LED <POWER 2> est allumée seulement si une deuxième alimentation est branchée au GTap.

- Connexion au réseau à surveiller :
  - Connecter les câbles du réseau à surveiller sur les connecteurs `Network A` et `Network 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 (LED Link/Activity)
  - Vérifier que les LED `Network A` et `Network B` du Tap soient allumées de façon fixe.

    Dans le cas d'une mise en baie, 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 ports `Network A` et `Network B` clignotent rapidement.
- Connexion vers la sonde de détection :
  - Connecter les ports `Monitor A` et `Monitor B` du Tap à la sonde de détection, à l 'aide de câbles RJ45 UTP, droits ou croisés, de catégorie 5e ou supérieure.

Note:

Le trafic réseau reçu sur le port `Network A` est dupliqué sur le port `Monitor A` et le trafic réseau reçu sur le port `Network B` est dupliqué sur le port `Monitor 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 `Monitor` fonctionnent à la même vitesse que les ports d'entrée réseau `Network`.

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®

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.

LFP
: Le Link Failure Propagation garantit que le GTap ne sera pas un point de défaillance dans le réseau, ce qui permet une capture des paquets dans un réseau redondant sans inquiétude.

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

G

GBox, 17
GCap, 17
GCenter, 17
GTap, 17

I

IDS, 17

L

LFP, 17

O

OSI, 17

P

PSU, 17

T

TAC, 17