Cahier des Charges (CDC)

Tac&Tic Brother — Suite du projet CCNA : Pérennisation & Exploitation

1. Synthèse exécutive

Tac&Tic Brother entre dans une phase de maturité : l'entreprise exige désormais un réseau **non seulement fonctionnel**, mais **exploitable par une équipe tierce**.

Le projet repose sur 3 piliers d'exploitation (**RUN**) :

- **NOC (Grafana)** : hypervision, performance, capacité, alerting.
- **ITSM (GLPI)** : actifs, SLA, incidents, changements (CHG).
- **SOC-lite (Wazuh)** : détection, triage, décision, ticketing sécurité.

Priorité absolue (P0) : Grafana devient la **console d'exploitation**. Tout aspect critique (disponibilité, performance) doit être visible et compréhensible via des dashboards conçus avec une logique **UX stricte**.

2. Note d'accueil — Guide de survie Ops (TTB)

De l'administration réseau à l'ingénierie d'exploitation

Bienvenue dans l'équipe Ops de Tac&Tic Brother.

Ici, on ne vous demande pas seulement de **faire fonctionner** une infra : on vous demande de livrer un **service métier** maintenable, prédictible et résilient.

Changement de paradigme : vous ne livrez pas « un réseau », vous livrez un **RUN** : **Visibilité** → **Alerte** → **Diagnostic** → **Correction** → **Preuve** → **Capitalisation**.

3.1 Les 3 commandements de l'exploitant

(1) Pas de preuve = pas fait

- Une modification sans preuve (avant/après, output de commande, export, log) est considérée comme **non livrée**.
- Une valeur annoncée sans donnée (ex : « 100 Mbps » sans graphe) est **non recevable**.

✅ Attendu : chaque affirmation renvoie à une **annexe de preuve**.

(2) L'UX n'est pas une option (règle des 30 secondes)

En incident, le stress réduit la capacité d'analyse. Un dashboard illisible est un risque.

Pyramide de l'information

- **Niveau 1 — Hypervue** : état global (OK/WARN/CRIT) — l'utilisateur peut-il travailler ?
- **Niveau 2 — Tendances** : évolution (24h) — rupture brutale ou dégradation lente ?
- **Niveau 3 — Détails** : métriques/ports/logs — pourquoi cela a échoué ?

✅ Attendu : drill-down fluide **Hypervue** → **Diagnostic** → **Logs** sans changer d'outil.

(3) Tracez tout (loi du ticket)

La mémoire de l'entreprise est **logicielle** (ITSM). Si vous partez, GLPI doit raconter l'histoire.

- Un changement (CHG) sans traçabilité = **anomalie**.
- Un incident (INC) non clôturé = **dette technique**.

✅ Attendu : **ALRT** ↔ **INC/CHG/SEC** (liens croisés obligatoires).

4. Contexte, objectifs et définition de succès

4.1 Contexte

Tac&Tic Brother déménage et souhaite pérenniser son réseau. L'objectif n'est plus la simple mise en service (**BUILD**), mais la **maintenabilité** et la capacité de reprise par un tiers (**RUN**).

4.2 Objectifs détaillés

Objectifs fonctionnels (attendus « entreprise »)

1. **Assurer une hypervision NOC (console unique)**
    - KPI « Business / Réseau / Sécurité / Exploitation ».
    - Drill-down vers diagnostic **≤ 2 clics**.
2. **Mesurer et visualiser la performance (observabilité)**
    - Réseau : débit, erreurs, drops, flaps, capacité/tendance.
    - Services : disponibilité + latence (**p95 recommandé**) + taux d'échec.
    - Système : CPU/RAM/Disk, saturation.
3. **Mettre en place un alerting utile (actionnable, anti-bruit)**
    - **6 alertes minimum** avec messages structurés.
    - Lien systématique : **runbook** + **ticket**.
    - Test réel : **FIRING** → **RESOLVED**.

4. **Centraliser et exploiter les logs**
    - Logs firewall OPNsense au minimum.
    - Vues orientées incident : volumes, top talkers, preuve **ALLOW/BLOCK**.
5. **Industrialiser l'exploitation via ITSM**
    - Service Desk : qualification, priorisation (**S1/S2/S3**), SLA.
    - Inventaire d'actifs exploitable (CI/Asset).
6. **Ajouter une couche SOC-lite**
    - Détection simple et justifiable.
    - Scénarios : auth failures / changement suspect.
    - Triage (FP vs incident) + décision + ticket associé.

Objectifs non-fonctionnels (qualité)

- **Lisibilité & UX** : compréhension en **< 30 s** sur l'hypervue.
- **Fiabilité** : éviter le « No data », labels propres, sources stables.
- **Sobriété** : éviter l'alert fatigue.
- **Traçabilité** : anomalie majeure = INC ; changement = CHG.
- **Maintenabilité** : conventions de nommage respectées.

4.3 Définition de succès (critères d'acceptation)

Le projet est validé si :

- L'hypervue indique immédiatement l'état de santé global.
- Un incident simulé est diagnostiqué avec **2 dashboards max + 1 requête logs**.
- Un ticket GLPI « exemplaire » permet à un tiers de reproduire les tests.
- **2 événements Wazuh** sont triés et reliés à des tickets.

5. Périmètre

5.1 Inclus

- Supervision (disponibilité, performance, capacité)
- Centralisation logs OPNsense (preuve ALLOW/BLOCK)
- Alerting Grafana actionnable
- ITSM GLPI (inventaire, SLA, incidents, journal CHG)
- SOC-lite Wazuh (agents, 2 scénarios, triage)

5.2 Hors périmètre (sauf bonus)

- Haute disponibilité / PRA complet
- SIEM avancé multi-sources
- IDS complet (Snort = bonus)

6. Contraintes d'architecture

6.1 Topologie

- **OPNsense (VM)** : **routeur central** (routage inter-VLAN + interconnexion WAN inter-divisions), NAT, DHCP/DNS, règles.
- **Routeur Cisco** : accès WAN / point de raccordement inter-groupes (liaison de transit vers OPNsense).
- **ESXi** : hébergement OPNsense + VMs.

6.2 Modèle ESXi recommandé

Pour garantir un fonctionnement stable sur ESXi (et éviter les erreurs de tagging), le modèle suivant est recommandé :

- Port Group **TRUNK** : VLAN 4095, connecté à l'interface **TRUNK** d'OPNsense (transport des VLAN).
- Port Group **TRANSIT** : réseau de transit entre le routeur et OPNsense (WAN OPNsense).

6.3 Contraintes d'exploitation (RUN)

- Tout changement réseau/sécurité doit faire l'objet d'un **CHG** et d'une **mini-recette** (tests critiques + preuve).
- Toute règle firewall significative doit être justifiée et accompagnée d'une **preuve log** (ALLOW/BLOCK).
- La supervision doit inclure la **supervision de la supervision** (état des sondes et des collectes).

7. Adressage imposé

`G` = numéro de groupe (1..4)

7.1 WAN inter-groupes

- 172.16.0.0/24 — G1: .11 / G2: .12 / G3: .13 / G4: .14

7.2 LAN par groupe : 10.100.G.0/24 (segmenté)

VLAN	Nom	Sous-réseau	Gateway
10	ADMIN	10.100.G.0/26	10.100.G.1
20	USERS	10.100.G.64/26	10.100.G.65
30	SRV	10.100.G.128/27	10.100.G.129

40	GUEST	10.100.G.160/27	10.100.G.161
99	MGMT (opt)	10.100.G.192/28	10.100.G.193

7.3 Transit routeur ↔ OPNsense

- 10.255.G.0/30 — Routeur: .1 / OPNsense WAN: .2

7.4 IP fixes exigées (monitoring standardisé)

- MON1 (VLAN10) : 10.100.G.10
- ITSM1 (VLAN30) : 10.100.G.140
- SEC1 (VLAN30) : 10.100.G.150
- PRB1 (option, VLAN20) : 10.100.G.90

8. Services & flux métier

8.1 Services socle

- DHCP : VLAN20 + VLAN40
- DNS : Unbound sur OPNsense (résolution prouvée)
- Admin firewall : accessible uniquement depuis VLAN10

8.2 Flux métier (Intranet)

- Cible : `intranet.ttb.local` (hébergé en **G2 VLAN30**)
- Protocole : HTTPS TCP/443

Matrice de flux

- ✅ G1 & G4 autorisés
- ❌ G3 interdit par défaut

9. Conventions de nommage & traçabilité

9.1 Hostnames / AssetID

Format : `TTB-G{G}-{ROLE}1`
Exemples : `TTB-G1-RTR1`, `TTB-G1-FW1`, `TTB-G1-MON1`, `TTB-G2-INTRA1`.

9.2 Identifiants (IDs)

Type	Format
Alerte	ALRT-YYYYMMDD-####
Incident	INC-YYYYMMDD-####
Changement	CHG-YYYYMMDD-####
Sécurité	SEC-YYYYMMDD-####

10. Gouvernance projet

10.1 Rôles (groupe de 5)

- **SPOC / Chef·fe** : pilotage, arbitrage, qualité, journal CHG
- **Référent Réseau** : Cisco, routage, SNMP, WAN
- **Référent ESXi** : PortGroups, trunk, placement VMs
- **Référent OPNsense/Logs** : VLAN, règles, syslog
- **Référent Exploitation** : Grafana (UX/alerting), GLPI, Wazuh

10.2 Rituels imposés

- Stand-up (10 min) : priorités, blocages
- Wrap-up (10 min) : preuves collectées + MAJ doc
- Checkpoint : démo + validation critères

11. Exigences — LOT 1 : Grafana (NOC) — P0

11.1 Stack minimale

11.1.1 Étape 1 — Supervision LAN (par groupe)

Chaque groupe déploie **sa propre stack de supervision sur son LAN** (MON1 en VLAN10) :

- Grafana, Prometheus, Node Exporter
- snmp_exporter (Cisco)
- Blackbox Exporter (ICMP/DNS/HTTPS)
- Loki + Promtail (logs OPNsense)

Périmètre LAN (obligatoire) :

- supervision des équipements **du groupe** (RTR1/FW1/ESX1 + VMs + services),
- supervision SLA “vue client” **depuis le LAN** (Blackbox),
- logs firewall OPNsense (preuve ALLOW/BLOCK).

11.1.2 Étape 1 — Supervision WAN (unique, mutualisée)

Tac&Tic Brother ne veut **qu’un seul point de supervision WAN** (éviter la duplication et garantir une référence unique).

➡️ **Supervision WAN hébergée par un seul groupe : Groupe G2 (NOC central)**

- Le groupe **G2** étend sa supervision (MON1) pour créer une vue **WAN globale**.
- Les groupes **G1, G3, G4** ne déploient **pas** de supervision WAN : ils fournissent uniquement l’accès nécessaire (SNMP/ICMP) à leurs routeurs.

Données WAN attendues (minimum)

- Disponibilité ICMP des routeurs WAN : `172.16.0.11` / `.12` / `.13` / `.14`
- SNMP des routeurs (interfaces WAN) : état, débit, erreurs/drops
- Latence & perte (Blackbox ICMP) vers chaque routeur WAN

Contraintes sécurité (lab mais “entreprise”)

- L’accès SNMP doit être **restreint** (ACL/filtrage) au **MON-WAN (G2)** autant que possible.
- Preuve exigée : capture config / ACL + test SNMP OK depuis G2, KO depuis un poste non autorisé.

Livrable coordination

- G2 fournit aux autres groupes : l’URL du dashboard WAN + identifiants d’accès (si besoin) + convention de nommage.
- Chaque groupe ajoute dans son hypervue un **lien** vers la vue WAN (preuve par capture).

11.2 UX / Design System (section notée)

- Hiérarchie : KPI → tendances → détails → logs
- Couleurs sémantiques : OK (vert), WARN (orange), CRIT (rouge), NO DATA (gris)
- Performance : chargement dashboard **< 5 s** (vue 1h)

11.3 Dashboards obligatoires (exports JSON)

> Chaque dashboard doit contenir un bandeau « santé de la supervision » (targets Prometheus/SNMP/Blackbox/Loki).

11.3.0 Découpage attendu

- **Dashboards LAN (obligatoires, par groupe)** : réalisés par **tous** les groupes sur MON1.
- **Dashboards WAN (obligatoires, mutualisés)** : réalisés **uniquement par G2** (NOC central), mais consommables par tous via lien.

11.3.1 `00_HYPERVUE_TAC-TIC` (LAN — décision rapide)

Structure UX imposée

- Ligne 1 : KPI cards (4–6)
- Ligne 2 : tendances (2–3 graphes)
- Ligne 3 : détails (tables)
- Bloc Runbook visible sans scroller

KPI minimum (LAN)

- HTTPS intranet UP + p95 (sonde depuis le LAN)
- DNS intranet UP + p95
- ICMP GW VLAN20 UP + loss
- WAN local : débit/utilisation (interface WAN du routeur)
- Firewall BLOCK/min

Critère clé : DNS KO ⇒ ICMP OK / DNS KO / HTTPS KO

Obligation navigation : ajouter un **lien** vers la vue WAN (G2) dans l'hypervue.

11.3.2 `10_NETWORK_INTERFACES` (LAN — perf réseau)

- Débit in/out + (reco) pps
- Errors, drops/discards, CRC
- Up/down + flaps
- Table synthèse (débit avg/p95, errors, drops)

11.3.3 `20_SECURITY_FIREWALL_LOGS` (LAN — preuve & contexte)

- ALLOW/min, BLOCK/min, ratio
- Top talkers (sources/destinations/ports)
- Stream filtrable + table "blocks critiques"
- Préfiltre "incident intranet"

11.3.4 `30_SLA_SERVICES` (LAN — vue client)

- UP% 1h/24h + p95 latence
- ICMP GW + loss

- DNS resolve intranet
- HTTPS intranet response time (+ code si possible)

11.3.5 `90_ADMIN_MONITORING` (LAN — supervision de la supervision)

- Targets down (stat + table)
- Ressources MON1 (CPU/RAM/Disk)
- Loki ingestion (logs/s + erreurs)

11.3.6 `40_CAPACITY_TRENDS` (LAN — bonus)

- 7 jours : top interfaces avg/p95, p95 DNS/HTTPS, CPU/RAM équipements
- Encadré “Reco capacité” (3 bullets)

11.3.7 `05_WAN_OVERVIEW` (WAN — unique, réalisé par G2)

Objectif : donner une vision WAN “single source of truth”.

Contenu minimum

- Stat “Routeurs WAN UP” (combien UP / combien DOWN)
- Table : routeur (G1..G4) / IP WAN / état / RTT p95 / perte %
- Interfaces WAN via SNMP : débit in/out, errors/drops (top 3)
- Graphes simples :
    - latence vers chaque routeur (timeseries)
    - pertes (timeseries)
    - débit WAN (timeseries)

UX attendu

- KPI en haut (UP%, RTT p95, loss)
- Drill-down possible vers un détail par routeur (via variable `$site`)
- Lien retour vers hypervue LAN (facultatif)

Critère d’acceptation WAN

- Si un routeur WAN est coupé, la vue WAN doit l’indiquer en < 30 secondes.

11.4 Alerting minimal (6 alertes)

- WAN interface DOWN
- Errors/Discards anormaux
- GW VLAN20 DOWN
- DNS KO
- HTTPS intranet KO
- Admin OPNsense KO

Format du message : AlertID / AssetID / Symptôme / Impact / Runbook / Ticket INC

Test imposé : 1 alerte **FIRING** → **RESOLVED** (preuves)

12. Exigences — LOT 2 : GLPI (ITSM)

12.1 Objectif

Mettre en place un **Service Desk** réaliste : actifs, SLA, incidents et changements tracés.

12.2 Exigences minimales

- Serveur ITSM1 opérationnel
- Inventaire : tous les équipements critiques saisis
- Tickets :
    - 1 ticket « service » (ex : DNS KO)
    - 1 ticket « réseau » (ex : drops interface)
- Traçabilité : chaque ticket cite les tests effectués et les dashboards consultés

13. Exigences — LOT 3 : Wazuh (SOC-lite)

13.1 Objectif

Mettre en place une démarche de détection et triage : **signal** → **preuve** → **décision** → **ticket**.

13.2 Scénarios imposés (minimum 2)

1. Auth failures / brute force
2. Changement suspect (fichier critique / service stoppé)

Bonus : corrélation avec logs firewall

13.3 Livrables SOC

Pour chaque scénario :

- 1 fiche **SEC-YYYYMMDD-####**
- 1 qualification (FP ou incident)
- 1 ticket **INC** associé si avéré

14. Déroulé logique (Étapes) + jalons

> Le projet se déroule en **3 étapes successives**. Chaque étape introduit une nouvelle couche (NOC → ITSM → SOC-lite).

Étape 1 — Supervision (Grafana) : LAN partout + WAN unique

- **Chaque groupe** : supervision complète de son **LAN** (MON1) + dashboards LAN + alerting minimum.
- **Un seul groupe (G2)** : supervision **WAN** mutualisée (dashboard `05_WAN_OVERVIEW`).

✅ Résultat attendu : une hypervue LAN par groupe + une vue WAN unique “référence”.

Étape 2 — ITSM (GLPI) : un GLPI dans chaque LAN

- **Chaque groupe** déploie **ITSM1** en VLAN30.
- Mise en place : inventaire actifs, priorités S1/S2/S3, SLA/OLA, tickets exemplaires.

✅ Résultat attendu : chaque groupe peut tracer un incident/changement local, avec preuves et reproductibilité.

Étape 3 — SOC-lite (Wazuh) : un Wazuh dans chaque LAN

- **Chaque groupe** déploie **SEC1** en VLAN30.
- Agents : MON1, ITSM1 + 1 VM au choix.
- Scénarios : brute-force + changement suspect, triage FP/incident, ticket associé.

✅ Résultat attendu : triage complet, preuve, ticket, et lien vers AssetID.

15. Recette & critères d’acceptation

15.1 Réseau

- DHCP, DNS, segmentation VLAN respectée
- Intranet : accessible G1/G4, bloqué G3

15.2 Exploitation

- Hypervue UX validée
- Preuve ALLOW/BLOCK disponible en **< 1 min**
- 1 alerte testée FIRING → RESOLVED
- 1 ticket exemplaire reproductible

16. Livrables — Dossier de reprise

16.1 Format

- **PDF** pour tout document rédactionnel
- **Format natif** pour exports/configs (JSON, TXT, XML, XLSX)

16.2 Contenu du rapport technique (PDF)

- Résumé & périmètre
- Architecture cible (topologie, flux)
- Configuration (détails par brique)
- Supervision (intentions UX, KPI choisis)
- Analyse (post-mortem de 2 incidents)
- Mise en service (procédure d'installation)

17. Règles de preuve (exigées)

Pour chaque élément critique validé :

- 1 capture « avant »
- 1 capture « après »
- 1 commande de validation (ex : `dig`, `nslookup`, `curl`) avec sortie visible

Annexes — Gabarits (à utiliser)

A) Ticket INC (GLPI)

- Détection (ALRT/SEC)
- Impact + priorité (S1/S2/S3)
- Vérifications : tests + dashboards + logs
- Cause racine + correctif
- Preuves avant/après
- CHG associé (si modif)
- MAJ runbook

B) Journal CHG

CHG-ID	Date/heure	Auteur	Objet	Backup	Actions	Tests	Résultat	Rollback

C) Fiche SEC (triage)

- Signal Wazuh
- Hypothèse + preuves
- Impact potentiel
- Décision : FP