Consultation N° 05/CERIST/2026 pour la sélection d'un opérateur Internet pour un Service managé de Protection Anti-DDoS

1. Contexte et Objectifs de la Consultation

L'objectif de cette consultation est de retenir un Opérateur Internet capable de fournir un service de protection managé contre les attaques par déni de service distribué (DDoS).

L'infrastructure Internet et les liaisons IP sous-jacentes étant **déjà fournies et opérées par notre Opérateur actuel**, la présente consultation vise exclusivement la mise en œuvre d'une couche de sécurité supérieure.

Le prestataire retenu devra déployer une solution d'atténuation (mitigation) dans son propre réseau s'appuyant sur une architecture de classe opérateur (type Netscout Arbor, Radware DefensePro, A10 Thunder TPS, Cloudflare Magic Transit, Akamai Prolexic ou équivalent), via ses plateformes de nettoyage (scrubbing centers) ou équipements de mitigation DDoS, interconnectée avec notre réseau avec le protocole BGP.

2. Description de l'existant (à prendre en compte)

- Interconnexion avec le réseau du fournisseur via le protocole BGP
- Deux (02) ASN (Autonomous System)
- Deux (02) préfixes, un prefixe par ASN :
- Deux (02) sessions BGP, une par ASN/Préfixe

3. Spécifications Techniques et Fonctionnelles

Le service de sécurité attendu doit assurer les trois exigences suivantes: **la Visibilité, la Détection, et le Contrôle.**

3.1. Visibilité et Accès à l'Interface Utilisateur (Dashboard UI)

Le soumissionnaire doit mettre à disposition un portail web d'administration (Dashboard UI) sécurisé, accessible en 24/7/365, respectant les caractéristiques de dimensionnement suivantes :

- **Accès User Interface (UI) & Périmètre :** L'accès à l'interface doit être fourni pour nos équipes de supervision. La solution doit permettre de gérer un compte principal (Parent) et un nombre maximum **de 5 sous-comptes / entités rattachées (Childs)** disposant de leurs propres périmètres de visibilité réseau.
- **Suivi en temps réel :** Affichage des débits binaires (Gbps) et des volumes de paquets (Mpps) du trafic propre et du trafic analysé avec un rafraîchissement instantanné.
- **Granularité et Historique :** Capacité à segmenter la vue du trafic (IP, protocoles, ports) avec une conservation des métriques réseau sur une période glissante minimale de **12 mois**.

3.2. Capacités de Détection et Notification sur Alerte

Le système, basé sur l'analyse asynchrone des flux, doit identifier immédiatement toute anomalie :

- **Notifications sur Alerte :** Dès le franchissement d'un seuil ou la détection d'un comportement suspect, le système doit envoyer une alerte immédiate (Email, SMS, Webhook/API) et faire remonter l'information de manière critique sur la UI.
- **Caractérisation de la menace :** En cas d'attaque volumétrique, l'interface doit qualifier en temps réel le vecteur (ex: Réflexion DNS, Amplification NTP, Flood SYN), l'IP ciblée, et cartographier/géolocaliser les principales sources de l'attaque.

3.3. Contrôle, Atténuation et Dimensionnement des Mitigations

Le prestataire doit garantir le nettoyage du trafic via ses équipements de filtrage avant de réacheminer le flux propre vers notre réseau

Une mitigation correspond à un événement d'attaque nécessitant l'activation du mécanisme de nettoyage du trafic, le prestataire devrait assurer :

- **Nombre de Mitigations Max :** Le forfait annuel/mensuel proposé doit inclure de base un **maximum de 10 mitigations par an** (le soumissionnaire précisera le coût unitaire en cas de dépassement).
- **Processus d'Auto-Mitigation (En synchronisation avec le client) :**

- La solution doit supporter l'application de l'**auto-mitigation** (bascule automatique et injection des routes/politiques vers les centres de nettoyage dès la détection.
- L'activation de cette fonctionnalité, la définition des seuils de déclenchement automatiques et les profils de filtrage associés doivent être **définis et validés en étroite synchronisation avec le client** lors de la phase de cadrage.
- *Alternative manuelle :* Possibilité de déclencher/forcer l'atténuation en un clic depuis l'interface utilisateur (UI) par annonce BGP (Remote Triggered Black Hole ou redirection vers le Scrubbing Center).

- **Notification suite aux mitigations :** À l'issue de chaque processus de nettoyage, une notification de clôture d'incident doit être immédiatement envoyée au client, confirmant le retour à la normale.
- **Graphique d'efficacité :** Affichage en temps réel sur la UI d'une courbe comparative superposant le trafic total reçu par le centre de nettoyage (attaque incluse), le trafic bloqué, et le trafic légitime effectivement délivré.

3.4. Rapports Mensuels et Suivi Détaillé

- **Rapports Mensuels :** Chaque mois, le prestataire transmettra un rapport consolidé reprenant les statistiques globales de trafic analysé, le détail des alertes levées, ainsi que l'analyse des mitigations éventuellement déclenchées.
- **Réunion de Synchronisation Périodique :** Une réunion de suivi détaillé sera organisée régulièrement (mensuelle ou trimestrielle) entre le prestataire et nos équipes techniques. Cette instance permettra de :
  - Analyser les rapports mensuels et l'évolution des profils de menaces.
  - Ajuster et optimiser les politiques de détection et les seuils d'auto-mitigation.
  - Faire un point sur la consommation du forfait (compteur des 10 mitigations).

4. Grille d'Évaluation des Offres

Les offres des soumissionnaires seront évaluées selon la répartition suivante :

- **Technique, UI, Mécanisme d'interconnexion & Dimensionnement : 70%**
- **Financier (Forfait annuel de protection + Forfait mitigations) : 30%**

Bordereau de Prix Unitaires

N°	**Désignation de la Prestation**	**Redevance Mensuelle**
1.	Forfait Service Anti-DDoS Managé (Inclus UI, multi-compte 5 Childs et Forfait 10 Mitigations/an)	...
2.	Prestation d'accompagnement (Gouvernance, Réunions de synchronisation, Rapports)	*Inclus*

Destail Quantitaif et Estimatif

N°	**Désignation de la Prestation**	**Redevance Mensuelle**	**Redevance Annuelle**
1.	Forfait Service Anti-DDoS Managé (Inclus UI, multi-compte 5 Childs et Forfait 10 Mitigations/an)	...	
2.	Prestation d'accompagnement (Gouvernance, Réunions de synchronisation, Rapports)	*Inclus*	
TOTAL HT			
TVA (... %)			
TOTAL TTC			