Fonctionnalités

- Centralisation des signalements d'abus
- Gestion rDNS (Forward & Reverse)
- Gestion AntiDDoS
- Analyse réseau
- Supervision par sondes
- Scan de vulnérabilités

Centralisation des signalements d'abus

La centralisation des signalements d'abus permet de regrouper tous les signalements liés aux IPs clients (spam, scans, comportements malveillants). Voici une explication des sources d'abus et de ce qu'est un abus :

Définition d'un abus

Un abus est un comportement malveillant ou non souhaité provenant d'une IP client. Cela peut inclure des activités telles que le spam, les scans de ports, les attaques par déni de service (DDoS), et d'autres comportements suspect.

Sources d'abus

Les signalements d'abus peuvent provenir de différentes sources, notamment :

- **AbuseIPDB** : Une base de données qui collecte et signale les adresses IP impliquées dans des activités malveillantes.
- **Mail** : Les signalements peuvent également provenir de plaintes par email, souvent envoyées par des administrateurs système ou des fournisseurs de services.

Sévérité des abus

La sévérité d'un abus est déterminée par le nombre de rapports détectés sur une même période donnée pour la même IP. Plus le nombre de rapports est élevé, plus la sévérité de l'abus est considérée comme importante.

Gestion rDNS (Forward & Reverse)

La gestion des enregistrements rDNS (Forward & Reverse) est une fonctionnalité clé de NetExpert. Voici une explication détaillée de cette fonctionnalité :

Définition des enregistrements rDNS

Les enregistrements rDNS (Reverse DNS) permettent de faire correspondre une adresse IP à un nom de domaine. Il existe deux types principaux d'enregistrements rDNS :

- **Forward DNS** : Fait correspondre un nom de domaine à une adresse IP.
- **Reverse DNS** : Fait correspondre une adresse IP à un nom de domaine.

Importance des enregistrements rDNS

Les enregistrements rDNS sont essentiels pour plusieurs raisons :

- **Identification** : Ils permettent d'identifier le nom de domaine associé à une adresse IP, ce qui est utile pour le dépannage et la gestion du réseau.
- **Réputation** : Certains services et fournisseurs utilisent les enregistrements rDNS pour vérifier la réputation d'une adresse IP.
- **Conformité** : Certains protocoles et services nécessitent des enregistrements rDNS valides pour fonctionner correctement.

Fonctionnalités de gestion rDNS dans NetExpert

NetExpert offre une interface intuitive pour gérer les enregistrements rDNS :

- **Édition / Création** : Permet de créer et de modifier vos enregistrements rDNS.
- **API pour intégration CI/CD** : Permet d'intégrer la gestion des enregistrements rDNS dans vos processus de développement et de déploiement.
- **Validation forward ↔ reverse** : Assure la cohérence entre les enregistrements forward et reverse.
- **Création automatique forward :** La plateforme créé automatiquement les rDNS et forward si vous ne spécifiez pas de valeur. Il est aussi possible de configurer un domaine personnalisé pour les blocs IPs annoncés en BGP

Gestion AntiDDoS

La gestion des règles AntiDDoS dans NetExpert permet de créer et de déployer des politiques AntiDDoS pour IP dédiées, transit ou tunnels. Voici une explication détaillée de cette fonctionnalité :

Définition des règles AntiDDoS

Les règles AntiDDoS permettent de protéger vos services contre les attaques par déni de service distribué (DDoS). Ces règles peuvent être configurées pour surveiller le trafic réseau et prendre des actions spécifiques en cas de détection d'une attaque.

Création de règles par IP

Vous pouvez créer des règles par IP pour prendre des actions en fonction du débit ou des paquets par seconde (pps). Voici les étapes pour créer une règle :

1. **Accéder à la section AntiDDoS** : Allez dans le menu "AntiDDoS" puis "Seuils".
2. **Créer une nouvelle règle** : Au dessus du tableau, vous pouvez configurer la nouvelle règle et l'ajouter

Actions possibles

Les actions possibles incluent :

- **Blackhole** : Bloquer tout le trafic vers l'IP.
- **Filtrage** : Filtrer le trafic pour permettre uniquement le trafic légitime. Notez que le filtrage avancé est soumis à une facturation spécifique.
- **Notification** : Envoyer une notification en cas de détection d'une attaque. Notez que cette option est uniquement disponible sous validation du support, car elle peut être dangereuse pour vos services.

Conditions spécifiques

- **Filtrage avancé** : Cette option est soumise à une facturation spécifique. Veuillez contacter notre équipe commerciale pour plus d'informations.
- **Notification** : Cette option est uniquement disponible sous validation du support. Veuillez contacter notre équipe de support pour activer cette fonctionnalité.

Alertes AntiDDoS

Les alertes AntiDDoS fonctionnent de manière similaire aux alertes d'abus. Vous pouvez configurer des notifiers pour recevoir des alertes en cas de détection d'une attaque. Les notifiers peuvent être configurés pour envoyer des alertes par email, Telegram, Slack, PagerDuty, etc.

Analyse réseau

L'analyse réseau dans NetExpert est basée sur un moteur d'analytiques réseau qui utilise les flows pour agréger les données. Bien que les valeurs ne soient pas 100% précises, les ratios sont fiables et permettent une analyse efficace du trafic réseau.

Définition de l'analyse réseau

L'analyse réseau permet de mesurer et d'analyser le trafic qui passe par votre réseau. Cela inclut toutes les informations principales des paquets, IPs, Ports, Protocoles, ASN, Pays

Fonctionnalités de l'analyse réseau

NetExpert offre plusieurs fonctionnalités pour l'analyse réseau :

- **Visualisation des flux** : Permet de visualiser les flux de trafic pour identifier les zones de congestion et les anomalies.
- **Analyse du trafic** : Permet d'analyser le trafic en fonction de la source, de la destination et de l'ASN.
- **Rapports exportables pour audits** : Permet d'exporter des rapports pour des audits ou des analyses ultérieures.

Moteur de filtres

Langage de filtrage

Le langage de filtrage de NetExpert est similaire à SQL avec quelques variations. Les champs listés comme dimensions peuvent généralement être utilisés. Les opérateurs acceptés sont =, !=, <, <=, >, >=, IN, NOTIN, LIKE, UNLIKE, ILIKE, IUNLIKE, <<, et !<<, lorsque cela est applicable. Voici quelques exemples :

- `srcPort = 443` sélectionne les flux où le port source est **443**. La valeur ne doit pas être entre guillemets.
- `SrcAS = AS12322`, `SrcAS = 12322`, ou `SrcAS IN (12322, 29447)` limite le numéro AS source des flux sélectionnés.
- `SrcAddr = 203.0.113.4` sélectionne uniquement les flux avec l'adresse spécifiée. Notez que le filtrage sur les adresses IP est généralement plus lent.
- `SrcAddr << 203.0.113.0/24` sélectionne uniquement les flux qui correspondent au sous-réseau spécifié.

Les noms de champs ne sont pas sensibles à la casse.

Notez que l'utilisation des champs suivants empêchera l'utilisation de données agrégées et sera donc plus lente :

- `SrcAddr` et `DstAddr`
- `SrcPort` et `DstPort`

Dimensions

Vous pouvez sélectionner un ensemble de dimensions. Pour les séries temporelles, les dimensions sont converties en séries. Elles sont empilées avec "stacked", affichées sous forme de lignes simples avec "lines". Pour les graphiques de Sankey, les dimensions sont converties en nœuds. Dans ce cas, vous devez sélectionner au moins deux dimensions.

L'ordre de sélection est important pour les dimensions.

Supervision par sondes

> **Avertissement : Cette fonctionnalité est actuellement en cours de développement.**

La supervision par sondes dans NetExpert permet de créer des sondes basées sur un réseau mondial de sondes qui effectuent des tests périodiques sur des IPs choisies. Cette fonctionnalité est conçue pour surveiller la disponibilité et la performance de vos services.

Définition de la supervision par sondes

La supervision par sondes consiste à utiliser un réseau de sondes réparties dans le monde pour effectuer des tests périodiques sur vos adresses IP. Ces tests permettent de surveiller la disponibilité et la performance de vos services.

Fonctionnalités de la supervision par sondes

NetExpert offre plusieurs fonctionnalités pour la supervision par sondes :

- **Tests périodiques** : Les sondes effectuent des tests périodiques sur les IPs choisies pour surveiller la disponibilité et la performance.
- **Agrégation des données** : Les données collectées par les sondes sont agrégées pour des analyses et des rapports.
- **Alertes** : Des alertes peuvent être configurées pour vous notifier en cas de problèmes détectés, tels que des erreurs ICMP ou HTTP.
- **Rapports périodiques :** Tout les X (semaines, mois), un rapport des résultats des sondes vous est envoyé.

Configuration des sondes

Pour configurer les sondes, suivez ces étapes :

1. **Créer une sonde** : Sélectionnez les IPs que vous souhaitez surveiller et configurez les tests à effectuer.
2. **Définir la fréquence des tests** : Configurez la fréquence à laquelle les sondes effectuent les tests.
3. **Configurer les alertes** : Définissez les conditions pour lesquelles des alertes doivent être déclenchées.

Alertes et analyses

Les données collectées par les sondes sont agrégées pour des analyses et des rapports. Vous pouvez configurer des alertes pour être notifié en cas de problèmes détectés, tels que des erreurs ICMP ou HTTP.

Options de facturation

Pour avoir plus de sondes ou une fréquence de tests plus élevée, cela est soumis à une facturation spécifique ou inclus dans certains contrats. Veuillez contacter notre équipe commerciale pour plus d'informations.

Scan de vulnérabilités

> **Avertissement : Cette fonctionnalité est actuellement en cours de développement.**

Le scan de vulnérabilités dans NetExpert permet une analyse automatisée sur principe de opt-in, avec différents niveaux d'analyses. Les scans sont à la fois applicatifs, réseau, et comportemental.

Définition du scan de vulnérabilités

Le scan de vulnérabilités est un processus automatisé qui permet de détecter et de signaler les vulnérabilités potentielles dans vos systèmes et applications. Ce processus est basé sur le principe de l'opt-in, ce qui signifie que vous devez explicitement activer cette fonctionnalité pour qu'elle soit exécutée.

Fonctionnalités du scan de vulnérabilités

NetExpert offre plusieurs fonctionnalités pour le scan de vulnérabilités :

- **Analyse applicative** : Détection des vulnérabilités dans les applications web et les services.
- **Analyse réseau** : Détection des vulnérabilités dans les configurations réseau et les services réseau.
- **Analyse comportementale** : Détection des anomalies et des comportements suspects.

Configuration des scans

Pour configurer les scans de vulnérabilités, suivez ces étapes :

1. **Activer le scan** : Activez la fonctionnalité de scan de vulnérabilités dans votre compte NetExpert.
2. **Choisir le niveau d'analyse** : Sélectionnez le niveau d'analyse souhaité (applicatif, réseau, comportemental).
3. **Configurer les alertes** : Définissez les conditions pour lesquelles des alertes doivent être déclenchées.

Niveaux d'analyse

Les scans de vulnérabilités sont effectués à différents niveaux :

- **Applicatif** : Analyse des applications web et des services pour détecter les vulnérabilités courantes (par exemple, les vulnérabilités OWASP).
- **Réseau** : Analyse des configurations réseau et des services réseau pour détecter les vulnérabilités potentielles.

- **Comportemental** : Analyse des comportements suspects et des anomalies pour détecter les activités malveillantes.
- **Aggressif :** Analyse Applicative, Réseau, Comportementale avec fuzzing et tests d'injections (XSS, SQL...) automatisés.**(Possiblement dangereux, à ne pas activer sans être certain)**

Whitelisting des IPs

Les scans sont opérés depuis des IPs centralisées, lesquelles vous pouvez whitelist dans votre pare-feu. Les adresses IP utilisées pour les scans sont indiquées sur NetExpert.