paloalto
TECHDOCS

Incidents et alertes NGFW

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

January 31, 2025

Table of Contents

Alertes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Pour vous aider à maintenir la santé continue de vos périphériques et éviter les incidents perturbant l'activité, AIOps for NGFW génère des alertes en fonction d'un ou plusieurs problèmes détectés lors du déploiement de votre pare-feu. Ces problèmes, ou *événements*, sont déclenchés de l'une des trois manières suivantes :

- Lorsqu'une mesure change de façon significative
- Lorsqu'un événement généré précédemment change
- Lorsque l'utilisateur ou le système exécute une action, telle que l'accusé de réception ou la fermeture d'une alerte

Une alerte indique un problème particulier (dégradation ou perte de fonctionnalité du pare-feu) qui doit être résolu. Des alertes peuvent également être générées sur la base d'une corrélation ou d'une agrégation de plusieurs événements. Cette agrégation des événements en une seule alerte facilite le triage, rationalise le transfert des alertes entre les équipes, centralise les informations critiques et réduit la fatigue liée aux notifications.

Les alertes sont classées en différentes catégories selon la mesure à laquelle elles sont associées. Vous pouvez utiliser des catégories d'alertes pour spécifier les types d'alertes pour lesquelles vous recevez des notifications. Par exemple, Matériel, Limites de configuration, Limites de ressources, Contenu dynamique et PAN-OS et abonnements.

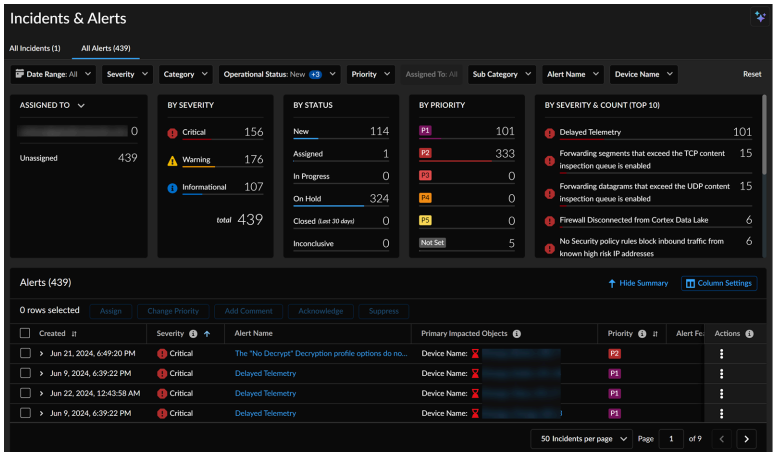
Depuis **Incidents & Alerts (Incidents et alertes)** > **NGFW** > **All Alerts (Toutes les alertes)**, vous pouvez afficher et gérer toutes les alertes générées pour votre déploiement. Dans **Notification Rules (Règles de notification)**, vous pouvez configurer des règles de notification qui spécifient quand et comment vous souhaitez être averti lorsque des événements déclenchent une alerte.

- Gérer les alertes NGFW
- Voir les détails de l'alerte
- Voir les causes probables
- Prévision et détection d'anomalies
- Gérer les alertes de l'analyseur de capacité
- Mesures d'utilisation du processeur dans AIOps pour NGFW
- Créer une règle de notification
- Intégration avec ServiceNow

Gérer les alertes NGFW

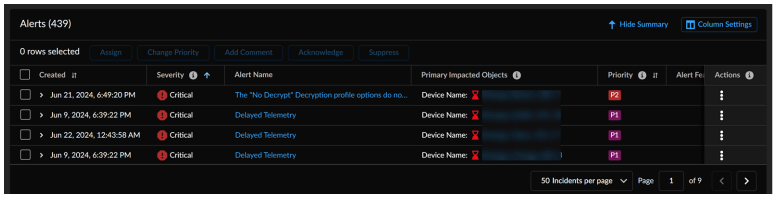
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Obtenez une vue d'ensemble des alertes NGFW en sélectionnant **Incidents & Alerts (Incidents et alertes)** > **NGFW** > **All Alerts (Toutes les alertes)**. Explorez la page des alertes pour vous aider à maintenir la santé continue de vos périphériques et de vos déploiements et pour éviter de perturber votre activité. Vous avez un accès direct à une liste détaillée d'alertes ainsi qu'à des résumés visuels critiques. Vous pouvez également **masquer le résumé** pour masquer les widgets et afficher uniquement les alertes dans un format tabulaire.



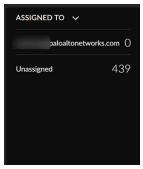
Voici les données affichées sous **All Alerts (Toutes les alertes)**.

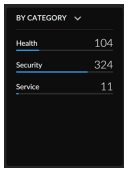
- **Alerts (Alertes)** : Affiche toutes les alertes.



  Dans ce tableau, vous pouvez effectuer les tâches suivantes :

  - **Hide Summary (Masquer Résumé)** pour masquer les widgets et afficher uniquement les alertes dans un format tabulaire.
  - Développez une alerte pour afficher sa description et son impact.
  - Sous Actions, vous pouvez effectuer les actions suivantes :
    - **Affectez** une alerte à un utilisateur, vous-même, ou désaffectez une alerte.
    - **Modifiez la priorité** d'une alerte ou sélectionnez « Not Set » (Non défini) pour supprimer la priorité.
    - **Accusez réception** d'une alerte en sélectionnant **Yes (Oui)**, ce qui confirme que vous avez vu l'alerte.
    - L'option **Suppress (Supprimer)** définit l'état opérationnel de l'alerte sur « On Hold » (En attente) lorsque vous ne prévoyez pas de résoudre activement une alerte.
    - **Ajoutez un commentaire** pour une alerte.
  - Cliquez sur une alerte pour afficher ses détails.
  - Utilisez **Column Settings (Paramètres de colonnes)** pour afficher ou masquer des colonnes spécifiques pour les alertes et réorganiser l'ordre par défaut des colonnes. Ces modifications seront conservées lors des sessions futures.
- **ASSIGNED TO (ATTRIBUÉ À)** : Affiche le nombre d'alertes par la personne ou l'entité qui a la tâche de les résoudre. En haut, il montre les alertes attribuées à l'utilisateur connecté actuel et les alertes non attribuées. Vous pouvez également afficher les nombres d'alertes **PAR CATÉGORIE** en le sélectionnant dans la liste déroulante.

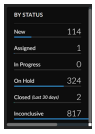




- **BY SEVERITY & COUNT (TOP 10) (PAR GRAVITÉ ET NOMBRE (TOP 10)) :** Affiche les alertes classées par gravité, ainsi que le nombre d'alertes dans chaque catégorie. Les alertes critiques

sont d'abord classées par ordre de priorité, suivies d'alertes d'avertissement, puis d'alertes d'information.

- **BY STATUS (PAR ÉTAT) :** Affiche le nombre total d'alertes par état.
  - New (Nouveau) indique les incidents dont l'attribution a été annulée.
  - Assigned (Attribué) indique les incidents qui ont été attribués à un utilisateur.
  - In Progress (En cours) indique que l'incident fait l'objet d'un traitement.
  - En attente indique que vous ne prévoyez pas de résoudre une alerte ou un incident activement.
  - Fermé indique les alertes fermées au cours des 30 derniers jours.
  - Non concluant indique qu'il n'y a pas de solution pour ces alertes.



- **BY SEVERITY (PAR GRAVITÉ) :** Affiche le nombre total d'alertes classées Critiques, Avertissements et Informationnelles.

- **BY PRIORITY (PAR PRIORITÉ) :** Affiche les alertes en fonction de leur priorité avec P1 qui est la plus grave.

Voir les détails de l’alerte

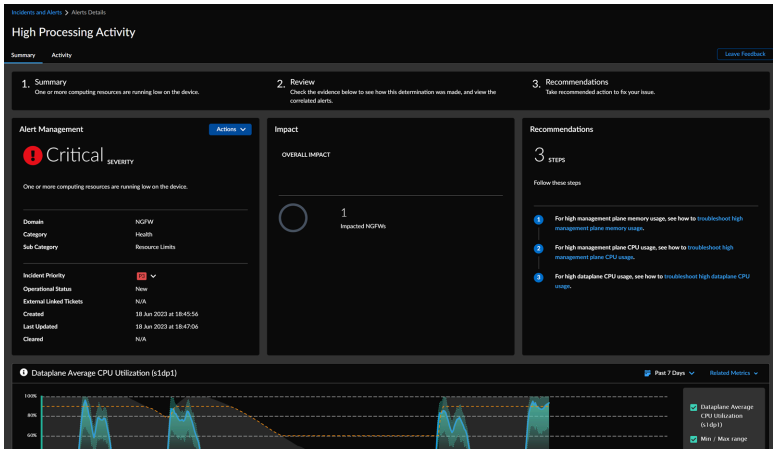
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Dans **All Alerts (Toutes les alertes)**, vous pouvez sélectionner une alerte pour ouvrir une page contenant des détails à son sujet. L’onglet **Summary (Résumé)** affiche les détails suivants :

1. Résumé de l’alerte avec détails. Vous pouvez modifier la priorité de l’alerte ou l’attribuer à un utilisateur.
2. Impact causé par l’alerte, c’est-à-dire le nombre de NGFW impactés.
3. Recommandations et ressources pour corriger votre problème.

Vous pouvez également consulter les tableaux des événements contributeurs.

L’onglet **Activity (Activité)** affiche l’activité enregistrée pour l’alerte.



Voir les causes probables

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	❑ ou

Grâce à des fonctionnalités avancées d'IA, AIOps pour NGFW affiche les causes probables des alertes et propose des recommandations pour résoudre le problème sous-jacent. Cette fonctionnalité garantit des performances réseau optimales en atténuant les perturbations et en maximisant l'efficacité de votre solution de cybersécurité.

Voici les alertes qui prennent en charge l'analyse de la cause probable:

- Activité de traitement élevée
- Latence accrue du trafic – Mémoire tampon de paquets
- Latence accrue du trafic – Descripteur de paquets sur puce
- Menaces autorisées
- Latence du trafic – Descripteurs de paquets (sur puce)
- Utilisation défavorable des ressources
- Homologues désynchronisés – Configuration
- Abus potentiel par vol d'informations d'identification
- Échec de l'opération Commit Push (validation transmission)

L'analyse de la cause probable est améliorée pour utiliser les registres de journaux Strata Logging Service et fournir des métadonnées supplémentaires à la cause probable qui a mené à la création d'alerte ou d'incident. Cette amélioration vous permet de localiser les stratégies, les applications, les zones sources, les URL, les adresses IP sources et les régions potentiellement à l'origine de l'alerte.

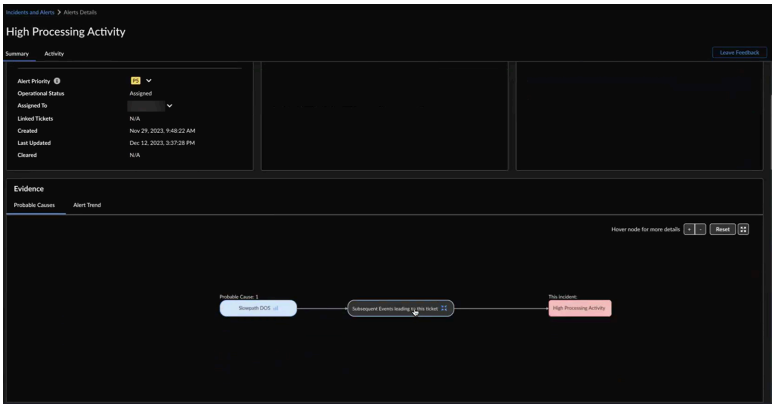
Vous pouvez afficher les causes probables des scénarios suivants :

- **Alerte d'activité de traitement élevée** : Lorsque l'utilisation du processeur du plan de données est élevée, cela peut entraîner divers problèmes tels que l'instabilité dans les pare-feux, des blocages de pare-feu ou des états bloqués, et les problèmes de perte de paquets ou de latence. Cela peut avoir un impact négatif sur vos opérations commerciales. Si l'utilisation du processeur du plan de données est d'au moins 60 % et qu'il y a un pic significatif d'utilisation, AIOps pour NGFW affichera les causes probables dans l'alerte d'activité de traitement élevée. Cependant, si l'utilisation du processeur du plan de données reste constante à un niveau élevé pendant une longue période sans aucune variation, la cause sera ambiguë et ne pourra pas être déterminée facilement. Il n'y aura donc pas de causes probables affichées. Par exemple, si l'utilisation du processeur du plan de données est constamment de 70 % pendant une période prolongée, AIOps pour NGFW n'affichera aucune cause probable.
- **Détection et correction de sessions gourmandes uniques ou multiples** (alerte d'activité de traitement élevée) : Le terme d'attaque de session gourmande sur un pare-feu désigne un attaquant créant rapidement de nombreuses connexions, exploitant les ressources internes

du pare-feu qui peuvent conduire à l'épuisement des ressources et à des incidents de déni de service (DoS). AIOps pour NGFW peut détecter ces problèmes et afficher les causes probables correspondantes.

- **Épuisement de session avec perte de connectivité** (alerte d'activité de traitement élevée) : Lorsqu'un pare-feu reçoit du trafic, il établit une session pour ce trafic afin de suivre son état et d'effectuer les inspections de sécurité nécessaires. Chaque session consomme des ressources système, y compris la mémoire et les cycles de processeur. Si le pare-feu atteint sa capacité maximale pour les sessions simultanées, cela entraînera l'épuisement de la session. Ce problème peut se produire pour plusieurs raisons, notamment un volume de trafic élevé, des stratégies de sécurité mal configurées et des paramètres de délai d'expiration de session inappropriés. AIOps pour NGFW utilise des fonctionnalités avancées d'IA pour détecter de manière proactive les problèmes d'épuisement de session dans les périphériques réseau. Cela permet une allocation optimisée des ressources, élève les performances du réseau et réduit les problèmes de connectivité pour garantir une disponibilité ininterrompue des services.
- **Utilisation élevée de la mémoire tampon de paquets due à une application unique** (Latence accrue du trafic – mémoire tampon de paquets) : AIOps pour NGFW détecte la cause première probable d'une utilisation élevée du tampon de paquets en raison d'une seule application monopolisant le tampon de paquets. AIOps pour NGFW exploite les capacités avancées de l'IA pour garantir des performances réseau optimales en alertant en temps opportun sur l'allocation des ressources sous-optimale et en empêchant la dégradation des performances.
- **Utilisation sur puce du descripteur de paquet élevé due à une application unique** (Latence accrue du trafic – Descripteur de paquet sur puce) : AIOps pour NGFW détecte la cause première probable d'une utilisation élevée des descripteurs de paquets sur puce. Cela aide à l'identification proactive et à la résolution de la congestion du réseau causée par une seule application monopolisant le descripteur de paquets sur puce.
- **Suggestion de détection et de correction des attaques DoS à parcours lent** (alerte d'activité de traitement élevée) : AIOps pour NGFW détecte les attaques de DoS à chemin lent grâce à une technologie alimentée par l'IA, garantissant la sécurité du réseau et une disponibilité ininterrompue des services. Il effectue des alertes d'activité de traitement de plan de données élevé, une analyse des causes premières d'activité de déni de politique élevée et des suggestions de mesures correctives basées sur l'analyse de causalité.
- **Détection et correction de l'activité de recherche de cache d'URL élevée** (alerte d'activité de traitement élevée) : AIOps pour NGFW détecte et traite l'activité de recherche de cache d'URL élevée, optimisant l'efficacité du traitement et maintenant la stabilité du système. Cette fonctionnalité établit une corrélation entre l'activité de recherche du cache d'URL et l'utilisation du processeur DP, identifie l'utilisation élevée du processeur et fournit des suggestions de correction pour éviter les scénarios de quasi-saturation.
- **Détection et correction des activités de traitement de contenu élevées** (alerte d'activité de traitement élevée) : La fonctionnalité AIOps pour NGFW détecte une activité de traitement de contenu élevée. Cette fonctionnalité analyse les corrélations entre les diverses étapes de traitement du contenu et l'utilisation du processeur du plan de données, identifie les cas d'utilisation élevée du processeur ou de conditions de quasi-saturation, et fournit des suggestions de correction exploitables pour améliorer la stabilité du système.
- **Rapport RCA de certificat trop long** (alerte d'échec d'opération Commit Push [validation et transmission]) : AIOps pour NGFW détecte un échec de validation et décrit les causes potentielles des échecs de validation, en particulier lorsque la longueur du certificat dépasse la taille de la mémoire tampon.

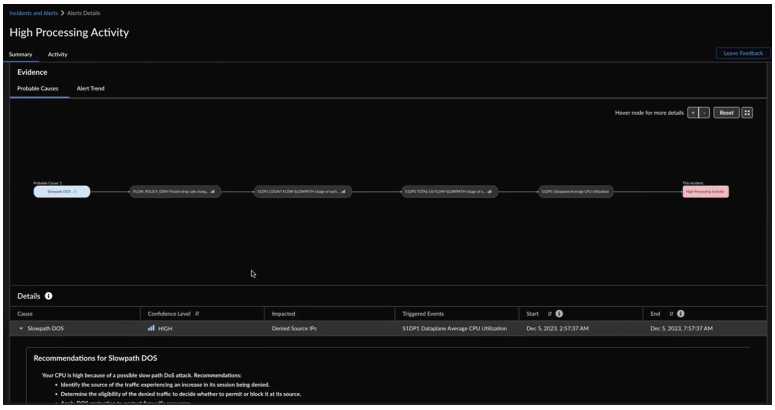
STEP 1 | Dans **Incidents & Alerts (Incidents et alertes)** > **Alerts (Alertes)**, sélectionnez une alerte pour ouvrir une page contenant les détails de l'alerte.



L'organigramme indique ce qui suit :

- événements qui ont déclenché l'alerte d'activité de traitement élevée
- cause probable de l'événement déclenché

Vous pouvez également passer votre curseur sur les nœuds pour afficher plus de détails tels que la cause probable, le niveau de confiance, l'événement déclenché et la durée de l'impact. Chaque fois qu'il y a trois nœuds d'événements ou plus, vous pouvez cliquer sur les événements et les développer pour afficher les détails.



AIOps pour NFGW affiche également les mêmes informations sous forme de tableau. Vous pouvez passer votre curseur sur une cause probable dans le tableau pour voir les nœuds en surbrillance et le chemin dans l'organigramme. Vous pouvez également cliquer sur une cause probable dans l'organigramme pour afficher ses détails dans le format tabulaire.

Confidence Level (Niveau de confiance) indique comment certains systèmes AIOp pour NGFW identifient les causes de l'alerte d'activité de traitement élevée. Les causes probables sont triées par ordre décroissant du niveau de confiance. Vous pouvez commencer par vérifier les causes avec un niveau de confiance élevé.

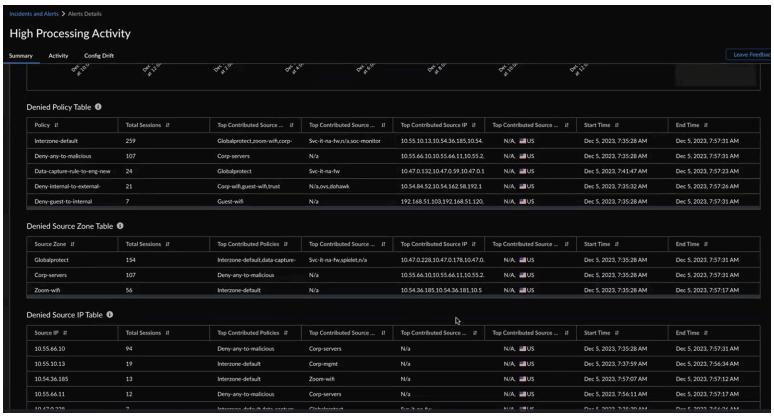
STEP 2 | Développez une cause probable dans le tableau pour afficher les graphiques et les mesures impactées que vous souhaitez étudier pour le déclenchement de l'alerte.

STEP 3 | Utilisez des outils graphiques pour inspecter les graphiques.

La période de causalité vous permet de visualiser la relation de cause à effet entre **la cause** de l'alerte et l'**événement déclenché** dans le temps.

Vous pouvez visualiser 6 heures, 24 heures ou 48 heures avant et après l'impact dans le graphique.

L'analyse de la cause probable est améliorée pour utiliser les registres SLS et fournir des métadonnées supplémentaires à la cause probable qui a mené à la création d'une alerte ou d'un incident. Cette amélioration vous permet de localiser les stratégies, les applications, les zones sources, les URL, les adresses IP sources et les régions potentiellement à l'origine de l'alerte. Par exemple, lorsque l'utilisation élevée du processeur du plan de données déclenche une alerte d'**activité de traitement élevée**, vous pouvez utiliser l'analyse des causes probables pour identifier les principaux contributeurs à l'alerte et suivre les recommandations de correction suggérées.



Prévision et détection d’anomalies

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Normalement, AIOps for NGFW détecte les problèmes en appliquant des règles fixes aux mesures de votre déploiement. Par exemple, si l’utilisation du processeur du plan de gestion dépasse 85 %, la mesure entre dans un état critique.

Cependant, pour vous alerter des événements que les règles fixes pourraient manquer, AIOps for NGFW peut utiliser l’apprentissage automatique pour comprendre votre déploiement et vous proposer des alertes et des incidents supplémentaires adaptés à vos tendances d’utilisation.

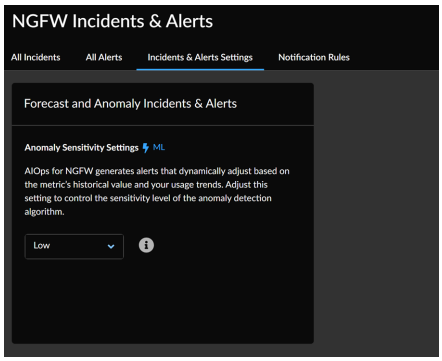
- Les **alertes basées sur les prévisions** vous aident à anticiper les problèmes en projetant la manière dont une mesure de périphérique peut changer et en vous alertant en conséquence.
- Les **alertes basées sur les anomalies** établissent un comportement de base pour une mesure de périphérique et vous alertent lorsque cette mesure dépasse les **paramètres de sensibilité aux anomalies** que vous spécifiez.

Les avantages de la prévision et de la détection des anomalies sont les suivants :

- Gestion proactive : En prévoyant les problèmes potentiels et en identifiant les anomalies à un stade précoce, les administrateurs peuvent prendre des mesures proactives pour prévenir les problèmes, réduire les interruptions et améliorer les performances globales du réseau.
- Sécurité renforcée : La détection de modèles et de comportements inhabituels peut aider à identifier les menaces et les vulnérabilités en matière de sécurité, permettant ainsi une intervention et une atténuation en temps opportun.
- Ressources optimisées : Les prévisions contribuent à une meilleure planification et à une meilleure allocation des ressources, garantissant que l’infrastructure du réseau est correctement préparée pour gérer les demandes futures.

Accédez à **Incidents & Alerts (Incidents et alertes)** > **Incident & Alert Settings (Paramètres d’incident et d’alerte)** > **Forecast and Anomaly Incidents & Alerts (Prévisions, incidents et alertes d’anomalies)**.

AIOps for NGFW génère des alertes et des incidents qui s’ajustent de manière dynamique en fonction de la valeur historique de la mesure et de vos tendances d’utilisation. Les écarts par rapport à la bande de normalité peuvent indiquer des problèmes potentiels. Cette option permet de contrôler le niveau de sensibilité de l’algorithme de détection des anomalies.



Gérer les alertes de l’analyseur de capacité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
•	❑ ou

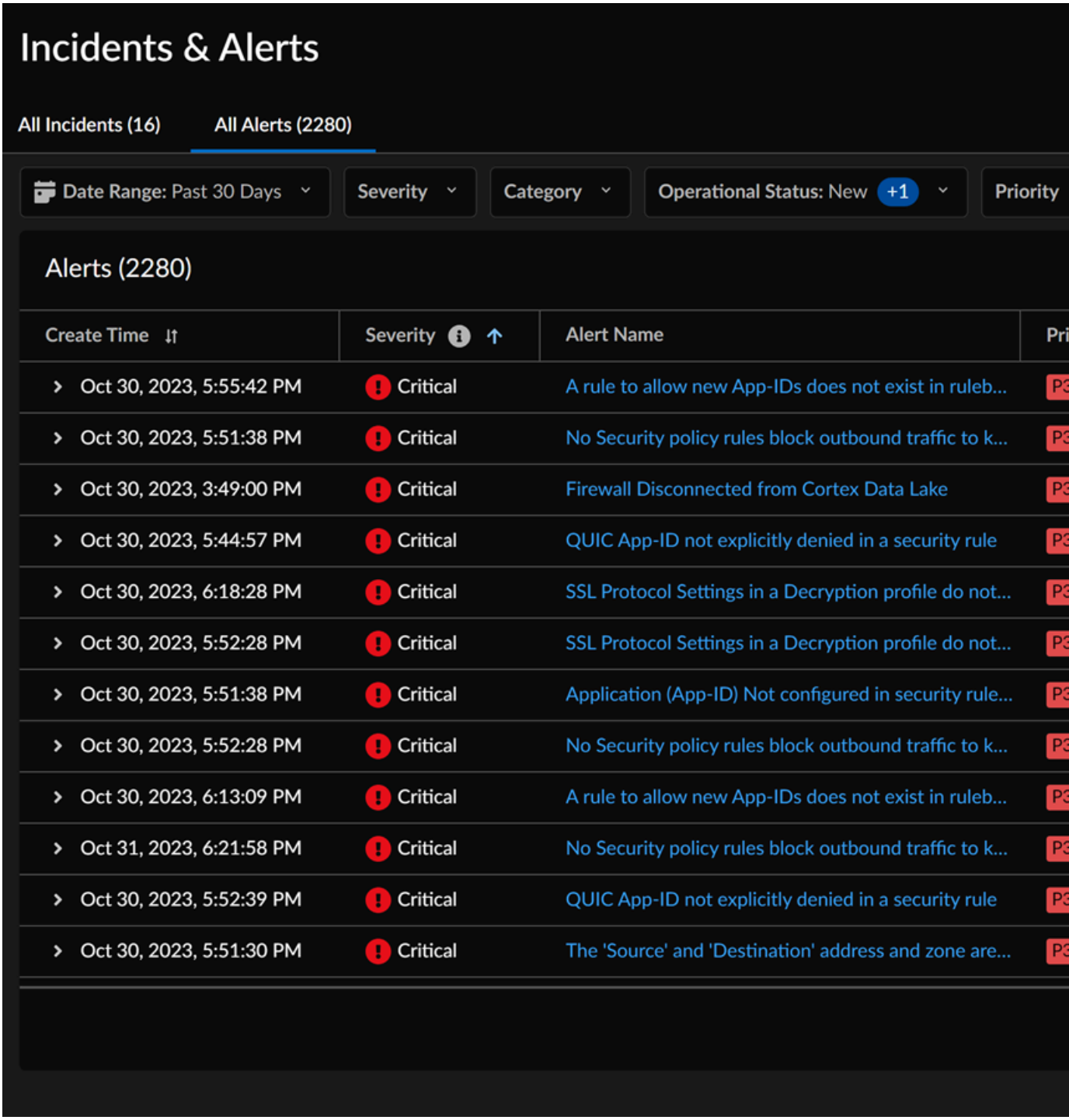
Capacity Analyzer utilise des modèles d’apprentissage automatique pour anticiper une consommation de ressources proche de sa capacité maximale et lancer des alertes. Les alertes Capacity Analyzer sont générées à l’avance en identifiant les bottlenecks potentiels.

Vous pouvez également créer une règle de notification pour déclencher des notifications pour les alertes de l’analyseur de capacité.

STEP 1 | Accédez à **Incidents & Alerts (Incidents et alertes)** > **NGFW** > **All Alerts (Toutes les alertes)** et cliquez sur **List View (Affichage de la liste)**.

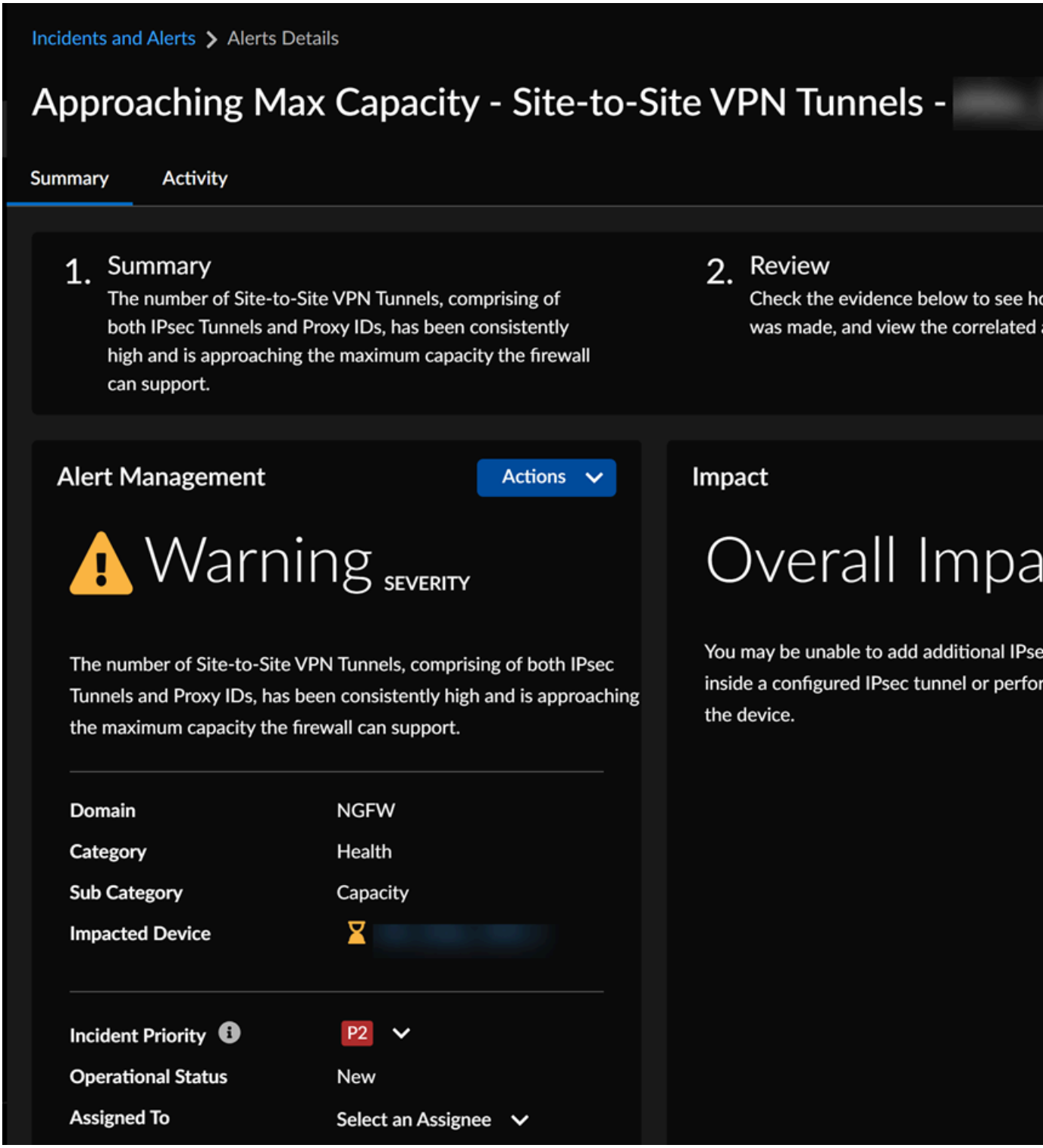
STEP 2 | Sous **Alert Name (Nom de l'alerte)**, recherchez les **alertes maximales proches**.

Les alertes levées pour la fonctionnalité d'analyseur de capacité sont nommées comme : **Approche de la capacité maximale approchante** : *<Metric-Name>*.



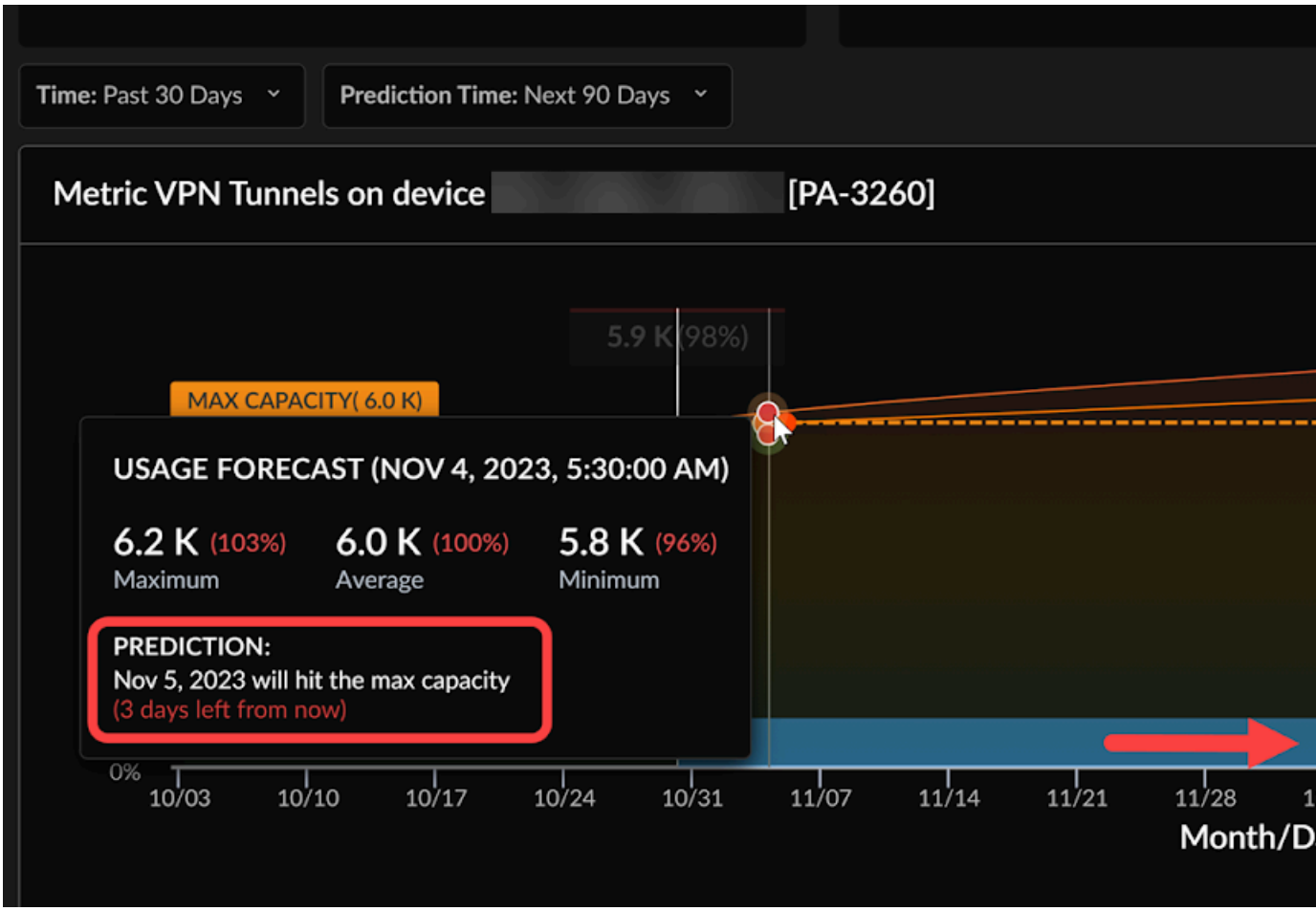
STEP 3 | Sélectionnez l'une des alertes pour afficher ses détails qui incluent:

- Résumé de l'alerte avec détails.
- Impact causé par l'alerte.
- Mesures recommandées pour résoudre votre problème.

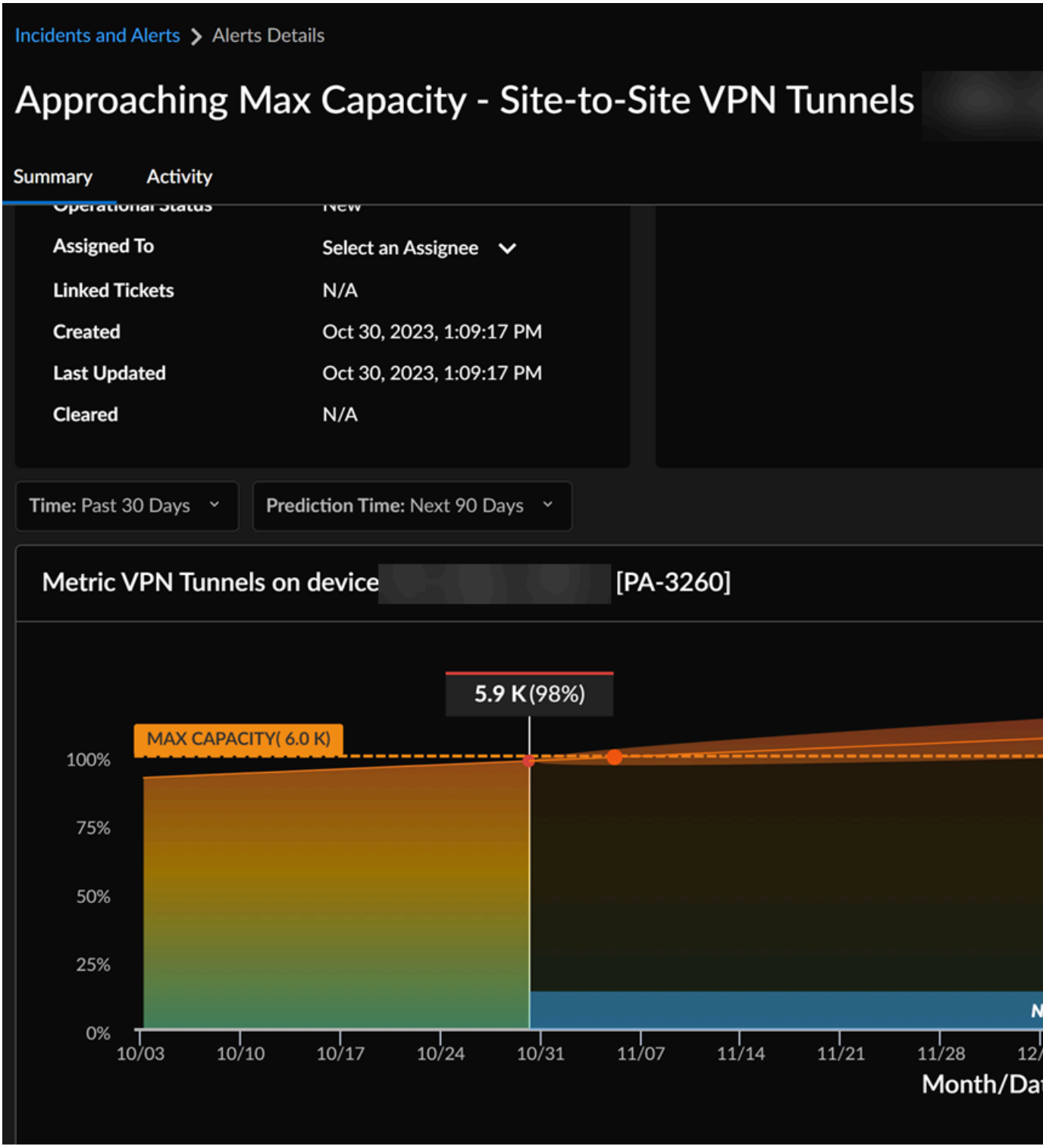


Dans les détails de l'alerte, vous pouvez également afficher un graphique qui montre la tendance pour la métrique. Strata Cloud Manager prévoit la date à laquelle la métrique atteindra la capacité maximale. Vous pouvez faire passer votre curseur sur le graphique pour vérifier la capacité métrique à un moment précis. Vous pouvez sélectionner un **temps de prévision** pour les 30 prochains jours ou 90 prochains jours.

Dans cet exemple, vous pouvez voir que la mesure des tunnels VPN sur le périphérique atteindra sa capacité maximale le **5 novembre 2023**.



STEP 4 | À partir de la page **Alerts (Alertes)**, vous pouvez vous **rendre sur Page Analyseur de capacité** pour afficher la carte thermique de l'analyseur de capacité.



Pour plus d'informations sur l'utilisation de la carte thermique de l'analyseur de capacité et vérifier les alertes de capacité, voir Analyser la capacité métrique.

Mesures d’utilisation du processeur dans AIOps pour NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

L’utilisation du processeur est suivie dans AIOps pour NGFW avec les mesures suivantes :

- **mp_system_resources.mp_cpu** : Indique l’utilisation totale du processeur.
- **mp_system_resources_daemon.cpu_usage_sum** : Indique l’utilisation du processeur résultant des tâches du plan de gestion exécutées dans le processeur du plan de gestion (MP-CPU). Cette mesure est équivalente à l’utilisation du processeur trouvée dans SNMP.
- **mp_system_resources_daemon.pan_task_cpu_usage** : Indique l’utilisation du processeur résultant des tâches PAN exécutées dans le processeur MP-CPU effectuant des opérations de type plan de données. Ces données ne font pas partie de SNMP et de la mesure **mp_system_resources_daemon.pan_task_cpu_usage**.

L’utilisation totale du processeur est calculée comme suit :

mp_system_resources.mp_cpu = **mp_system_resources_daemon.cpu_usage_sum** + **mp_system_resources_daemon.pan_task_cpu_usage**

Créer une règle de notification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

L'intégration de Strata Cloud Manager à vos opérations existantes implique la configuration d'alertes proactives, vous permettant de détecter et de gérer les problèmes potentiels avant qu'ils ne dégénèrent en complications graves. Ces alertes peuvent être adaptées pour correspondre au protocole de gestion des cas de votre équipe d'exploitation, comme les P1 ou P2 couramment utilisés.

Par exemple, vous pouvez configurer un système d'alerte dans lequel les alertes critiques, qui représentent les problèmes les plus critiques, sont instantanément transmises à votre équipe de sécurité pour une attention immédiate. D'un autre côté, les alertes d'alerte, qui sont moins urgentes mais toujours importantes, peuvent être organisées pour un examen quotidien. Un tel arrangement assure une gestion efficace des incidents tout en maintenant le bon déroulement de vos opérations.

Une autre option consiste à acheminer les alertes en fonction des équipes ; certaines catégories d'alertes, voire des alertes spécifiques, peuvent être acheminées vers différentes équipes qui seront les mieux armées pour les traiter. Vous pouvez définir des préférences de notification, telles que les alertes qui déclenchent des notifications, la façon dont vous recevez les notifications et la fréquence à laquelle vous les recevez ; pour cela, créez une règle de notification.

Voici une vidéo qui montre comment créer une règle de notification.

STEP 1 | Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Incident & Alert Settings (Paramètres d'incident et d'alerte)** > **Notification Rules (Règles de notification)** > **+ Add Notification Rule (Ajouter une règle de notification)**

STEP 2 | Entrez un `nom` et une `description`.

STEP 3 | **Ajoutez une nouvelle condition** pour spécifier l'icône `Rule Conditions (Conditions de la règle)` cela déclenchera la notification.

Par exemple, pour créer une notification pour les alertes matérielles, sélectionnez **subCategory (Sous-catégorie)**, **Equals (Égale)**et **Hardware (Matériel)**.

STEP 4 | Sélectionnez le `type de notification et destinataires` de la notification.

1. Si vous choisissez **Email**, sélectionnez un groupe d'email, c'est-à-dire un groupe d'utilisateurs qui recevront les notifications par e-mail. Vous pouvez aussi choisir **Create a New Email Group (Créer un nouveau groupe d'email)**.
   1. Si vous créez un nouveau groupe d'email, entrez un nom de groupe d'email et commencez à saisir les adresses email des personnes que vous souhaitez ajouter au groupe. Appuyez sur la touche Retour après avoir renseigné chaque adresse email.
   2. Sélectionnez **Next (Suivant)**.
   3. Sélectionnez la fréquence à laquelle vous souhaitez envoyer ces notifications :
   - Immédiatement
   - Groupé et envoyé toutes les 4 heures
   - Groupé et envoyé une fois par jour
2. Si vous choisissez **ServiceNow**, entrez l'URL `ServiceNow`, les informations d'identification du client, les informations d'identification ServiceNow et la `version de l'API ServiceNow`.
   1. **Testez** votre connexion pour vous assurer que l'intégration fonctionne.
   2. Sélectionnez **Next (Suivant)**.

STEP 5 | **Enregistrez la règle**.

Intégration avec ServiceNow

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	❑ ou

Lors de la configuration de votre intégration ServiceNow sur la règle de notification AIOps for NGFW, vous avez besoin des éléments suivants :

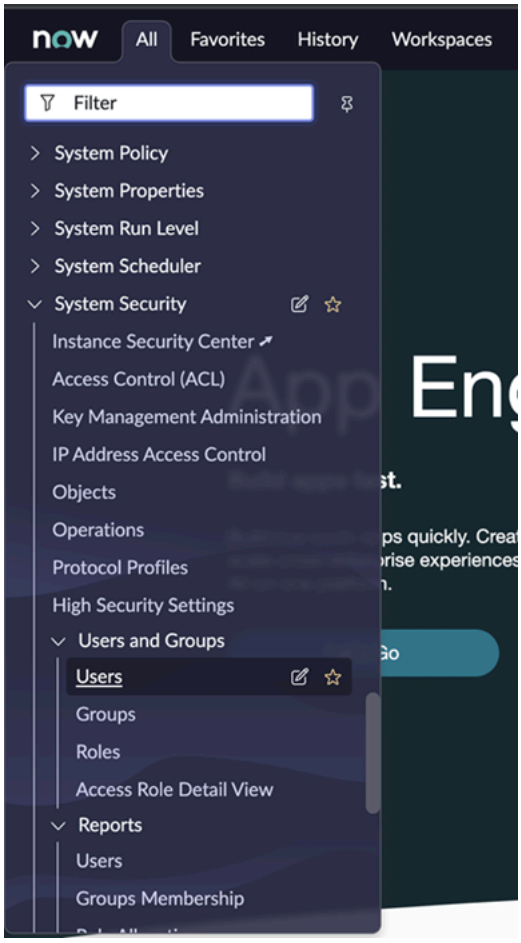
- Instance ServiceNow configurée avec accès administratif
- Nom d'utilisateur et mot de passe ServiceNow avec accès Web et rôles spécifiques pour créer des incidents ou interroger diverses tables
- Identifiant client et mot de passe créés sous Application Registry (Registre d'applications) afin d'autoriser AIOps à accéder à votre instance ServiceNow
- URL de votre instance ServiceNow

Votre instance ServiceNow devrait également disposer d'une table **Incidents** à laquelle AIOps pourrait envoyer des alertes et des **groupes d'affectation** avec des **destinataires** afin que ces alertes puissent être destinées à des personnes spécifiques.

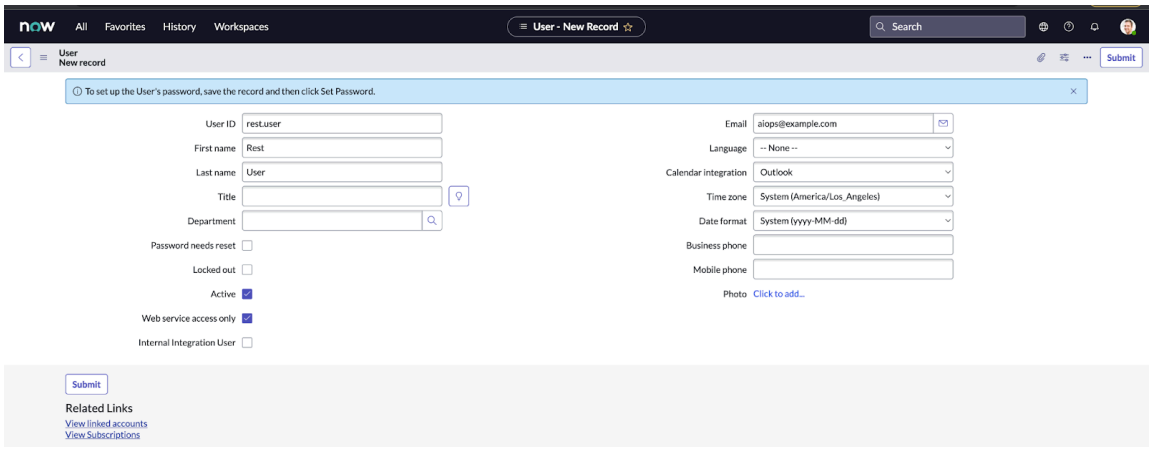
STEP 1 | Création d'un utilisateur ServiceNow Rest.

Créez un nouvel utilisateur ServiceNow avec des rôles spécifiques pour lire et écrire dans les différentes tables nécessaires à l'intégration (Incident, Groupes d'affectation et Destinataires).

1. Pour créer un utilisateur dans ServiceNow, accédez à **Users (Utilisateurs)** sous **Security (Sécurité) > Users and Groups (Utilisateurs et groupes)**.

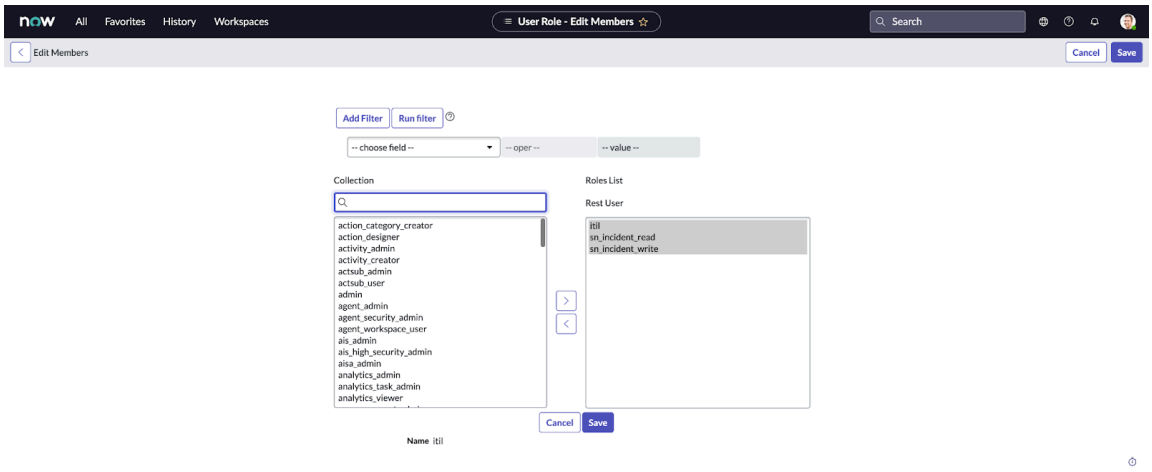


2. Cochez la case **Web service access only (Accès au service web uniquement)** et soumettez vos modifications.



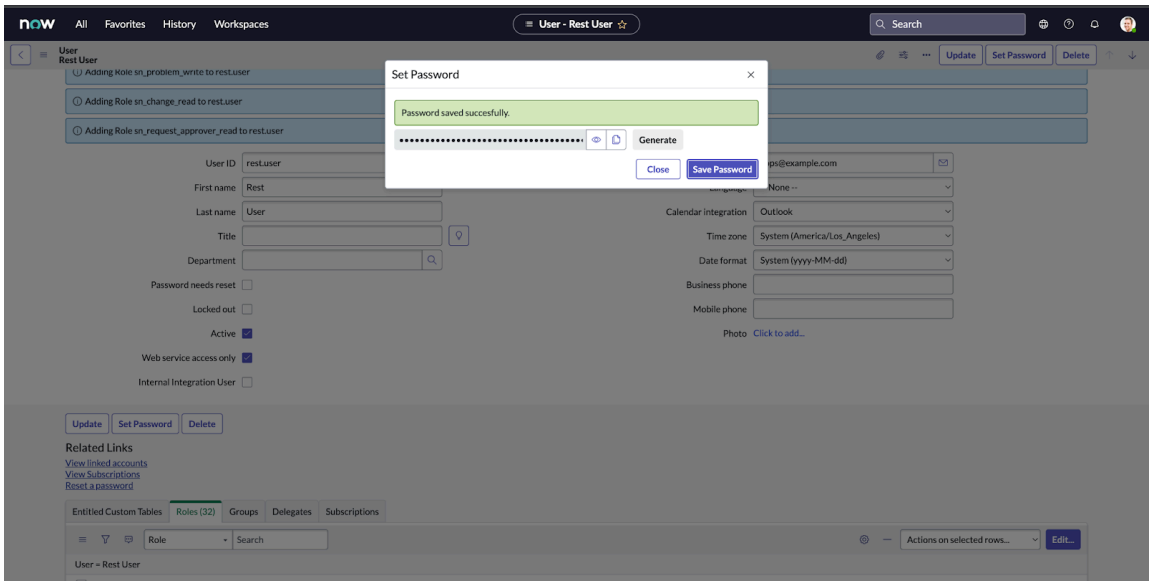
3. Recherchez l'utilisateur nouvellement créé. Sélectionnez l'onglet **Roles (Rôles)** dans le tableau en bas de page et cliquez sur **Edit (Modifier)**. Vous devrez donner à l'utilisateur

les autorisations pour les trois rôles suivants : **itil, sn_incident_read** et **sn_incident_write**. Cliquez sur Save (Enregistrer) pour enregistrer vos modifications.



4. Cliquez sur **Set Password (Définir le mot de passe)** sur la page User (Utilisateur). Dans la fenêtre contextuelle, cliquez sur **Generate (Générer)** et **Save Password (Enregistrer le mot de passe)**. Assurez-vous de copier le mot de passe dans un endroit sécurisé avec l'identifiant de l'utilisateur. Ces informations seront utilisées pour remplir

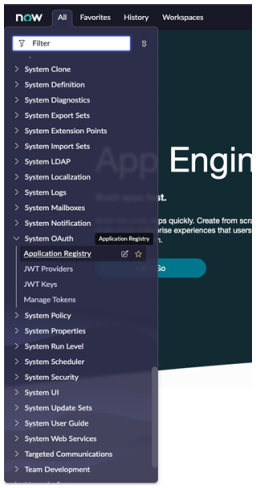
les informations d'identification **ServiceNow User (Utilisateur ServiceNow)** dans AIOps for NGFW.



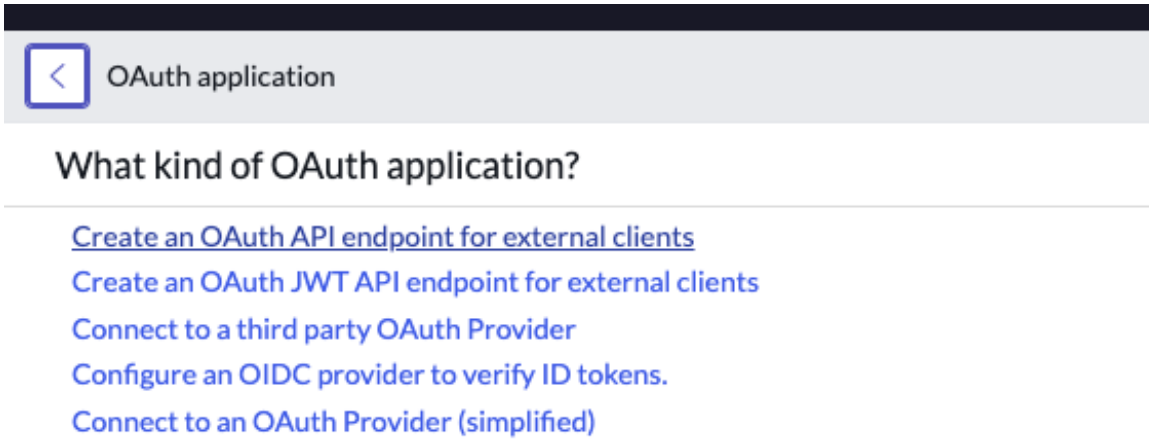
STEP 2 | Créez un client OAuth web.

Un client OAuth est nécessaire pour qu'AIOps for NGFW puisse s'authentifier dans votre instance ServiceNow.

1. Accédez à **System OAuth (OAuth système) > Application Registry (Registre d'applications)**.

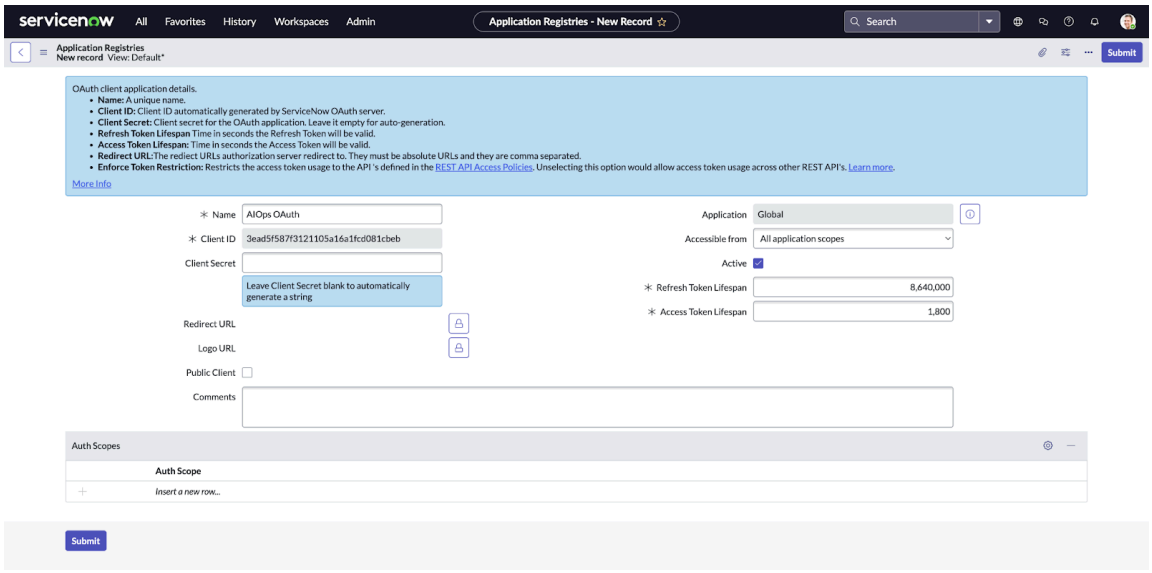


2. Créez une nouvelle entrée et sélectionnez **Create an OAuth API endpoint for external clients (Créer un terminal API OAuth pour clients externes)** dans la page suivante.



3. Ajoutez un nom pour l'OAuth et créez un **secret client**. Le **secret client** peut également être laissé vide si un secret généré automatiquement est recherché. Cliquez sur **Submit (Envoyer)**, puis accédez à nouveau à l'entrée Application Registry (Registre d'applications) et enregistrez l'**identifiant client** et le **secret client** dans un endroit sûr.

Ces informations seront utilisées sous les formulaires **Client credential (informations d'identification du client)** en AIOps for NGFW.



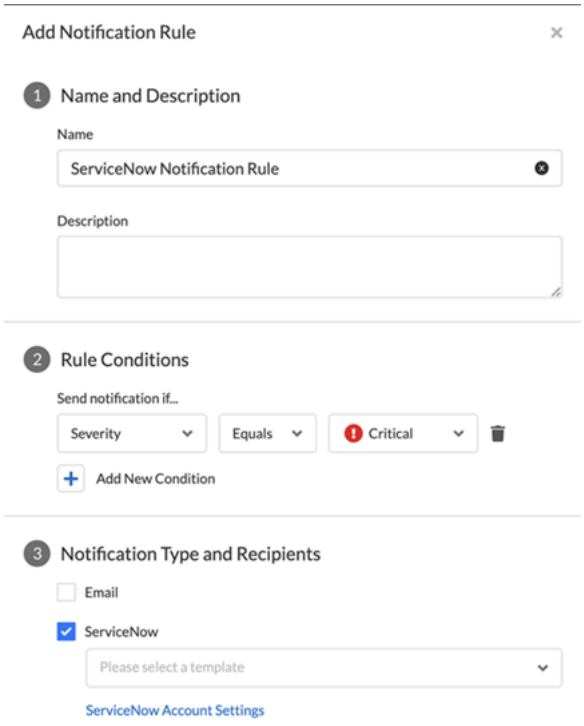
STEP 3 | Ajoutez des informations sur les paramètres du compte ServiceNow dans AIOps for NGFW.

Ajoutez les informations des étapes précédentes dans AIOps for NGFW pour terminer l'intégration entre ServiceNow et AIOps for NGFW.

Vous avez besoin des éléments suivants :

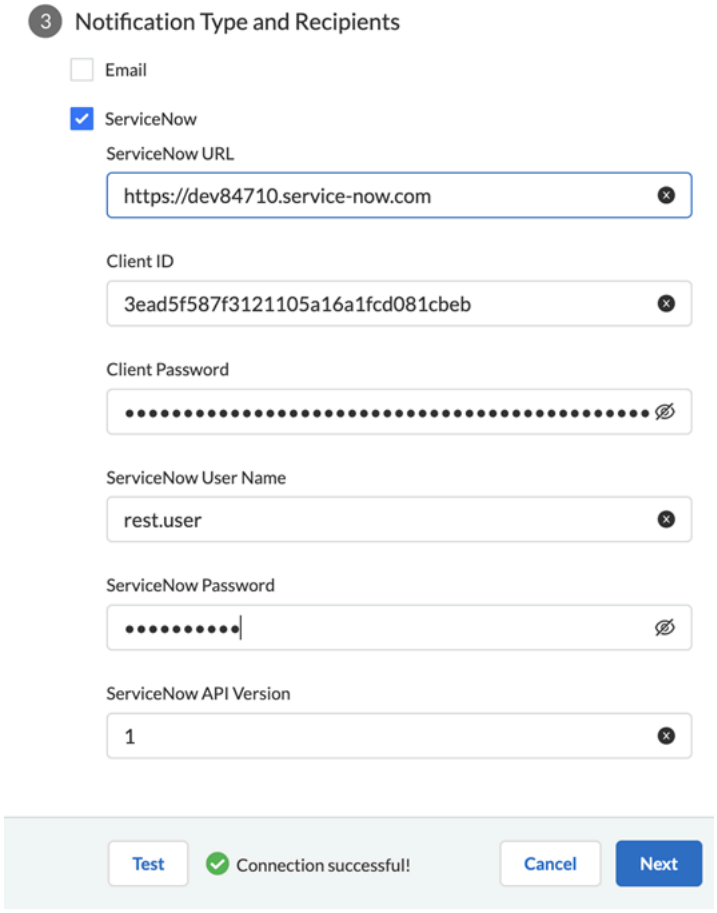
- Votre **URL d'instance ServiceNow**
- **Utilisateur ServiceNow** et **mot de passe** de l'étape 1
- **ID client** et **secret client** de l'étape 2

1. Dans AIOps for NGFW, accédez à **Alert Notification Rules (Règles de notification d'alerte)** et cliquez sur **Add Notification Rule (Ajouter une règle de notification)**.

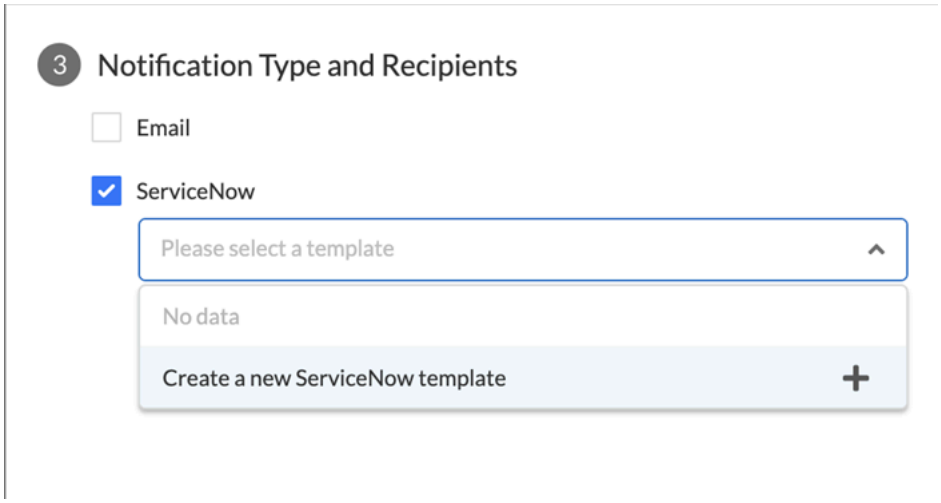


2. Remplissez des champs tels que **Rule Name (Nom de règle)** et **Alert Condition (Condition d'alerte)**, puis cochez la case **ServiceNow** sous **Notification Type and Recipients (Type de notification et destinataires)**.
3. Cliquez sur **ServiceNow Account Settings (Paramètres du compte ServiceNow)** en bas de la barre latérale. Remplissez le formulaire suivant avec les informations qui ont été enregistrées précédemment. **Utilisateur ServiceNow** et **mot de passe ServiceNow** l'étape 1, où vous devez configurer l'utilisateur Rest. **ID du client** et **secret client** de l'étape 2, où vous devez configurer l'enregistrement de l'application. Laissez la version telle quelle. Cliquez sur **Test** pour enregistrer la configuration et poster un incident de

test sur votre instance ServiceNow. Cette action doit réussir pour que vous puissiez continuer. Cliquez sur **Next (Suivant)**.



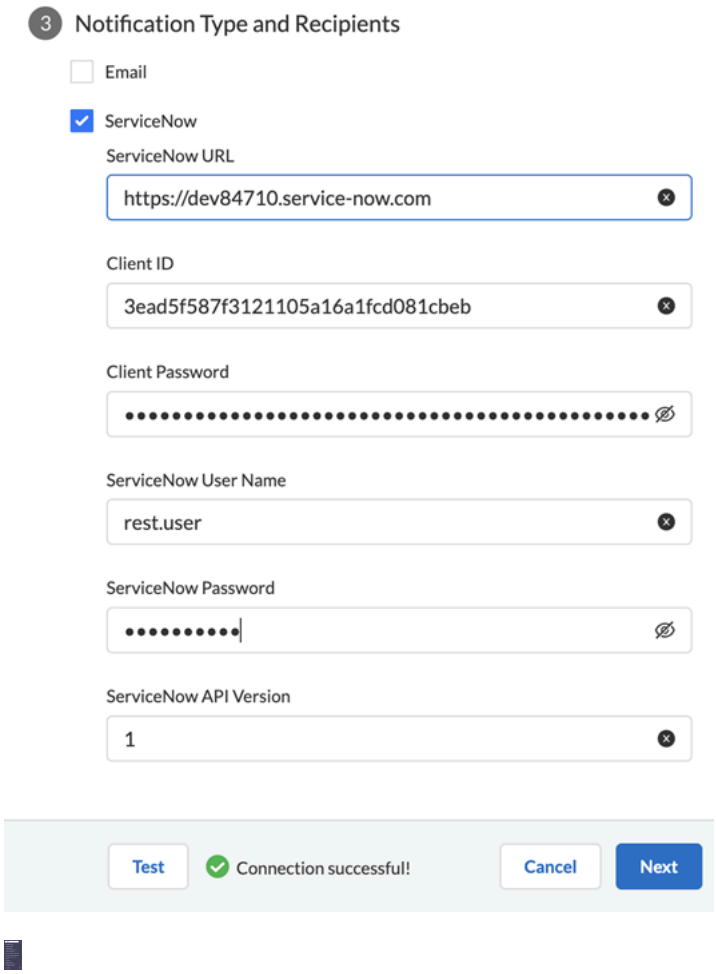
4. Développez la liste déroulante **Please select a template (Veuillez sélectionner un modèle)**, puis cliquez sur **Create a new ServiceNow Template (Créer un nouveau modèle ServiceNow)**.



5. Entrez le **nom du modèle ServiceNow**, puis choisissez un groupe dans la liste déroulante **Assignment Group (Groupe d'affectation)**. Choisissez un destinataire dans la liste déroulante **Assignee (Destinataire)**. Notez que ces listes déroulantes doivent être remplies par appel des tables suivantes depuis votre instance ServiceNow :

   - **System Security (Sécurité système) > Users and Groups (Utilisateurs et groupes) > Users (Utilisateurs)**
   - **System Security (Sécurité système) > Users and Groups (Utilisateurs et groupes) > Groups (Groupes)**

   S'il n'y a pas de groupes définis, la liste déroulante **Assignment Group (Groupe d'affectation)** ne se remplira pas. S'il n'y a pas d'Utilisateurs affectés à un Groupe spécifique, la liste déroulante **Assignees (Affectés)** ne s'affichera pas. Cliquez sur **Next (Suivant)**, puis sur **Save Rule (Enregistrer la règle)**.



Référence d'alerte AIOps for NGFW

Bienvenue dans la référence d'alerte AIOps for NGFW. Les alertes sur la santé surveillent activement la santé et les performances de votre plateforme en temps réel. Cette approche aide à identifier les problèmes, à prévoir les problèmes potentiels et à mettre en œuvre des mesures correctives pour garantir le fonctionnement optimal de vos périphériques. Voici quelques aspects clés :

- Surveillance des mesures : Surveillez en permanence diverses mesures des NGFW, y compris l'utilisation du processeur, l'utilisation de la mémoire, l'espace disque, le débit réseau et d'autres indicateurs de performance pertinents. Cette surveillance constante garantit que tout écart par rapport à la performance normale est rapidement identifié.
- Détection des anomalies : Générez des alertes qui s'ajustent de manière dynamique en fonction de la valeur historique de la mesure et de vos tendances d'utilisation. En exploitant les données historiques, le système peut détecter les anomalies qui pourraient indiquer des problèmes potentiels, ce qui permet une gestion proactive.
- Analyse prédictive : Prévoyez quand certains seuils sont dépassés ou quand des événements spécifiques se produisent en analysant les données et les modèles historiques. Cela permet de prévoir les problèmes potentiels avant qu'ils ne dégénèrent.

Les pages suivantes identifient les alertes qu'AIOps for NGFW peut déclencher.

- Alertes de santé premium : Consultez les alertes premium que Strata Cloud Manager peut déclencher et qui sont liées à la santé de votre plateforme.
- Alertes de santé gratuites : Consultez les alertes gratuites qu'AIOps for NGFW peut déclencher et qui sont liées à la santé de votre plateforme.
- Alertes de service : Consultez les alertes qu'AIOps for NGFW peut déclencher en rapport avec les services qui y sont liés.
- Alertes déclenchées par l'apprentissage automatique : Consultez les alertes que Strata Cloud Manager peut déclencher en tirant parti de l'apprentissage automatique.

Pour obtenir des informations sur les vérifications de posture de sécurité qu'AIOps for NGFW peut déclencher, accédez au tableau **Manage (Gérer) > Security Posture (Posture de sécurité) > Settings (Paramètres) > Security Checks (Vérifications de sécurité)** pour afficher les vérifications.

Alertes de santé premium

Le tableau suivant identifie les alertes premium que Strata Cloud Manager peut déclencher et qui sont liées à la santé de votre plateforme.

Une licence Premium AIOps for NGFW est requise pour que Strata Cloud Manager déclenche ces alertes.

Alerter	Description
Défaillance de la requête ACC (Alerte premium)	Cette alerte détecte si la requête Application Command Center (Centre de commande des applications - ACC) a échoué. Classe : Santé Catégorie : Création de rapports Ticket de support intégré dans l'appli : Non
Utilisation défavorable des ressources de trafic chiffré (Alerte premium)	Les ressources de trafic chiffrées sont faibles. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Utilisation défavorable des ressources (Alerte premium)	Le pare-feu présente des valeurs anormales de connexions par seconde (CPS), de débit ou de nombre de sessions. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : table ARP (Alerte premium)	L'analyse des prévisions de données montre que les entrées de la table ARP sont en passe d'atteindre bientôt la capacité maximale du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : groupes d'adresses (Alerte premium)	Le nombre d'objets de groupe d'adresses a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non

Alerter	Description
Approche de la capacité maximale : objets d'adresse (Alerte premium)	Le nombre d'objets d'adresse a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : processeur du plan de données (Alerte premium)	L'utilisation du processeur du plan de données (DP) a été constamment élevée au fil du temps et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : utilisation du décryptage (Alerte premium)	L'analyse des prévisions de données montre que les sessions de décryptage SSL sont en passe d'atteindre bientôt la capacité maximale du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : adresses FQDN (Alerte premium)	Le nombre d'objets d'adresse FQDN a été constamment élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : tunnels GlobalProtect (sans client) (Alerte premium)	Le nombre de tunnels VPN GlobalProtect sans client s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : homologues IKE (Alerte premium)	Le nombre d'homologues IKE a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non

Alerter	Description
Approche de la capacité maximale : processeur du plan de gestion (Alerte premium)	L'utilisation du processeur du plan de gestion (MP) a été constamment élevée et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : mémoire du plan de gestion (Alerte premium)	L'utilisation de la mémoire du plan de gestion (MP) a été constamment élevée et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : politiques NAT (Alerte premium)	Le nombre de règles de politique NAT a été constamment élevé au fil du temps et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : politiques de sécurité (Alerte premium)	Le nombre de règles de politique de sécurité a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : groupes de services (Alerte premium)	Le nombre d'objets de groupe de services a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : objets de service (Alerte premium)	Le nombre d'objets de service a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité

Alerter	Description
	Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : utilisation de la table de session (Alerte premium)	L'utilisation de la table de session (%) a été constamment élevée au fil du temps et s'approche de la capacité maximale que le pare-feu ou la licence de VM peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : tunnels VPN site à site (Alerte premium)	Le nombre de tunnels VPN site à site, comprenant à la fois des tunnels IPsec et des ID de proxy, a été constamment élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : URL ou adresses IP dans les EDL (Alerte premium)	Le nombre d'URL, d'adresses IP ou de domaines au sein des EDL configurées utilisées dans la politique sur ce pare-feu s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : systèmes virtuels (Alerte premium)	L'analyse des prévisions de données montre que la configuration des systèmes virtuels est en passe d'atteindre la capacité maximale prise en charge par la licence du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche des limites de configuration maximales (Alerte premium)	Les objets de pare-feu tels que les règles, les groupes et les profils de sécurité approchent des limites de périphérique. Classe : Santé Catégorie : Configurer les limites Ticket de support intégré dans l'appli : Non
Expiration du certificat (Alerte premium)	Un ou plusieurs certificats sur le pare-feu ont été révoqués ou expirent bientôt. Classe : Santé

Alerter	Description
	Catégorie : certificate Ticket de support intégré dans l'appli : Non
Échec de l'opération Commit Push (validation transmission) (Alerte premium)	La transmission de la configuration a échoué. Classe : Santé Catégorie : Configuration Ticket de support intégré dans l'appli : Non
L'utilisation de la mémoire de configuration s'approche des limites maximales (Alerte premium)	La configuration du pare-feu s'approche de sa limite maximale d'utilisation de la mémoire. Lors des validations, la mémoire de configuration totale du pare-feu doit prendre en charge deux copies : la configuration « en cours d'utilisation » et la nouvelle configuration « à utiliser ». Si la mémoire allouée par configuration dépasse 50 %, le pare-feu atteint sa capacité, ce qui entraîne la défaillance de la validation. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Abandon de paquet DP (Alerte premium)	L'alerte détecte un abandon anormal de paquet pour différentes raisons Classe : Santé Catégorie : Performance Ticket de support intégré dans l'appli : Non
État des liaisons HA (Alerte premium)	Intégrité d'un lien connecté au pare-feu. Le pare-feu est connecté à divers systèmes pour divers services. Cette alerte fournit l'intégrité de ces connexions. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non
Taux d'ingestion logarithmique élevé (Alerte premium)	Un collecteur de journaux approche de son taux d'ingestion maximal pris en charge. Classe : Santé Catégorie : de journalisation Ticket de support intégré dans l'appli : Non
Activité de requête de journal élevée	Le collecteur de journaux approche de sa capacité de tâches de requête ou de rapports.

Alerter	Description
(Alerte premium)	Classe : Santé Catégorie : de journalisation Ticket de support intégré dans l'appli : Non
Latence accrue du trafic – Mémoire tampon de paquets (Alerte premium)	Les ressources de la mémoire tampon de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Latence accrue du trafic – Descripteur de paquets (Alerte premium)	Les ressources du descripteur de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Augmentation de la latence du trafic : TCP ou UDP inconnu (Alerte premium)	Le pare-feu a reçu une grande quantité de trafic dont l'application est classée comme unknown-tcp (TCP inconnu) ou unknown-udp (UDP inconnu). Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Perte de connexion à la destination de transfert de journaux (Alerte premium)	Le périphérique ne parvient pas à se connecter à sa destination de transfert de journaux. Classe : Santé Catégorie : de journalisation Ticket de support intégré dans l'appli : Non
Période minimale de conservation des journaux dépassée (Alerte premium)	Le collecteur de journaux contient des journaux antérieurs à la période de rétention minimale définie. Classe : Santé Catégorie : de journalisation Ticket de support intégré dans l'appli : Non
Échec de l'allocation NAT (Alerte premium)	Au moins une règle NAT n'est pas en mesure d'allouer suffisamment de ressources à des fins de traduction. Classe : Santé

Alerter	Description
	Catégorie : Ressource de pool NAT Ticket de support intégré dans l'appli : Oui
Utilisation du pool NAT (Alerte premium)	Une ou plusieurs règles NAT ont une utilisation élevée des ressources. Classe : Santé Catégorie : Ressource de pool NAT Ticket de support intégré dans l'appli : Non
Alerte de performance de l'application NGFW SD-WAN (Alerte premium)	Indique la liste des applications affectées par des performances de liaison médiocres. Classe : Santé Catégorie : Performance SD-WAN Ticket de support intégré dans l'appli : Non
Alerte de performance des liens NGFW SD-WAN (Alerte premium)	Indique ce qui entraîne une dégradation des performances de vos applications, services ou liaisons. Classe : Santé Catégorie : Performance SD-WAN Ticket de support intégré dans l'appli : Non
Niveau de journalisation autre que le niveau par défaut (Alerte premium)	Cette alerte est déclenchée lorsque le niveau de journalisation d'un service n'est pas défini sur sa configuration par défaut. Cette alerte permet de s'assurer que les services maintiennent systématiquement leurs paramètres de journalisation désignés. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Serveur surveillé d'agent User-ID intégré à PAN-OS déconnecté (Alerte premium)	Cette alerte se déclenche lorsque le serveur, surveillé par l'agent User-ID intégré à PAN-OS (ID utilisateur sans agent), perd la connexion avec le pare-feu. Ce serveur surveillé est un composant essentiel pour mapper les identités des utilisateurs aux activités réseau. Classe : Santé Catégorie : Ticket de support intégré dans l'appli : Non
L'utilisation de la mémoire de configuration de la	Cette alerte détecte si l'utilisation de la mémoire de configuration de la politique dépasse un seuil critique.

Alerter	Description
politique s'approche des limites maximales (Alerte premium)	Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Latence du trafic – Descripteurs de paquets (sur puce) (Alerte premium)	Les ressources (sur puce) du descripteur de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Saturation/DoS Ticket de support intégré dans l'appli : Non
Tunnel vers le bas (Alerte premium)	Un ou plusieurs tunnels VPN site à site sont défaillants. Classe : Santé Catégorie : VPN de site à site Ticket de support intégré dans l'appli : Oui
Profil de protection de zone – détection des saturations (Alerte premium)	Les connexions établies sur la zone ou le débit de paquets entrant sont excessifs ou anormaux. Classe : Santé Catégorie : Saturation/DoS Ticket de support intégré dans l'appli : Oui
Profil de protection de zone – recommandation de seuil (Alerte premium)	Il manque un profil de protection de zone dans une zone ou les valeurs de seuil d'un profil de protection de zone doivent être ajustées. Classe : Santé Catégorie : Saturation/DoS Ticket de support intégré dans l'appli : Non

Alertes de santé gratuites

Le tableau suivant identifie les alertes gratuites qu'AIOps for NGFW peut déclencher et qui sont liées à la santé de votre plateforme.

Une licence Premium n'est pas requise pour qu'AIOps for NGFW déclenche ces alertes.

Alerter	Description
Défaillance d'alimentation de la carte (Alerte gratuite)	Une défaillance de la carte a été détectée, suggérant un problème potentiel avec la carte ou son emplacement dans le châssis. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
La taille de la configuration atteint la limite de capacité du périphérique (Alerte gratuite)	La taille de configuration de cet périphérique a atteint sa limite de capacité. Classe : Santé Catégorie : Configuration Ticket de support intégré dans l'appli : Non
Lecteur système dégradé (Alerte gratuite)	Un lecteur système dégradé a été identifié lors de la surveillance de ses valeurs d'attributs. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Télémétrie retardée (Alerte gratuite)	Les moteurs d'analyse ne disposent d'aucune nouvelle télémétrie provenant de ce NGFW/Panorama. Classe : Santé Catégorie : Télémétrie Ticket de support intégré dans l'appli : Oui
Défaillance de la puce FE100 (Alerte gratuite)	Une erreur d'étalonnage a été détectée sur la puce FE100 dans le pare-feu. Ce problème indique généralement une défaillance matérielle. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non

Alerter	Description
Problèmes de ventilateur (Alerte gratuite)	Un ventilateur ou un plateau de ventilateur a déclenché une alarme sur le périphérique. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Défaillance fatale de vérification de la machine (Alerte gratuite)	Une défaillance fatale de vérification de la machine a été détectée. Ce problème indique généralement une défaillance matérielle du processeur. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Pare-feu déconnecté de Cortex Data Lake (Alerte gratuite)	La connexion entre FW et le service de journalisation Strata a été perdue. Classe : Santé Catégorie : Connectivité SLS Ticket de support intégré dans l'appli : Non
Pare-feu déconnecté de Panorama (Alerte gratuite)	La connexion entre le pare-feu et Panorama a été perdue. Classe : Santé Catégorie : Défaillance de connexion Ticket de support intégré dans l'appli : Non
Liaison HA de secours (Alerte gratuite)	La ou les liaisons HA de secours ne sont pas configurées pour le moment. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non
État de la connexion homologue HA (Alerte gratuite)	L'un des pare-feu de la paire HA est dans un état non intègre. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Oui
Utilisation élevée de l'espace disque – Partition Pancfg	La partition du disque dur approche de sa pleine capacité ou l'a atteinte. Classe : Santé

Alerter	Description
(Alerte gratuite)	Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Utilisation élevée de l'espace disque – Partition Panlogs (Alerte gratuite)	La partition du disque dur approche de sa pleine capacité ou l'a atteinte. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Utilisation élevée de l'espace disque – Partition racine (Alerte gratuite)	La partition du disque dur approche de sa pleine capacité ou l'a atteinte. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Activité de traitement élevée (Alerte gratuite)	Une ou plusieurs ressources informatiques sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Erreur IPQ (Alerte gratuite)	Une erreur IPQ (Ingress Packet Queue, file d'attente de paquet de sortie) a été détectée sur l'une des puces FE100 du pare-feu. Cette erreur indique généralement qu'une réinstallation est nécessaire ou qu'il y a une défaillance matérielle. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Alimentation d'entrée irrégulière (Alerte gratuite)	Les niveaux d'alimentation du périphérique ne sont pas compris dans la plage normale. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Expiration de la licence (Alerte gratuite)	Une ou plusieurs de vos licences approchent de leur expiration ou l'ont atteinte. Classe : Santé Catégorie : PanOS et abonnement

Alerter	Description
	Ticket de support intégré dans l'appli : Non
Défaillance du lecteur de journalisation (Alerte gratuite)	Un lecteur de journalisation défectueux a été identifié grâce à la surveillance de l'état du disque du pare-feu. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Carte MPC : défaillance CPLD (Alerte gratuite)	La carte processeur de gestion (MPC) est un composant essentiel du PA-5450, fournissant des fonctions de gestion, de journalisation et High Availability (haute disponibilité - HA). La carte MPC a subi une défaillance en raison d'un problème avec son composant, le périphérique logique complexe programmable (CPLD). Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Expiration du certificat de gestion NGFW/Panorama (Alerte gratuite)	Cette alerte détecte l'expiration du certificat de gestion NGFW/Panorama. Classe : Santé Catégorie : certificate Ticket de support intégré dans l'appli : Non
Carte NPC : défaillance FE100 (Alerte gratuite)	Les cartes de traitement réseau (Network Processing Card, NPC) fournissent une connectivité réseau et sont essentielles au traitement du trafic réseau. Une carte NPC a rencontré un problème avec son composant FE100, entraînant sa défaillance. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Homologues désynchronisés – Configuration (Alerte gratuite)	Les configurations système sur les homologues à haute disponibilité ne correspondent pas. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non

Alerter	Description
Homologues désynchronisés – Contenu dynamique (Alerte gratuite)	Le contenu dynamique, tel que des antivirus ou des applications et des menaces, ne correspond pas aux homologues à haute disponibilité. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non
Homologues désynchronisés : sessions (Alerte gratuite)	Les sessions ne correspondent pas ou ne sont pas à jour entre les homologues à haute disponibilité. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non
Homologues désynchronisés – Logiciel (Alerte gratuite)	Les versions logicielles PAN-OS sur les homologues à haute disponibilité ne correspondent pas. Classe : Santé Catégorie : Haute disponibilité Ticket de support intégré dans l'appli : Non
Contenu dynamique obsolète (Alerte gratuite)	Le contenu dynamique installé sur le périphérique est obsolète, par comparaison au contenu disponible sur le serveur de mise à jour. Classe : Santé Catégorie : Contenu dynamique Ticket de support intégré dans l'appli : Non
Fin de vie de PAN-OS (Alerte gratuite)	Votre version actuelle de PAN-OS n'est plus prise en charge. Classe : Santé Catégorie : PanOS et abonnement Ticket de support intégré dans l'appli : Non
Vulnérabilité connue dans PAN-OS (Alerte gratuite)	Votre version actuelle de PAN-OS présente des vulnérabilités connues. Classe : Santé Catégorie : Contenu dynamique Ticket de support intégré dans l'appli : Non

Alerter	Description
Expiration du certificat racine et par défaut PAN-OS : scénario 1 (Alerte gratuite)	Le certificat racine et le certificat par défaut sur le pare-feu ont expiré. Classe : Santé Catégorie : certificate Ticket de support intégré dans l'appli : Non
Erreur PCI (Alerte gratuite)	Une interconnexion de composants périphériques (PCI) est responsable de la connexion du plan de gestion (MP) au plan de contrôle (CP). Une certaine erreur liée à ce composant indique une défaillance dans sa fonctionnalité. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Défaillance de surveillance des chemins : carte (Alerte gratuite)	Une défaillance de surveillance des chemins a été détectée sur une carte située dans les emplacements du pare-feu. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Défaillance de port (Alerte gratuite)	Une défaillance liée au port physique de gestion ou à l'un des ports physiques à haute disponibilité a été détectée. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non
Épuisement de la mémoire de processus – Configuration (Alerte gratuite)	Les processus du plan de gestion du périphérique épuisent la mémoire disponible de ce dernier. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Épuisement de la mémoire de processus – Serveur de périphérique (Alerte gratuite)	Les processus du plan de gestion du périphérique épuisent la mémoire disponible de ce dernier. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui

Alerter	Description
Épuisement de la mémoire de processus – Destinataire de journaux (Alerte gratuite)	Les processus du plan de gestion du périphérique épuisent la mémoire disponible de ce dernier. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Épuisement de la mémoire de processus – Serveur de gestion (Alerte gratuite)	Les processus du plan de gestion du périphérique épuisent la mémoire disponible de ce dernier. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Épuisement de la mémoire de processus – ID utilisateur (Alerte gratuite)	Les processus du plan de gestion du périphérique épuisent la mémoire disponible de ce dernier. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui
Panne d'alimentation électrique redondante (Alerte gratuite)	La redondance de l'alimentation n'est pas atteinte, soit parce que le bloc d'alimentation n'a pas été inséré, soit parce que l'alimentation a mal fonctionné, soit parce que la redondance complète n'a pas été réalisée. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Oui
Latence de transfert des journaux du service de journalisation Strata (Alerte gratuite)	La latence de transfert sur le service de journalisation Strata dépasse une valeur acceptable. Classe : Santé Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Transfert des journaux du service de journalisation Strata hors ligne (Alerte gratuite)	Le service de transfert des journaux du service de journalisation Strata n'est pas fonctionnel Classe : Santé Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non

Alerter	Description
Latence d'ingestion des journaux du service de journalisation Strata (Alerte gratuite)	La latence d'ingestion sur le service de journalisation Strata dépasse une valeur acceptable. Classe : Santé Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Ingestion des journaux du service de journalisation Strata hors ligne (Alerte gratuite)	Le service d'ingestion du service de journalisation Strata n'est pas fonctionnel. Classe : Santé Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Le stockage des journaux du service de journalisation Strata s'approche des limites (Alerte gratuite)	Les types de journaux approchent de la limite de stockage maximale configurée. Classe : Santé Catégorie : de journalisation Ticket de support intégré dans l'appli : Non
Problèmes thermiques (Alerte gratuite)	La température du périphérique n'est pas comprise dans la plage normale. Classe : Santé Catégorie : Matériel Ticket de support intégré dans l'appli : Non

Alertes de service

Le tableau suivant identifie les alertes qu'AIOps for NGFW peut déclencher en rapport avec les services qui lui sont liés.

Alerter	Description
Pare-feu déconnecté du Strata Logging Service (Alerte gratuite)	La connexion entre FW et le SLS est perdue depuis plus de 5 minutes. Catégorie : Connectivité SLS Ticket de support intégré dans l'appli : Non
Ingestion des journaux du service de journalisation Strata hors ligne (Alerte gratuite)	Le service d'ingestion du SLS n'est pas fonctionnel pendant plus de 5 minutes. Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Transfert des journaux du service de journalisation Strata hors ligne (Alerte gratuite)	Le service de transfert des journaux du SLS n'est pas fonctionnel pendant plus de 5 minutes. Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Latence d'ingestion des journaux du service de journalisation Strata (Alerte gratuite)	La latence d'ingestion du SLS dépasse 10 minutes au cours des 15 dernières minutes. Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Latence de transfert des journaux du service de journalisation Strata (Alerte gratuite)	La latence de transfert du SLS dépasse 10 minutes sur les 15 dernières minutes. Catégorie : Santé du service de journalisation Strata (SLS) Ticket de support intégré dans l'appli : Non
Le stockage des journaux du service de journalisation Strata s'approche des limites (Alerte gratuite)	Les types de journaux approchent de la limite de stockage maximale configurée. Catégorie : de journalisation Ticket de support intégré dans l'appli : Non

Alertes déclenchées par l'utilisation de l'apprentissage automatique

Le tableau suivant identifie les alertes qu'AIOps for NGFW peuvent déclencher en tirant parti de l'apprentissage automatique.

Alerter	Description
Utilisation défavorable des ressources de trafic chiffré (Alerte premium)	Les ressources de trafic chiffrées sont faibles. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non Type de détection : Anomalie
Utilisation défavorable des ressources (Alerte premium)	Le pare-feu présente des valeurs anormales de connexions par seconde (CPS), de débit ou de nombre de sessions. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non Type de détection : Anomalie
Approche des limites de configuration maximales (Alerte premium)	Les objets de pare-feu tels que les règles, les groupes et les profils de sécurité approchent des limites de périphérique. Classe : Santé Catégorie : Configurer les limites Ticket de support intégré dans l'appli : Non Type de détection : Anomalie
Activité de traitement élevée (Alerte gratuite)	Une ou plusieurs ressources informatiques sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Non
Latence accrue du trafic – Mémoire tampon de paquets (Alerte premium)	Les ressources de la mémoire tampon de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources

Alerter	Description
	Ticket de support intégré dans l'appli : Oui Type de détection : Anomalie
Latence accrue du trafic – Descripteur de paquets (Alerte premium)	Les ressources du descripteur de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Utilisation des ressources Ticket de support intégré dans l'appli : Oui Type de détection : Anomalie
Latence du trafic – Descripteurs de paquets (sur puce) (Alerte premium)	Les ressources (sur puce) du descripteur de paquets sont faibles sur le périphérique. Classe : Santé Catégorie : Saturation/DoS Ticket de support intégré dans l'appli : Non Type de détection : Anomalie
Approche de la capacité maximale : table ARP (Alerte premium)	L'analyse des prévisions de données montre que les entrées de la table ARP sont en passe d'atteindre bientôt la capacité maximale du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : groupes d'adresses (Alerte premium)	Le nombre d'objets de groupe d'adresses a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : objets d'adresse (Alerte premium)	Le nombre d'objets d'adresse a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non

Alerter	Description
Approche de la capacité maximale : processeur du plan de données (Alerte premium)	L'utilisation du processeur du plan de données (DP) a été constamment élevée au fil du temps et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : utilisation du décryptage (Alerte premium)	L'analyse des prévisions de données montre que les sessions de décryptage SSL sont en passe d'atteindre bientôt la capacité maximale du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : adresses FQDN (Alerte premium)	Le nombre d'objets d'adresse FQDN a été constamment élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : tunnels GlobalProtect (sans client) (Alerte premium)	Le nombre de tunnels VPN GlobalProtect sans client s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : homologues IKE (Alerte premium)	Le nombre d'homologues IKE a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : processeur du plan de gestion (Alerte premium)	L'utilisation du processeur du plan de gestion (MP) a été constamment élevée et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité

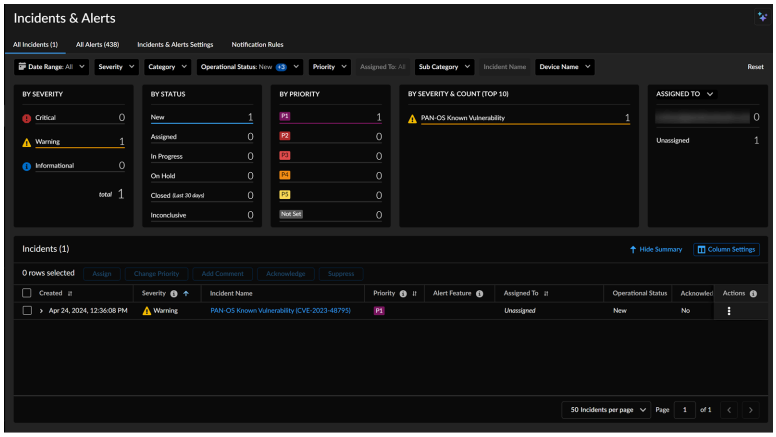
Alerter	Description
	Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : mémoire du plan de gestion (Alerte premium)	L'utilisation de la mémoire du plan de gestion (MP) a été constamment élevée et s'approche de la capacité maximale que le périphérique peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : politiques NAT (Alerte premium)	Le nombre de règles de politique NAT a été constamment élevé au fil du temps et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : politiques de sécurité (Alerte premium)	Le nombre de règles de politique de sécurité a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : groupes de services (Alerte premium)	Le nombre d'objets de groupe de services a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : objets de service (Alerte premium)	Le nombre d'objets de service a toujours été élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : utilisation de la table de session	L'utilisation de la table de session (%) a été constamment élevée au fil du temps et s'approche de la capacité maximale que le pare-feu ou la licence de VM peut prendre en charge. Classe : Santé

Alerter	Description
(Alerte premium)	Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : systèmes virtuels (Alerte premium)	L'analyse des prévisions de données montre que la configuration des systèmes virtuels est en passe d'atteindre la capacité maximale prise en charge par la licence du pare-feu. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Approche de la capacité maximale : tunnels VPN site à site (Alerte premium)	Le nombre de tunnels VPN site à site, comprenant à la fois des tunnels IPsec et des ID de proxy, a été constamment élevé et s'approche de la capacité maximale que le pare-feu peut prendre en charge. Classe : Santé Catégorie : Capacité Ticket de support intégré dans l'appli : Non
Alerte de performance de l'application NGFW SD-WAN (Alerte premium)	Indique la liste des applications affectées par des performances de liaison médiocres. Classe : Santé Catégorie : Performance SD-WAN Ticket de support intégré dans l'appli : Non Type de détection : Anomalie
Alerte de performance des liens NGFW SD-WAN (Alerte premium)	Indique ce qui entraîne une dégradation des performances de vos applications, services ou liaisons. Classe : Santé Catégorie : Performance SD-WAN Ticket de support intégré dans l'appli : Non Type de détection : Anomalie

Gérer les incidents NGFW

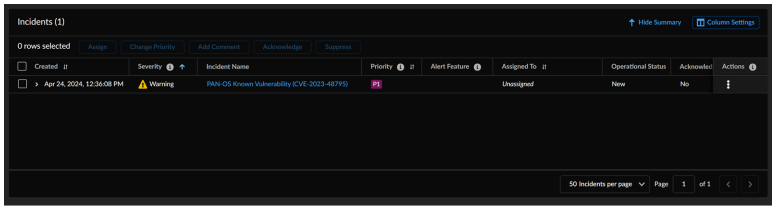
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Obtenez une vue d'ensemble des incidents NGFW en sélectionnant **Incidents & Alerts (Incidents et alertes)** > **NGFW** > **All Incidents (Tous les incidents)**. Explorez la page des incidents pour vous tenir informé des modifications apportées à votre déploiement afin de pouvoir les examiner et prendre des mesures préventives si nécessaire. Vous avez un accès direct à une liste détaillée des incidents ainsi qu'à des résumés visuels critiques. Vous pouvez également **masquer le résumé** pour masquer les widgets et n'afficher les incidents que sous forme de tableau.



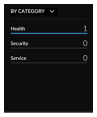
Voici les données présentées sous **All Incidents (Tous les incidents)**.

- **Incidents** : Affiche tous les incidents.



  Dans ce tableau, vous pouvez effectuer les tâches suivantes :

  - **Masquez le résumé** pour masquer les widgets et n'afficher les incidents que sous forme de tableau.
  - Développez un incident pour afficher sa description et son impact.
  - Sous Actions, vous pouvez effectuer les actions suivantes :
    - **Attribuez** un incident à un utilisateur, à vous-même ou à annulez l'attribution d'un incident.
    - **Modifiez la priorité** d'un incident ou sélectionnez Not Set (Non défini) pour supprimer la priorité.
    - **Accusez réception** d'un incident en sélectionnant **Yes (Oui)**, ce qui confirme que vous avez vu l'incident.
    - **Suppress (Supprimer)** définit un incident sur un état opérationnel « On Hold » (« En attente ») lorsque vous ne prévoyez pas de le résoudre activement.
    - **Ajoutez un commentaire** pour un incident.
  - Cliquez sur un incident pour afficher ses détails.
  - Utilisez l'option **Column Settings (Paramètres de colonne)** pour afficher ou masquer des colonnes spécifiques pour des incidents et réorganiser l'ordre par défaut des colonnes. Ces modifications seront conservées lors des sessions futures.
- **ASSIGNED TO (ATTRIBUÉ À)** : Affiche le nombre d'incidents par la personne ou l'entité chargée de les résoudre. En haut, l'écran affiche les incidents attribués à l'utilisateur actuellement connecté et les incidents non attribués. Vous pouvez également consulter le nombre d'incidents **PAR CATÉGORIE** en le sélectionnant dans la liste déroulante.



- **BY SEVERITY & COUNT (TOP 10) (PAR GRAVITÉ ET NOMBRE (TOP 10)) :** Affiche les incidents classés par gravité, ainsi que le nombre d'incidents dans chaque catégorie. Les incidents critiques sont d'abord classés par ordre de priorité, suivis des incidents d'avertissement, puis des incidents informationnels.

- **BY STATUS (PAR ÉTAT) :** Affiche le nombre total d'incidents par état.
  - New (Nouveau) indique les incidents dont l'attribution a été annulée.
  - Assigned (Attribué) indique les incidents qui ont été attribués à un utilisateur.
  - In Progress (En cours) indique que l'incident fait l'objet d'un traitement.
  - On Hold (En attente) indique que vous ne prévoyez pas de résoudre activement un incident.
  - Closed (Clôturé) indique les incidents clôturés au cours des 30 derniers jours.
  - Inconclusive (Non concluant) indique qu'il n'y a pas de solution à ces incidents.

- **BY SEVERITY (PAR GRAVITÉ) :** Affiche le nombre total d'incidents classés comme critiques, avertissements et informations.

- **BY PRIORITY (PAR PRIORITÉ) :** Affiche les incidents en fonction de leur priorité, le niveau P1 étant le plus grave.

Voir les détails de l’incident

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les Crédits NGFW logiciels	Un des éléments suivants : ❑ ou ❑ ou

Dans **All Incidents (Tous les incidents)**, vous pouvez sélectionner un incident pour ouvrir une page contenant des détails à son sujet. L’onglet **Summary (Résumé)** affiche les détails suivants :

1. Résumé de l’incident avec des détails. Vous pouvez modifier la priorité de l’incident ou l’attribuer à un utilisateur.
2. Impact causé par l’incident, c’est-à-dire le nombre de NGFW touchés.
3. Mesures recommandées pour résoudre votre problème.

Vous pouvez également cliquer sur le CVE pour afficher ses détails dans les Avis de sécurité Palo Alto Networks et les vulnérabilités dans la version PAN-OS.

L’onglet **Correlated Alerts & Activity (Alertes et activités corrélées)** affiche les détails suivants :

- Les alertes corrélées pour l’incident sélectionné
- Activité enregistrée pour l’incident