paloalto
TECHDOCS

Vorfälle und Benachrichtigungen

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

Benachrichtigungen

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Damit Sie den laufenden Zustand Ihrer Geräte aufrechterhalten und Vorfälle, die den Geschäftsbetrieb stören, vermeiden können, generiert AIOps for NGFW Benachrichtigungen basierend auf einem oder mehreren Problemen, die bei Ihrer Firewallbereitstellung festgestellt wurden. Diese Probleme, oder *Ereignisse*, werden auf eine von drei Arten ausgelöst:

- Wenn sich eine Metrik signifikant ändert
- Wenn sich ein zuvor generiertes Ereignis ändert
- Wenn der Benutzer oder das System eine Aktion ausführt, z. B. eine Benachrichtigung bestätigt oder schließt

Eine Benachrichtigung weist auf ein bestimmtes Problem hin (Verschlechterung oder Ausfall der Firewall-Funktionalität), das behoben werden muss. Benachrichtigungen können auch auf der Grundlage von Korrelation oder Aggregation mehrerer Ereignisse generiert werden. Diese Aggregation von Ereignissen zu einer einzigen Benachrichtigung hilft bei der Triage, beim Optimieren der Benachrichtigungsweiterleitung zwischen Teams, bei der Zentralisierung kritischer Informationen und sorgt für eine Verringerung der Benachrichtigungsmüdigkeit.

Benachrichtigungen fallen in verschiedene Kategorien, je nachdem, welcher Metrik sie zugeordnet sind. Sie können Benachrichtigungskategorien verwenden, um festzulegen, zu welchen Ereignissen Sie Benachrichtigungen erhalten möchten. Beispielsweise zu Hardware, Konfigurationslimits, Ressourcenlimits, dynamischen Inhalten und PAN-OS und Abonnements.

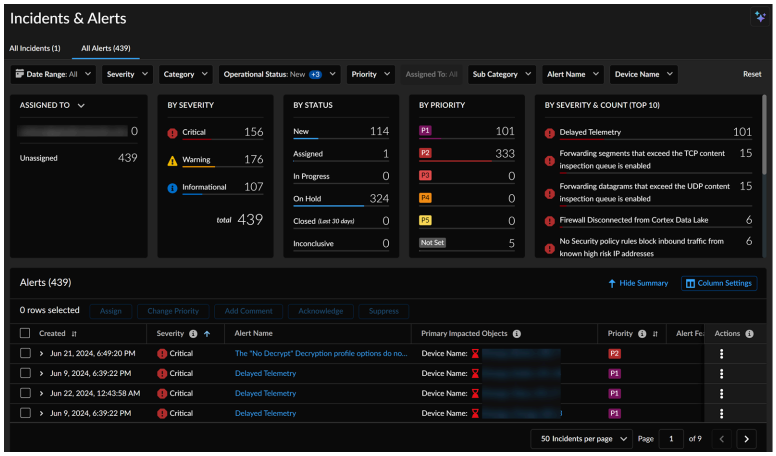
Über **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Alarme** können Sie alle für Ihre Bereitstellung generierten Benachrichtigungen anzeigen und verwalten. Unter **Benachrichtigungsregeln** können Sie Benachrichtigungsregeln konfigurieren, die festlegen, wann und wie Sie benachrichtigt werden möchten, wenn Ereignisse eine Benachrichtigung auslösen.

- Verwalten von NGFW-Benachrichtigungen
- Anzeigen von Benachrichtigungsdetails
- Anzeigen möglicher Ursachen
- Prognosen und Anomalieerkennung
- Verwalten von Kapazitätsanalysebenachrichtigungen
- CPU-Auslastungsmetriken in AIOps für NGFW
- Erstellen einer Benachrichtigungsregel
- Integration in ServiceNow

Verwalten von NGFW-Benachrichtigungen

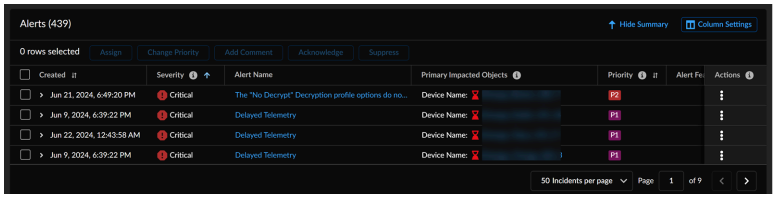
Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Erhalten Sie einen Überblick über die NGFW-Benachrichtigungen, indem Sie **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Alarme** auswählen. Sehen Sie sich die Seite mit den Benachrichtigungen an, um die kontinuierliche Integrität Ihrer Geräte und Bereitstellungen aufrechtzuerhalten und Störungen Ihres Geschäftsbetriebs zu vermeiden. Sie haben direkten Zugriff auf eine detaillierte Liste mit Benachrichtigungen und auf wichtige visuelle Zusammenfassungen. Sie können die **Zusammenfassung ausblenden**, um die Widgets auszublenden und nur die Benachrichtigungen in tabellarischer Form anzuzeigen.



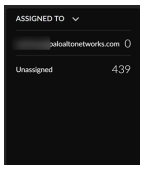
Unter **Alle Alarme** werden die folgenden Daten angezeigt.

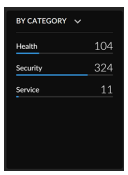
- **Benachrichtigungen**: Es werden alle Benachrichtigungen angezeigt.



  In dieser Tabelle können Sie die folgenden Aufgaben ausführen:

  - **Zusammenfassung ausblenden**, um die Widgets auszublenden und nur die Benachrichtigungen in tabellarischer Form anzuzeigen.
  - Erweitern Sie eine Benachrichtigung, um ihre Beschreibung und Auswirkung anzuzeigen.
  - Unter „Aktionen“ können Sie die folgenden Aktionen ausführen:
    - Sie können einem Benutzer oder sich selbst eine Benachrichtigung **zuweisen** oder die Zuweisung einer Benachrichtigung aufheben.
    - Mit **Priorität ändern** können Sie die Priorität einer Benachrichtigung ändern. Oder wählen Sie „Nicht gesetzt“ aus, um die Priorität zu entfernen.
    - Sie können eine Benachrichtigung **anerkennen**, indem Sie **Ja** auswählen. Damit wird bestätigt, dass Sie sie gesehen haben.
    - Mit **Unterdrücken** können Sie einer Benachrichtigung den Betriebsstatus „In der Warteschleife“ zuweisen, wenn Sie nicht vorhaben, sie aktiv aufzulösen.
    - Hier können Sie für eine Benachrichtigung einen **Kommentar hinzufügen**.
  - Klicken Sie auf eine Benachrichtigung, um deren Details anzuzeigen.
  - Verwenden Sie die **Spalteneinstellungen**, um bestimmte Spalten für Benachrichtigungen ein- oder auszublenden und die Standardreihenfolge der Spalten neu anzuordnen. Diese Änderungen bleiben in zukünftigen Sitzungen beibehalten.
- **ZUGEWIESEN ZU**: Zeigt die Anzahl der Benachrichtigungen nach der Person oder Entität an, die für deren Auflösung zuständig ist. Ganz oben werden die dem aktuell angemeldeten Benutzer zugewiesenen Benachrichtigungen sowie die nicht zugewiesenen Benachrichtigungen angezeigt. Sie können die Anzahl der Benachrichtigungen auch **NACH KATEGORIE** anzeigen, indem Sie diese Option in der Dropdown-Liste auswählen.

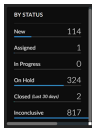




- **NACH SCHWEREGRAD UND ANZAHL (TOP 10):** Zeigt die nach Schweregrad kategorisierten Benachrichtigungen zusammen mit der Anzahl der Benachrichtigungen in jeder Kategorie

an. Kritische Benachrichtigungen erhalten oberste Priorität, gefolgt von Warnhinweisen und schließlich informativen Benachrichtigungen.

- **NACH STATUS:** Zeigt die Gesamtzahl der Benachrichtigungen nach Status an.
  - „Neu“ gibt an, wie viele Vorfälle nicht zugewiesen wurden.
  - „Zugewiesen“ gibt an, wie viele Vorfälle einem Benutzer zugewiesen wurden.
  - „In Bearbeitung“ gibt an, an wie vielen Vorfällen gearbeitet wird.
  - „In der Warteschleife“ gibt an, dass Sie nicht vorhaben, eine Benachrichtigung oder einen Vorfall aktiv aufzulösen.
  - „Geschlossen“ gibt die Anzahl der Benachrichtigungen an, die in den letzten 30 Tage geschlossen wurden.
  - „Uneindeutig“ gibt an, dass es für diese Benachrichtigungen keine Lösung gibt.



- **NACH SCHWERGRAD:** Zeigt die Gesamtzahl der Benachrichtigungen an, denen die Kategorie „Kritisch“, „Warnung“ und „Information“ zugewiesen wurde.

- **NACH PRIORITÄT:** Zeigt die Benachrichtigungen entsprechend ihrer Priorität an, wobei P1 den Benachrichtigungen mit der höchsten Priorität entspricht.

Anzeigen von Benachrichtigungsdetails

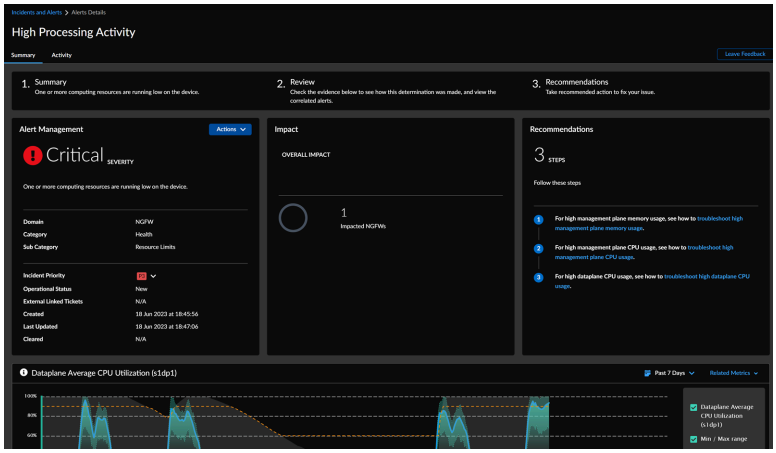
Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Unter **Alle Alarme** können Sie eine Benachrichtigung auswählen, um eine Seite mit Details zu dieser Benachrichtigung zu öffnen. Auf der Registerkarte **Zusammenfassung** werden die folgenden Details angezeigt:

1. Zusammenfassung der Benachrichtigung mit Details. Sie können die Priorität der Benachrichtigung ändern oder die Benachrichtigung einem Benutzer zuweisen.
2. Auswirkung der Benachrichtigung, d. h. die Anzahl der betroffenen NGFW.
3. Empfohlene Korrekturmaßnahmen und Ressourcen zur Behebung Ihres Problems.

Sie können auch die Diagramme der beitragenden Ereignisse überprüfen.

Auf der Registerkarte **Aktivität** wird die aufgezeichnete Aktivität für die Benachrichtigung angezeigt.



Anzeigen möglicher Ursachen

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ oder

Mithilfe erweiterter KI-Funktionen zeigt AIOps für NGFW die wahrscheinlichen Ursachen für Benachrichtigungen an und bietet Empfehlungen zur Behebung des zugrunde liegenden Problems. Diese Funktion gewährleistet eine optimale Netzwerkleistung, indem sie Störungen verringert und die Effektivität Ihrer Cybersicherheitslösung maximiert.

Im Folgenden sind die Benachrichtigungen aufgeführt, die die Analyse der möglichen Ursache unterstützen:

- Hohe Verarbeitungsaktivität
- Erhöhte Datenverkehrslatenz – Paketpuffer
- Erhöhte Datenverkehrslatenz – Paketdeskriptor (On-Chip)
- Zulässige Bedrohungen
- Datenverkehrslatenz – Paketdeskriptoren (On-Chip)
- Unerwünschte Nutzung von Ressourcen
- Nicht synchrone Peers – Konfiguration
- Möglicher Missbrauch durch Diebstahl von Anmeldeinformationen
- Commit und Push fehlgeschlagen

Die Analyse der möglichen Ursache wird um die Strata Logging Service-Protokolle erweitert und stellt zusätzliche Metadaten zur möglichen Ursache bereit, die zum Erstellen der Benachrichtigung oder des Vorfalls geführt hat. Mit dieser Erweiterung können Sie die Richtlinien, Anwendungen, Quellzonen, URLs, Quell-IPs und Regionen genau bestimmen, die möglicherweise zum Auslösen der Benachrichtigung führen.

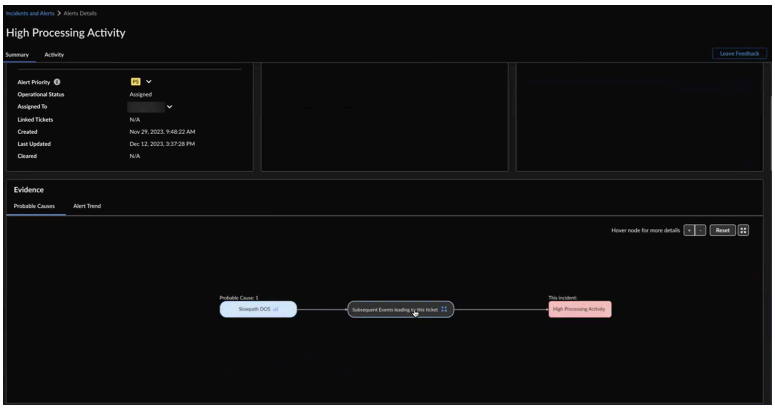
Sie können die möglichen Ursachen für die folgenden Szenarien anzeigen:

- **Hohe Verarbeitungsaktivität** (Benachrichtigung „Hohe Verarbeitungsaktivität“): Eine hohe CPU-Auslastung auf Datenebene kann zu verschiedenen Problemen führen, beispielsweise zu Instabilitäten in Firewalls, zum Blockieren von Firewalls sowie zu Paketverlusten oder Latenzproblemen. Dies kann sich negativ auf Ihren Geschäftsbetrieb auswirken. Wenn die CPU-Auslastung auf Datenebene mindestens 60 % beträgt und es zu einer erheblichen Auslastungsspitze kommt, zeigt AIOps für NGFW wahrscheinliche Ursachen in der Benachrichtigung „Hohe Verarbeitungsaktivität“ an. Bleibt die CPU-Auslastung auf Datenebene jedoch über einen langen Zeitraum ohne Schwankungen konstant auf einem hohen Niveau, ist die Ursache nicht eindeutig und kann nicht auf einfache Weise ermittelt werden. Daher werden keine möglichen Ursachen angezeigt. Wenn beispielsweise die CPU-Auslastung der Datenebene über einen längeren Zeitraum konstant 70 % beträgt, zeigt AIOps für NGFW keine möglichen Ursachen an.

- **Erkennung und Korrektur einzelner oder mehrerer Greedy-Sitzungen** (Benachrichtigung „Hohe Verarbeitungsaktivität“): Bei einem Angriff durch Greedy-Sitzungen auf eine Firewall stellt ein Angreifer in schneller Folge zahlreiche Verbindungen her und nutzt dabei die internen Ressourcen der Firewall aus. Dies kann zur Erschöpfung der Ressourcen und zu Denial-of-Service-(DoS-)Vorfällen führen. AIOps für NGFW kann diese Probleme erkennen und wahrscheinliche Ursachen dafür anzeigen.
- **Sitzungserschöpfung mit Verbindungsverlust** (Benachrichtigung „Hohe Verarbeitungsaktivität“): Wenn eine Firewall Datenverkehr empfängt, richtet sie für diesen Datenverkehr eine Sitzung ein, um seinen Status zu verfolgen und erforderliche Sicherheitsüberprüfungen durchzuführen. Jede Sitzung verbraucht Systemressourcen, einschließlich Arbeitsspeicher und CPU-Zyklen. Wenn die Firewall ihre maximale Kapazität für gleichzeitige Sitzungen erreicht, führt dies zur Sitzungserschöpfung. Dieses Problem kann mehrere Ursachen haben, z. B. ein hohes Datenverkehrsaufkommen, falsch konfigurierte Sicherheitsrichtlinien und falsche Einstellungen für das Sitzungs-Timeout. AIOps für NGFW nutzt erweiterte KI-Funktionen, um Probleme mit Sitzungserschöpfung in Netzwerkgeräten proaktiv zu erkennen. Dies ermöglicht eine optimierte Ressourcenzuweisung, steigert die Netzwerkleistung und mindert Verbindungsprobleme, um eine unterbrechungsfreie Verfügbarkeit des Dienstes zu gewährleisten.
- **Hohe Paketpufferauslastung aufgrund einer einzelnen Anwendung** (erhöhte Datenverkehrslatenz – Paketpuffer): AIOps für NGFW erkennt die wahrscheinliche Ursache einer hohen Paketpufferauslastung, die darauf zurückzuführen ist, dass eine einzelne Anwendung den Paketpuffer monopolisiert. AIOps für NGFW nutzt erweiterte KI-Funktionen, um eine optimale Netzwerkleistung sicherzustellen, indem rechtzeitig auf eine suboptimale Ressourcenzuweisung hingewiesen wird und Leistungseinbußen verhindert werden.
- **Hohe Auslastung des On-Chip-Paketdeskriptors aufgrund einer einzelnen Anwendung** (erhöhte Datenverkehrslatenz – On-Chip-Paketdeskriptor): AIOps für NGFW erkennt die mögliche Grundursache einer hohen Auslastung des On-Chip-Paketdeskriptors. Dies unterstützt die proaktive Identifizierung und Lösung von Netzwerküberlastungen, die durch eine einzelne Anwendung verursacht werden, die den On-Chip-Paketdeskriptor monopolisiert.
- **Erkennung von Slow-Path-DoS-Angriffen und Vorschläge zu Korrekturmaßnahmen** (Benachrichtigung „Hohe Verarbeitungsaktivität“): AIOps für NGFW erkennt Slow-Path-DoS-Angriffe mit KI-gestützter Technologie und gewährleistet so Netzwerksicherheit und eine unterbrechungsfreie Verfügbarkeit des Dienstes. Es werden Benachrichtigungen zu hoher Verarbeitungsaktivität auf Datenebene ausgelöst, eine Ursachenanalyse bei hoher Richtlinienverweigerungs-Aktivität durchgeführt und Korrekturmaßnahmen basierend auf der Kausalitätsanalyse vorgeschlagen.
- **Erkennung und Korrektur einer hohen Suchaktivität im URL-Cache** (Benachrichtigung „Hohe Verarbeitungsaktivität“): AIOps für NGFW erkennt und behebt eine hohe Suchaktivität im URL-Cache, optimiert die Verarbeitungseffizienz und erhält die Systemstabilität aufrecht. Diese Funktion korreliert die Suchaktivität im URL-Cache mit der DP-CPU-Auslastung, identifiziert eine hohe CPU-Auslastung und schlägt Korrekturmaßnahmen vor, um Szenarien mit nahezu vollständiger Sättigung zu verhindern.
- **Erkennung und Korrektur hoher Inhaltsverarbeitungsaktivität** (Benachrichtigung „Hohe Verarbeitungsaktivität“): AIOps für NGFW-Funktion erkennt eine hohe Inhaltsverarbeitungsaktivität. Diese Funktion analysiert Korrelationen zwischen verschiedenen Phasen der Inhaltsverarbeitung und der CPU-Auslastung auf Datenebene, identifiziert Fälle hoher CPU-Auslastung oder Zustände nahezu vollständiger Sättigung und schlägt umsetzbare Korrekturmaßnahmen zur Verbesserung der Systemstabilität vor.

- **RCA-Bericht über zu langes Zertifikat** (Benachrichtigung „Commit und Push fehlgeschlagen“): AIOps für NGFW erkennt Commit-Fehler und beschreibt die möglichen Ursachen von Commit-Fehlern, insbesondere wenn die Länge des Zertifikats die Puffergröße überschreitet.

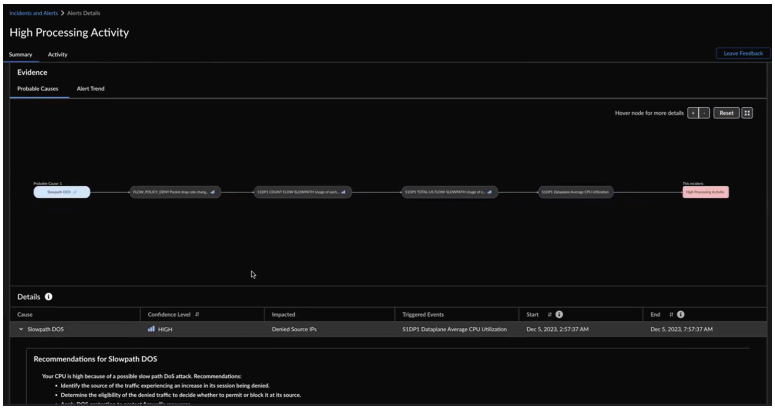
STEP 1 | Wählen Sie unter **Vorfälle und Benachrichtigungen** > **Benachrichtigungen** eine Benachrichtigung aus, um eine Seite mit Details zur Benachrichtigung zu öffnen.



Das Flussdiagramm weist auf Folgendes hin:

- Ereignisse, die zum Auslösen der Benachrichtigung „Hohe Verarbeitungsaktivität“ geführt haben
- Mögliche Ursache des ausgelösten Ereignisses

Sie können den Cursor auch über die Knoten bewegen, um weitere Details anzuzeigen, beispielsweise die mögliche Ursache, das Konfidenzniveau, das ausgelöste Ereignis und die Dauer der Auswirkung. Wenn drei oder mehr Ereignisknoten vorhanden sind, können Sie auf die Ereignisse klicken und sie erweitern, um die Details anzuzeigen.



AIOps für NGFW zeigt dieselben Informationen auch in tabellarischer Form an. Sie können den Cursor über eine mögliche Ursache in der Tabelle bewegen, um die hervorgehobenen Knoten und den Pfad im Flussdiagramm anzuzeigen. Sie können im Flussdiagramm auch auf eine mögliche Ursache klicken, um deren Details in tabellarischer Form anzuzeigen.

Das **Konfidenzniveau** gibt an, wie sicher AIOps für NGFW die Ursachen für die Benachrichtigung „Hohe Verarbeitungsaktivität“ bestimmt. Die wahrscheinlichen Ursachen werden nach Konfidenzniveau in absteigender Reihenfolge sortiert. Beginnen Sie mit dem Überprüfen der Ursachen, die ein hohes Konfidenzniveau aufweisen.

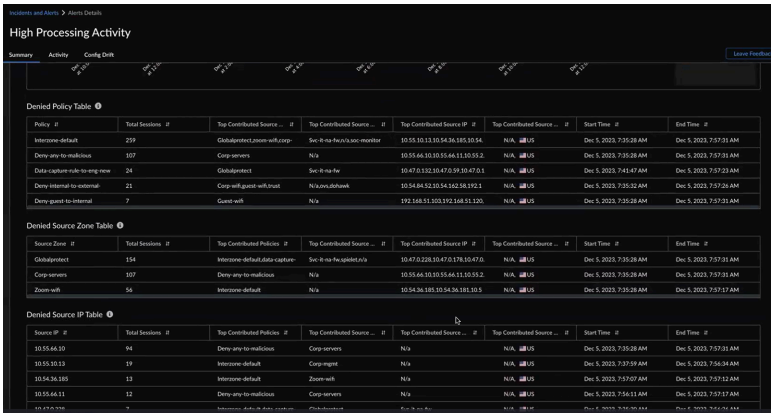
STEP 2 | Erweitern Sie eine mögliche Ursache in der Tabelle, um Diagramme und betroffene Metriken anzuzeigen, die Sie näher untersuchen möchten, da sie zum Auslösen der Benachrichtigung geführt haben.

STEP 3 | Verwenden Sie Diagrammtools, um die Grafiken zu überprüfen.

Mithilfe des Kausalitätszeitraums können Sie die Ursache-Wirkungs-Beziehung zwischen der **Ursache** der Benachrichtigung und dem **ausgelösten Ereignis** im Zeitverlauf visualisieren.

Sie können im Diagramm Zeiträume von 6 Stunden, 24 Stunden oder 48 Stunden vor und nach der Auswirkung anzeigen.

Die Analyse der möglichen Ursache wird erweitert, um die SLS-Protokolle zu verwenden und zusätzliche Metadaten zur möglichen Ursache bereitzustellen, die zum Erstellen einer Benachrichtigung oder eines Vorfalls geführt hat. Mit dieser Erweiterung können Sie die Richtlinien, Anwendungen, Quellzonen, URLs, Quell-IPs und Regionen genau bestimmen, die möglicherweise zum Auslösen der Benachrichtigung führen. Wenn beispielsweise die hohe CPU-Auslastung auf Datenebene die Benachrichtigung **Hohe Verarbeitungsaktivität** auslöst, können Sie die Analyse der möglichen Ursache nutzen, um die Hauptverursacher der Benachrichtigung zu ermitteln, und die empfohlenen Korrekturmaßnahmen befolgen.



Prognosen und Anomalieerkennung

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Normalerweise erkennt AIOps for NGFW Probleme, indem feste Regeln auf die Metriken in Ihrer Bereitstellung angewendet werden. Wenn beispielsweise die CPU-Auslastung der Verwaltungsebene 85 % überschreitet, wechselt die Metrik in den Zustand „Kritisch“.

Um Sie jedoch auf Ereignisse aufmerksam zu machen, die bei festen Regeln möglicherweise übersehen werden, kann AIOps for NGFW maschinelles Lernen verwenden, um Ihre Bereitstellung zu verstehen und Ihnen zusätzliche Benachrichtigungen und Vorfälle zur Verfügung zu stellen, die auf Ihre Nutzungstrends zugeschnitten sind.

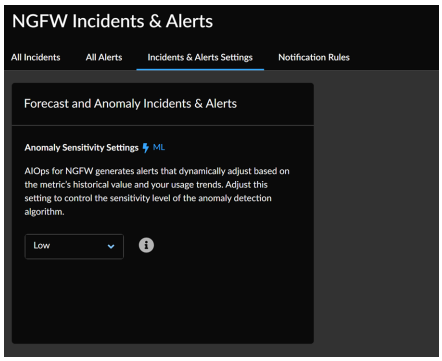
- **Prognosebasierte Benachrichtigungen** helfen Ihnen, Probleme vorauszusehen, indem prognostiziert wird, wie sich eine Gerätemetrik verändern könnte, und Sie entsprechend informiert werden.
- **Anomaliebasierte Benachrichtigungen** legen ein grundlegendes Verhalten für eine Gerätemetrik fest und informieren Sie, wenn diese Metrik die von Ihnen angegebenen **Einstellungen der Anomalieempfindlichkeit** überschreitet.

Prognose- und anomaliebasierte Erkennung bietet folgende Vorteile:

- Proaktive Verwaltung: Durch die Vorhersage potenzieller Probleme und die frühzeitige Erkennung von Anomalien können Administratoren proaktive Maßnahmen ergreifen, um Problemen vorzubeugen, Ausfallzeiten zu reduzieren und die allgemeine Netzwerkleistung zu verbessern.
- Verbesserte Sicherheit: Durch das Erkennen ungewöhnlicher Muster und Verhaltensweisen können Sicherheitsbedrohungen und Schwachstellen identifiziert werden, sodass frühzeitig eingegriffen und Abhilfe geschaffen werden kann.
- Optimierte Ressourcen: Prognosen helfen bei der besseren Planung und Zuweisung von Ressourcen und stellen sicher, dass die Netzwerkinfrastruktur ausreichend auf die Bewältigung zukünftiger Anforderungen vorbereitet ist.

Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **Vorfall- und Benachrichtigungseinstellungen** > **Prognose- und Anomalievorfälle und Benachrichtigungen**.

AIOps for NGFW generiert Benachrichtigungen und Vorfälle, die basierend auf dem historischen Wert der Metrik und Ihren Nutzungstrends dynamisch angepasst werden. Abweichungen vom Normalitätsband können auf potenzielle Probleme hinweisen. Sie können diese Einstellung anpassen, um die Empfindlichkeit des Anomalieerkennungsalgorithmus zu steuern.



Verwalten von Kapazitätsanalysebenachrichtigungen

Wo kann ich das verwenden?	Was brauche ich?
•	❑ oder

Kapazitätsanalyse verwendet Modelle maschinellen Lernens, um vorherzusehen, wann sich der Ressourcenverbrauch der maximalen Kapazität nähert und Benachrichtigungen auslöst. Die Kapazitätsanalysebenachrichtigungen werden im Voraus generiert und weisen auf potenzielle Kapazitätsengpässe hin.

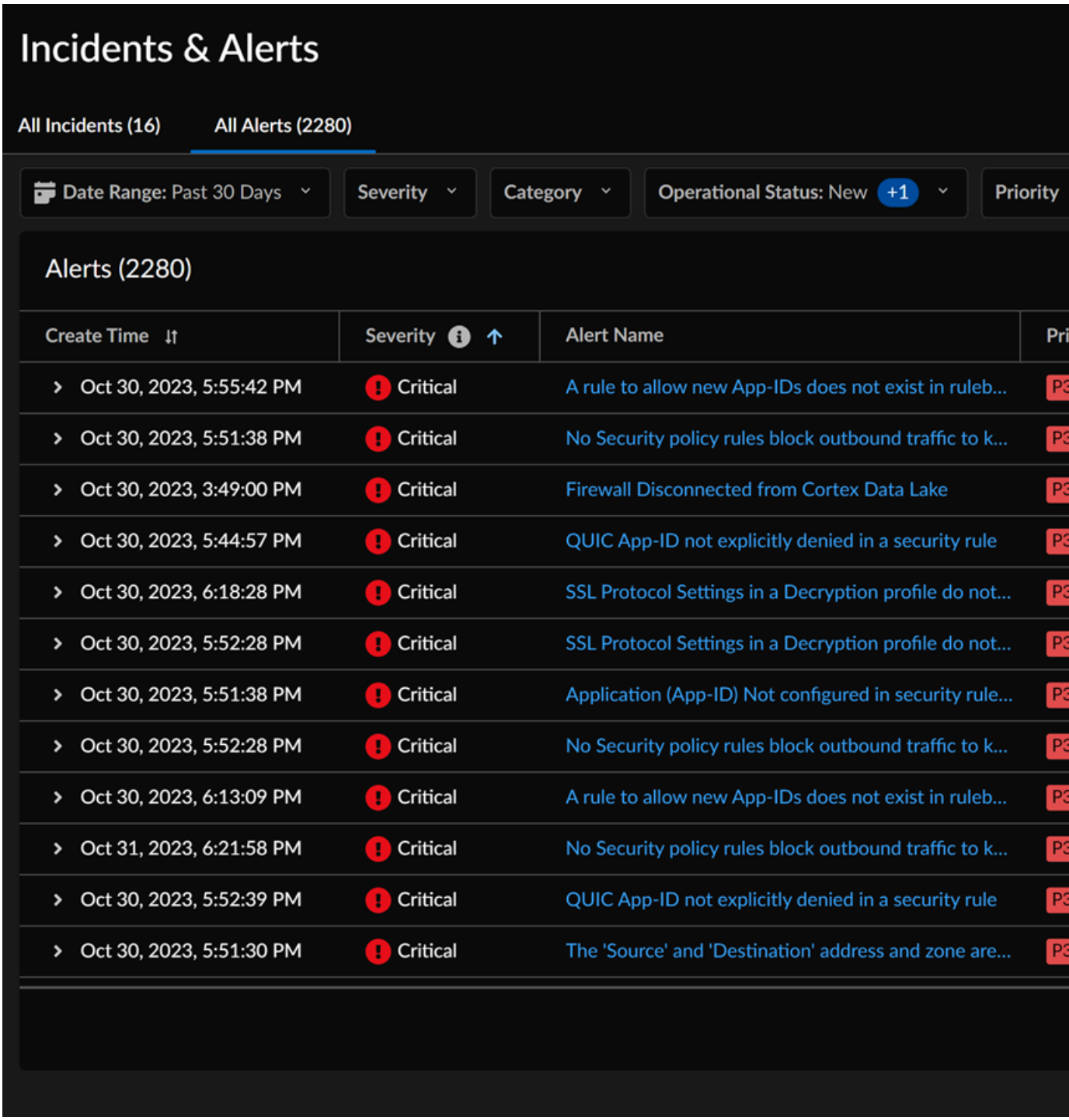
Sie können auch eine Benachrichtigungsregel erstellen, um Kapazitätsanalysebenachrichtigungen auszulösen.

STEP 1 | Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Alarme** und klicken Sie auf **Listenansicht**.

STEP 2 | Suchen Sie unter **Benachrichtigungsname** nach Benachrichtigungen, die sich auf die **Annäherung an Maximalwerte** beziehen.

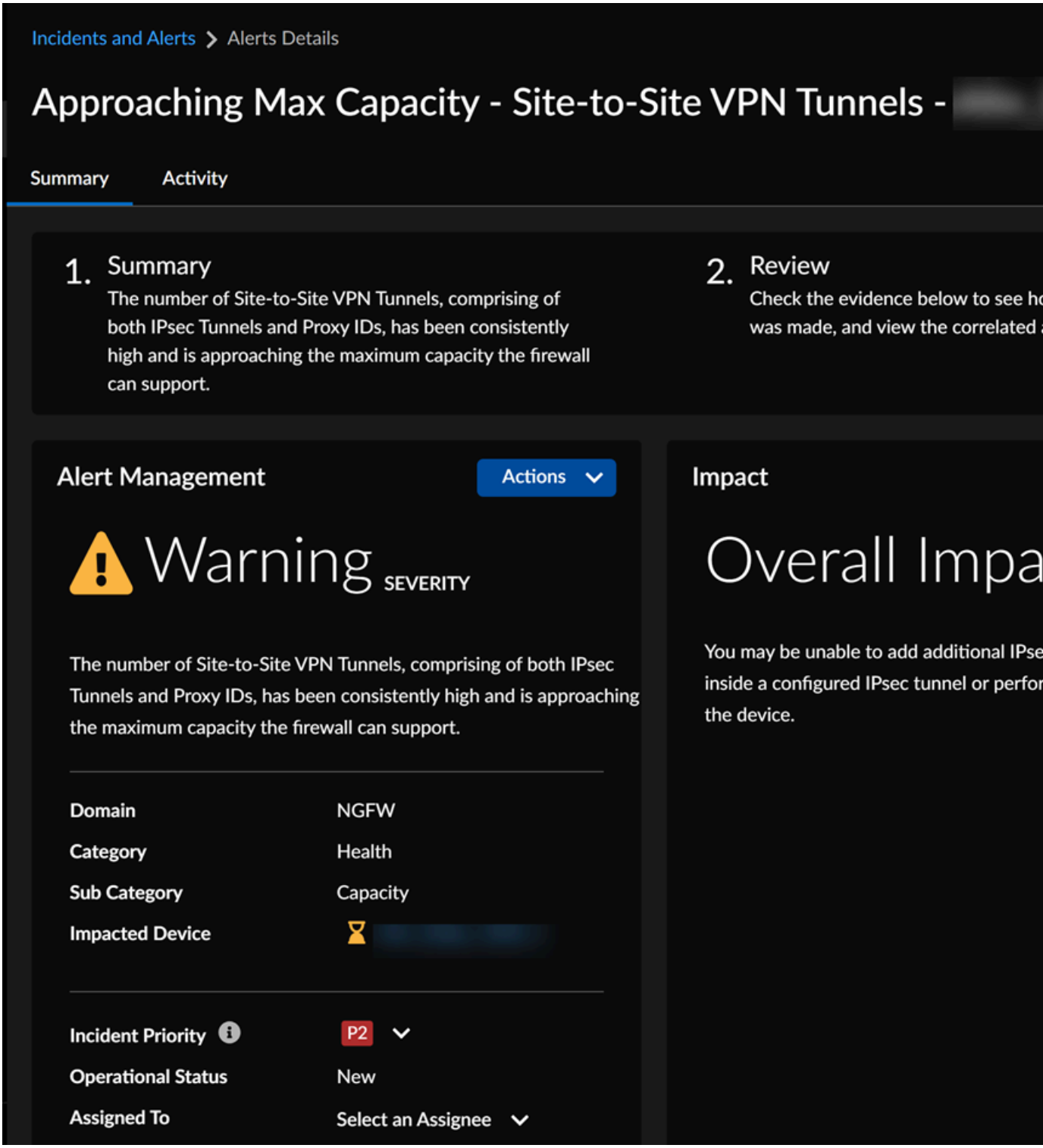
Die für die Kapazitätsanalysefunktion ausgelösten Benachrichtigungen sind wie folgt benannt:

Annäherung an maximale Kapazität – *<Metric-Name>*.



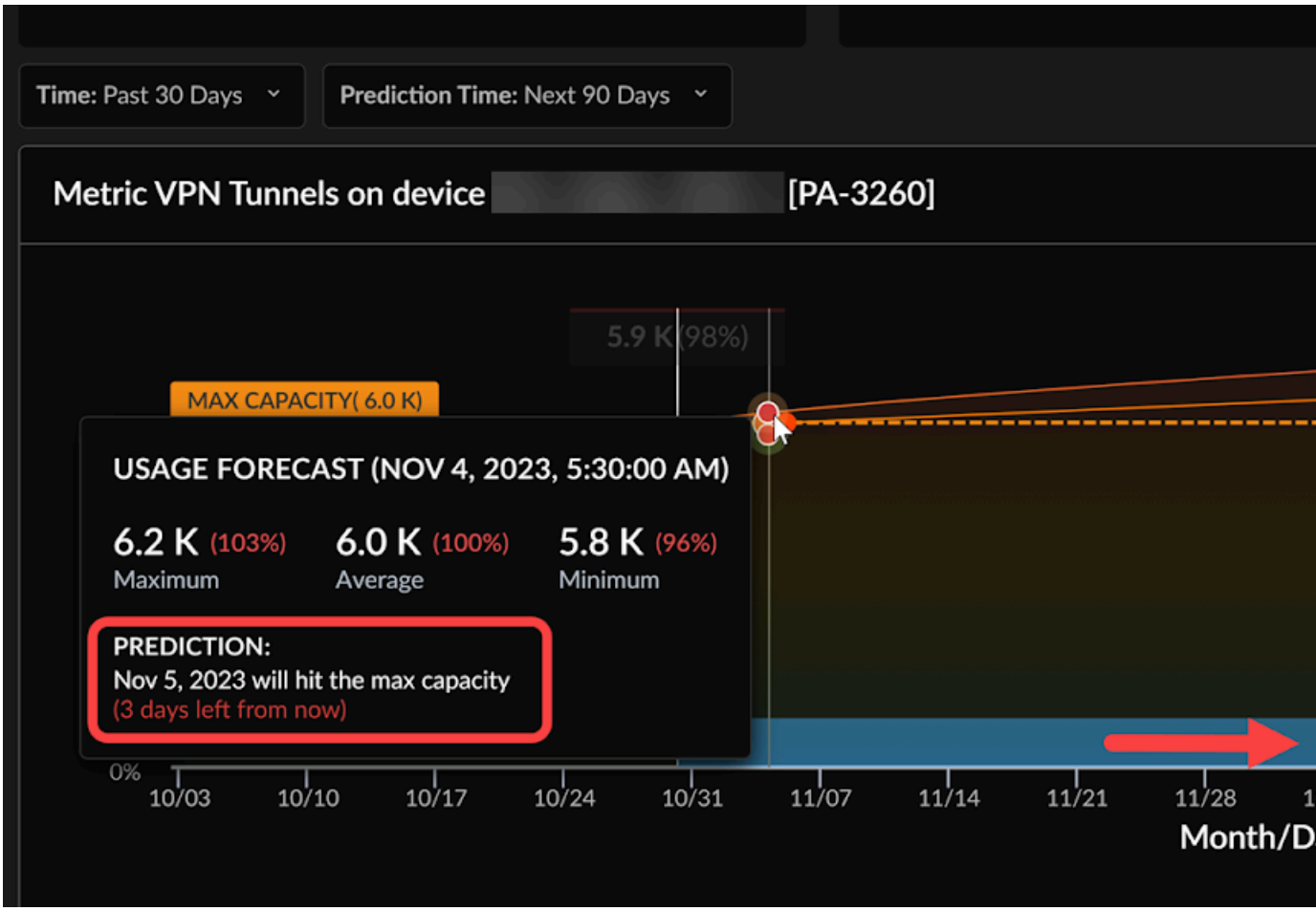
STEP 3 | Wählen Sie eine der Benachrichtigungen aus, um ihre Details anzuzeigen, darunter:

- Zusammenfassung der Benachrichtigung mit Details.
- Durch die Benachrichtigung verursachte Auswirkungen.
- Empfohlene Maßnahmen zur Behebung des Problems.

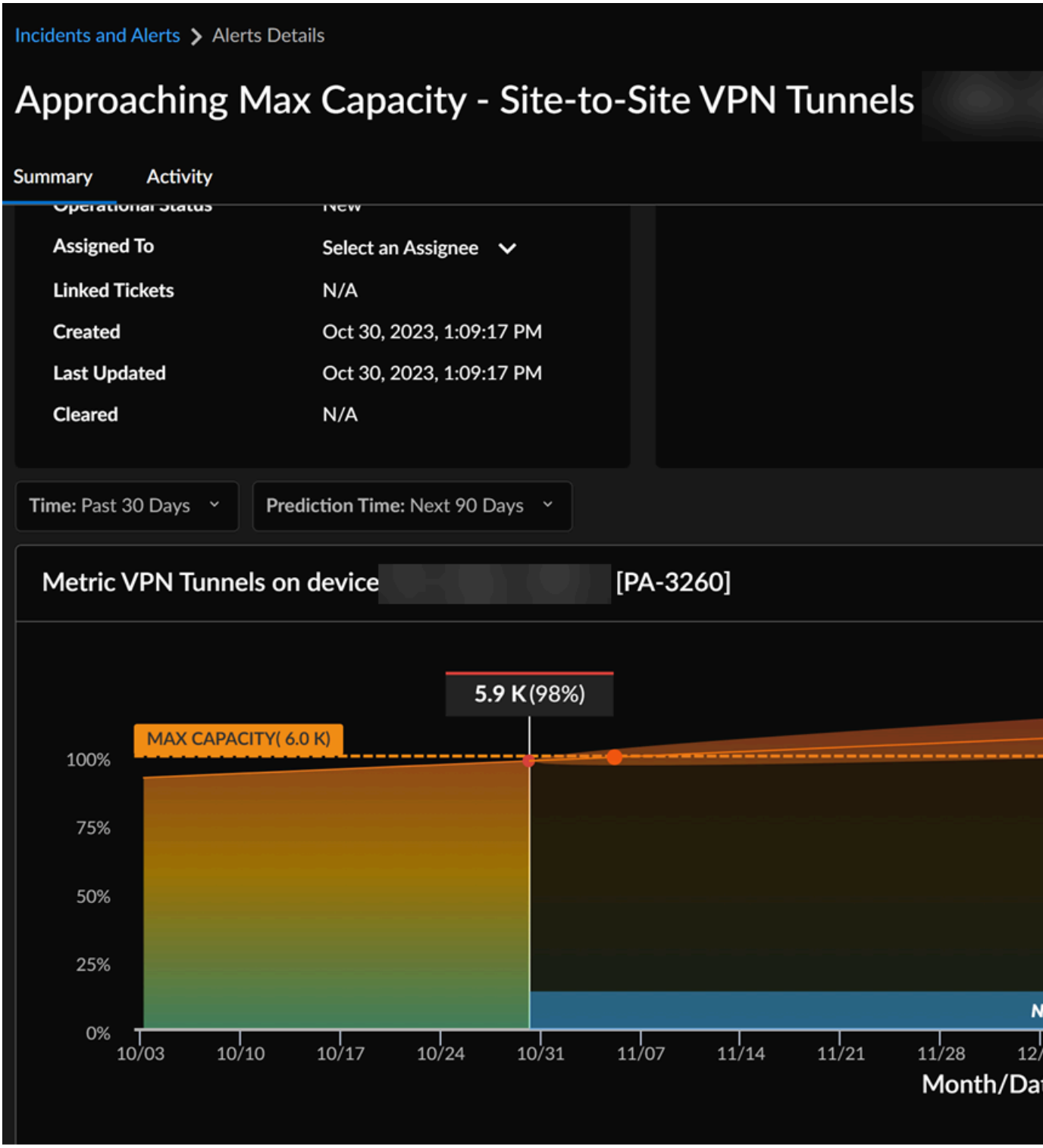


In den Benachrichtigungsdetails können Sie auch ein Diagramm anzeigen, das den Trend für die Metrik aufzeigt. Strata Cloud Manager prognostiziert das Datum, an dem die Metrik die maximale Kapazität erreichen wird. Sie können den Cursor über das Diagramm bewegen, um die Kapazität einer Metrik zu einem beliebigen Zeitpunkt zu überprüfen. Sie können eine **Prognosezeit** für die nächsten 30 oder 90 Tage auswählen.

In diesem Beispiel können Sie sehen, dass die VPN-Tunnel-Metrik auf dem Gerät am **5. November 2023**die maximale Kapazität erreichen wird.



STEP 4 | Von der Seite **Benachrichtigungen** aus können Sie **Zur Kapazitätsanalyseseite gehen** auswählen, um die Heatmap der Kapazitätsanalyse anzuzeigen.



Informationen zur Verwendung der Heatmap der Kapazitätsanalyse und zum Überprüfen der Kapazitätsbenachrichtigungen finden Sie unter Analysieren der metrischen Kapazität.

CPU-Auslastungsmetriken in AIOps für NGFW

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Die CPU-Auslastung wird in AIOps für NGFW mit den folgenden Metriken verfolgt:

- **mp_system_resources.mp_cpu**: Gibt die Gesamtauslastung der CPU an.
- **mp_system_resources_daemon.cpu_usage_sum**: Gibt die CPU-Auslastung an, die sich aus den Aufgaben der Verwaltungsebene ergibt, die in der CPU der Verwaltungsebene (Management Plane CPU, MP-CPU) ausgeführt werden. Diese Metrik entspricht der CPU-Auslastung von SNMP.
- **mp_system_resources_daemon.pan_task_cpu_usage**: Gibt die CPU-Auslastung an, die sich aus den in der MP-CPU verarbeiteten PAN-Aufgaben ergibt, die Vorgänge auf Datenebene ausführen. Diese Daten sind nicht Teil der SNMP- und **mp_system_resources_daemon.pan_task_cpu_usage**-Metrik.

Die Gesamtauslastung der CPU wird wie folgt berechnet:

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

Erstellen einer Benachrichtigungsregel

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Die Integration von Strata Cloud Manager in Ihre bestehenden Abläufe umfasst die Einrichtung proaktiver Benachrichtigungen, durch die Sie potenzielle Probleme erkennen und Gegenmaßnahmen ergreifen können, bevor sie zu schwerwiegenden Komplikationen führen. Diese Benachrichtigungen können an das Fallverwaltungsprotokoll Ihres Betriebsteams angepasst werden, beispielsweise mit den häufig verwendeten Prioritäten P1 oder P2.

Sie können beispielsweise ein Benachrichtigungssystem einrichten, bei dem kritische Benachrichtigungen zu den kritischsten Problemen sofort an Ihr Sicherheitsteam weitergeleitet werden, damit es sich umgehend darum kümmern kann. Andererseits können Warnhinweise, die weniger dringlich, aber dennoch wichtig sind, zur täglichen Überprüfung eingerichtet werden. Eine solche Regelung gewährleistet eine effiziente Vorfallverwaltung und sorgt gleichzeitig für reibungslose Betriebsabläufe.

Eine weitere Option ist die teambasierte Weiterleitung von Benachrichtigungen. Bestimmte Benachrichtigungskategorien oder selbst spezifische Benachrichtigungen können an unterschiedliche Teams weitergeleitet werden, die am besten für die Bearbeitung dieser Meldungen gerüstet sind. Sie können Benachrichtigungseinstellungen definieren, z. B. welche Alarme Benachrichtigungen auslösen, wie und wie oft Sie Benachrichtigungen erhalten, und Sie können eine Benachrichtigungsregel erstellen.

In diesem Video erfahren Sie, wie Sie eine Benachrichtigungsregel erstellen.

STEP 1 | Wählen Sie **Vorfälle und Benachrichtigungen** > **Vorfall- und Benachrichtigungseinstellungen** > **Benachrichtigungsregeln** > **Benachrichtigungsregel hinzufügen** aus.

STEP 2 | Geben Sie einen `Namen` und eine `Beschreibung` ein.

STEP 3 | Wählen Sie **Neue Bedingung hinzufügen** aus, um die `Regelbedingungen` anzugeben, die zum Auslösen der Benachrichtigung führen.

Um beispielsweise eine Benachrichtigung zur Hardware zu erstellen, wählen Sie **Unterkategorie**, **Gleich** und **Hardware** aus.

STEP 4 | Wählen Sie `Benachrichtigungstyp und Empfänger` für die Benachrichtigung aus.

1. Wenn Sie **E-Mail** auswählen, wählen Sie eine E-Mail-Gruppe aus, also eine Gruppe von Benutzern, die die E-Mail-Benachrichtigungen erhalten. Alternativ wählen Sie **Neue E-Mail-Gruppe erstellen** aus.

   1. Wenn Sie eine neue E-Mail-Gruppe erstellen, geben Sie den Namen einer E-Mail-Gruppe ein und beginnen Sie mit der Eingabe der E-Mail-Adressen derjenigen, die Sie der Gruppe hinzufügen möchten. Drücken Sie nach der Eingabe der einzelnen E-Mail-Adressen die Eingabetaste.

2. Wählen Sie **Next (Weiter)**.
3. Wählen Sie aus, wie oft diese Benachrichtigungen gesendet werden sollen:
   - Sofort
   - Gruppiert und alle 4 Stunden
   - Gruppiert und einmal pro Tag
2. Wenn Sie **ServiceNow** auswählen, geben Sie die `ServiceNow-URL`, die Anmeldeinformationen für den Client, die Anmeldeinformationen für ServiceNow und die `ServiceNow-API-Version` ein.
   1. **Testen** Sie Ihre Verbindung, um sicherzustellen, dass die Integration funktioniert.
   2. Wählen Sie **Next (Weiter)**.

STEP 5 | **Regel speichern**

Integration in ServiceNow

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	❑ oder

Wenn Sie Ihre ServiceNow-Integration für die AIOps for NGFW-Benachrichtigungsregel konfigurieren, benötigen Sie Folgendes:

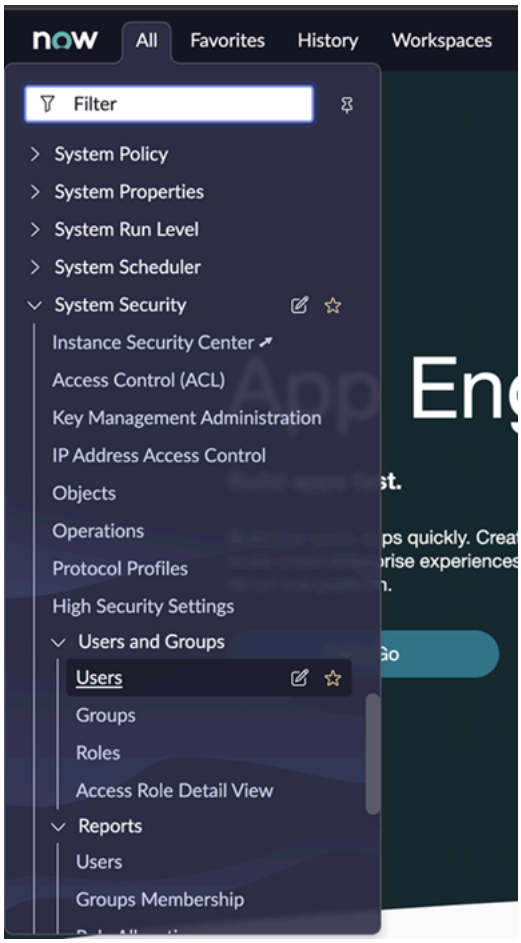
- Konfigurierte ServiceNow-Instanz mit Administratorzugriff
- ServiceNow-Benutzername und -Passwort mit Webzugriff und spezifischen Rollen zum Erstellen von Vorfällen oder Abfragen verschiedener Tabellen
- Client-ID und Passwort, die in der Anwendungsregistrierung erstellt wurden, um AIOps den Zugriff auf Ihre ServiceNow-Instanz zu gewähren
- URL Ihrer ServiceNow-Instanz

Ihre ServiceNow-Instanz sollte auch über eine **Vorfall**-Tabelle verfügen, an die AIOps Benachrichtigungen senden kann, sowie über **Zuweisungsgruppen** mit **Verantwortlichen**, damit diese Benachrichtigungen an bestimmte Personen gesendet werden können.

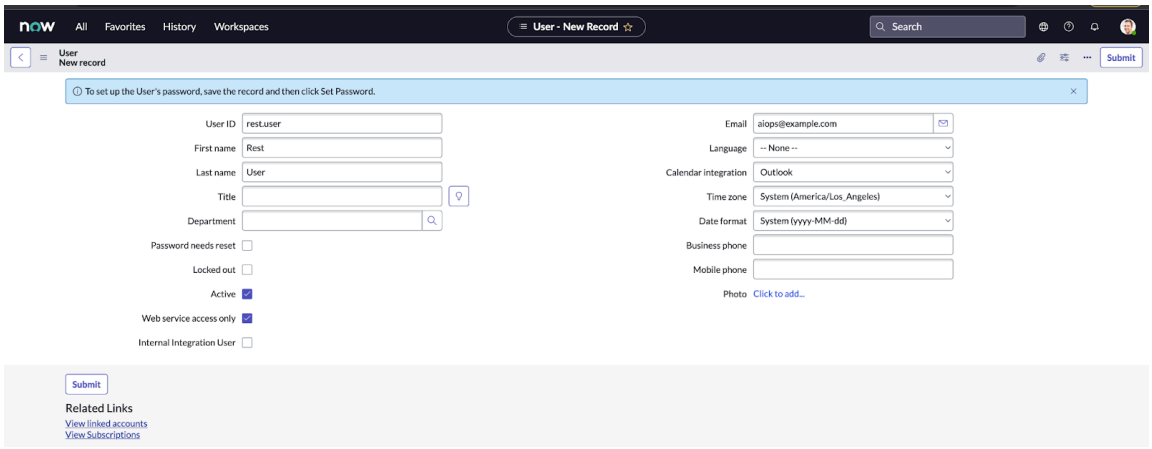
STEP 1 | Erstellen eines ServiceNow-Rest-Benutzers.

Erstellen Sie einen neuen ServiceNow-Benutzer mit bestimmten Rollen zum Lesen von und Schreiben in die verschiedenen Tabellen, die für die Integration benötigt werden („Vorfall“, „Zuweisungsgruppen“ und „Verantwortliche“).

1. Um einen Benutzer in ServiceNow zu erstellen, navigieren Sie unter **Systemsicherheit > Benutzer und Gruppen** zu **Benutzer**.

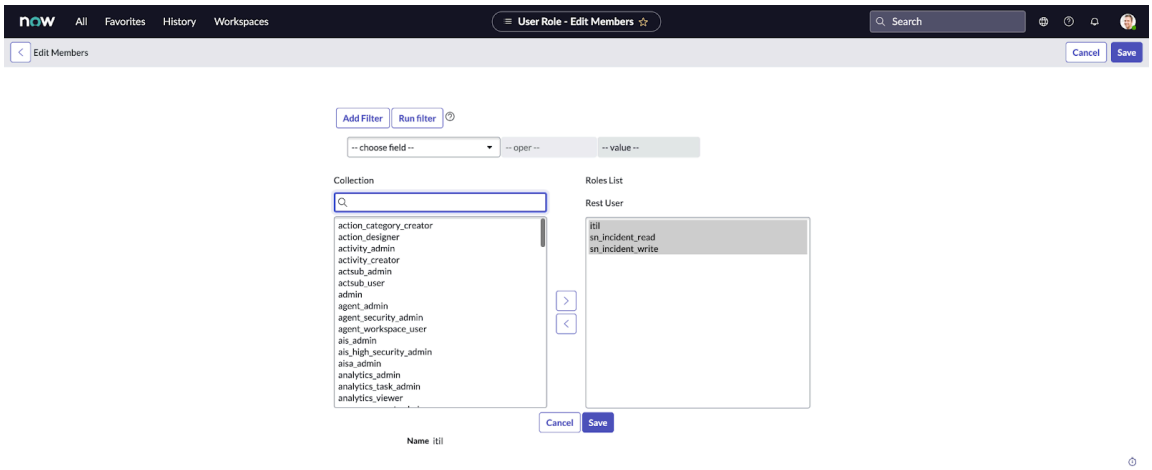


2. Aktivieren Sie das Kontrollkästchen **Nur Webdienst-Zugriff** und senden Sie Ihre Änderungen.



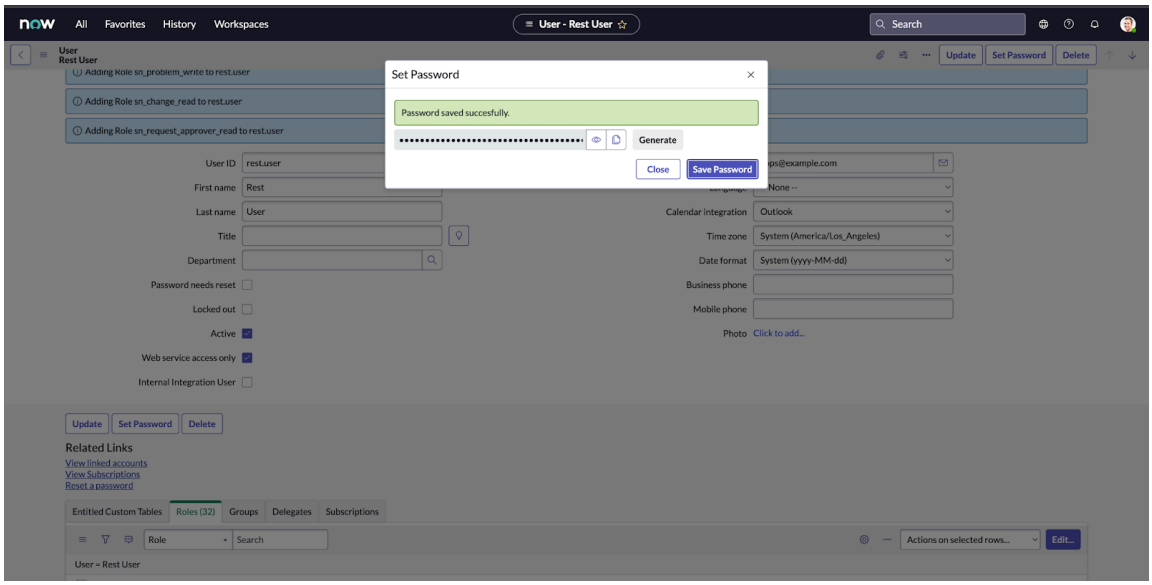
3. Suchen Sie nach dem neu erstellten Benutzer. Wählen Sie in der Tabelle unten auf der Seite die Registerkarte **Rollen** aus und klicken Sie auf **Bearbeiten**. Sie müssen dem

Benutzer Berechtigungen für die drei folgenden Rollen erteilen: **itil, sn_incident_read** und **sn_incident_write**. Speichern Sie Ihre Änderungen.



4. Klicken Sie auf der Seite „Benutzer“ auf **Passwort festlegen**. Klicken Sie im Popup-Fenster auf **Generieren** und **Passwort speichern**. Stellen Sie sicher, dass Sie das Passwort zusammen mit der Benutzer-ID an einen sicheren Ort kopieren. Diese

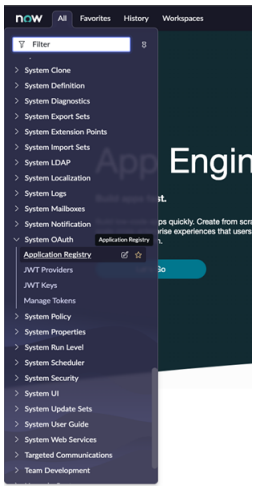
Informationen werden verwendet, um die Anmeldeinformationen für den **ServiceNow-Benutzer** in AIOps for NGFW auszufüllen.



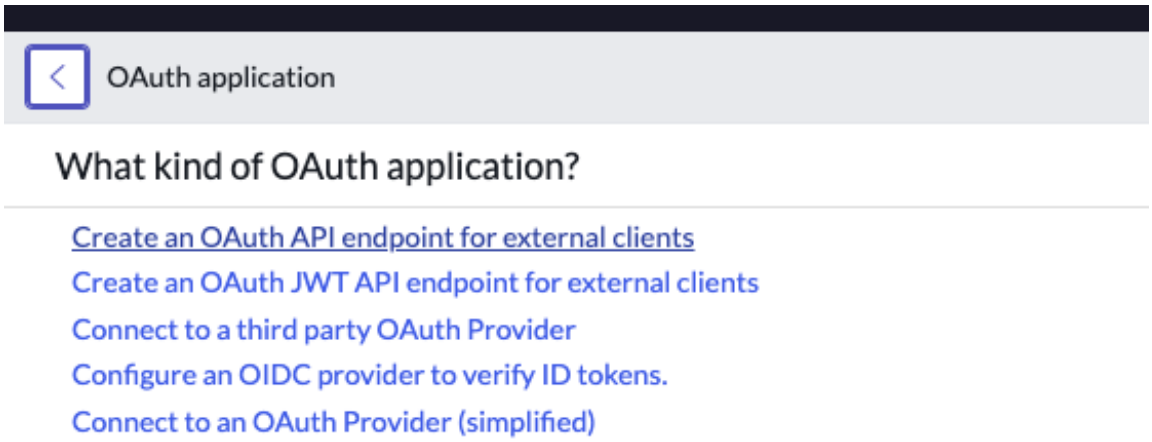
STEP 2 | Erstellen eines Web-OAuth-Clients.

Für die Authentifizierung von AIOps for NGFW bei Ihrer ServiceNow-Instanz ist ein OAuth-Client erforderlich.

1. Navigieren Sie zu **System-OAuth > Anwendungsregistrierung**.

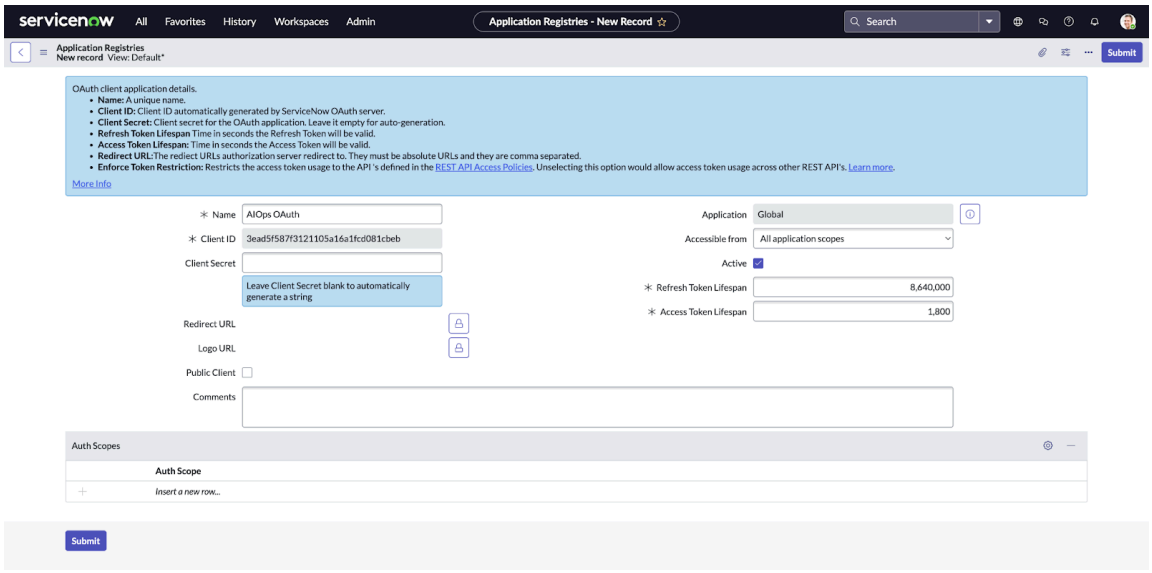


2. Erstellen Sie einen neuen Eintrag und wählen Sie auf der folgenden Seite den Link **OAuth-API-Endpunkt für externe Clients erstellen** aus.



3. Fügen Sie einen Namen für das OAuth-Protokoll hinzu und erstellen Sie einen **geheimen Client-Schlüssel**. Der **geheime Client-Schlüssel** kann auch leer gelassen werden, wenn der geheime Schlüssel automatisch generiert werden soll. Klicken Sie auf **Übermitteln**, navigieren Sie dann zurück zum Eintrag in der Anwendungsregistrierung und speichern Sie sowohl die **Client-ID** als auch den **geheimen Client-Schlüssel** an einem sicheren Ort.

Diese Informationen werden in den Formularen für **Client-Anmeldeinformationen** in AIOps for NGFW verwendet.



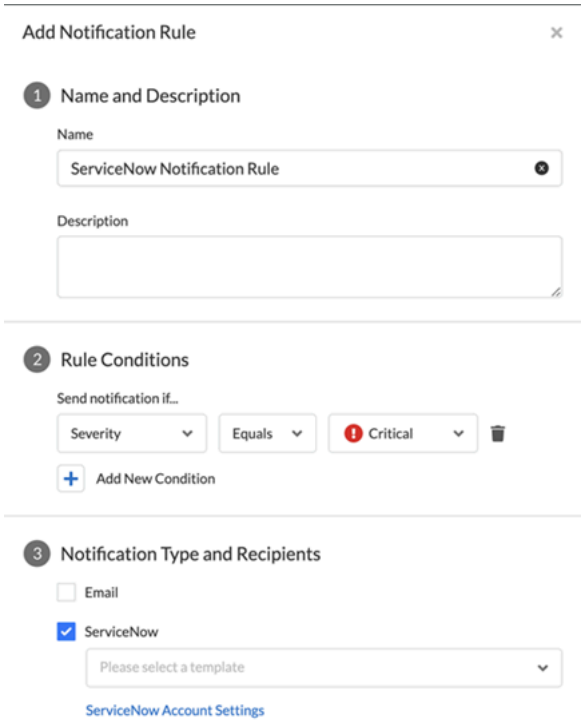
STEP 3 | Hinzufügen von Informationen zu den ServiceNow-Kontoeinstellungen in AIOps for NGFW.

Fügen Sie die Informationen aus den vorherigen Schritten in AIOps for NGFW hinzu, um die Integration zwischen ServiceNow und AIOps for NGFW abzuschließen.

Sie benötigen Folgendes:

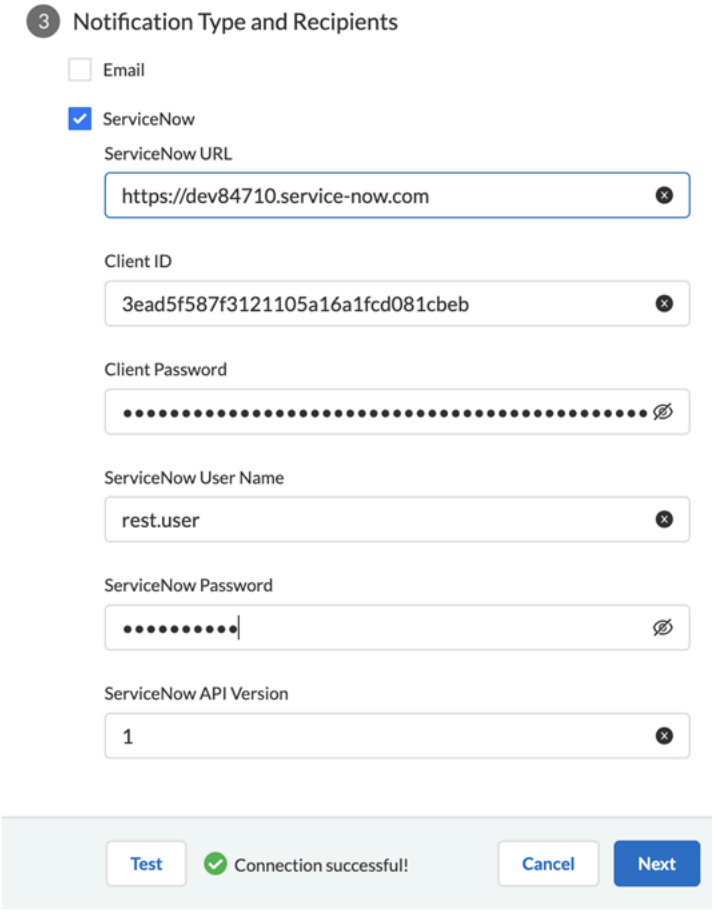
- Die **URL Ihrer ServiceNow-Instanz**
- Den **ServiceNow-Benutzer** und das **Passwort** aus Schritt 1
- Die **Client-ID** und den **geheimen Client-Schlüssel** aus Schritt 2

1. Navigieren Sie in AIOps for NGFW zu **Benachrichtigungsregeln** und klicken Sie auf **Benachrichtigungsregel hinzufügen**.

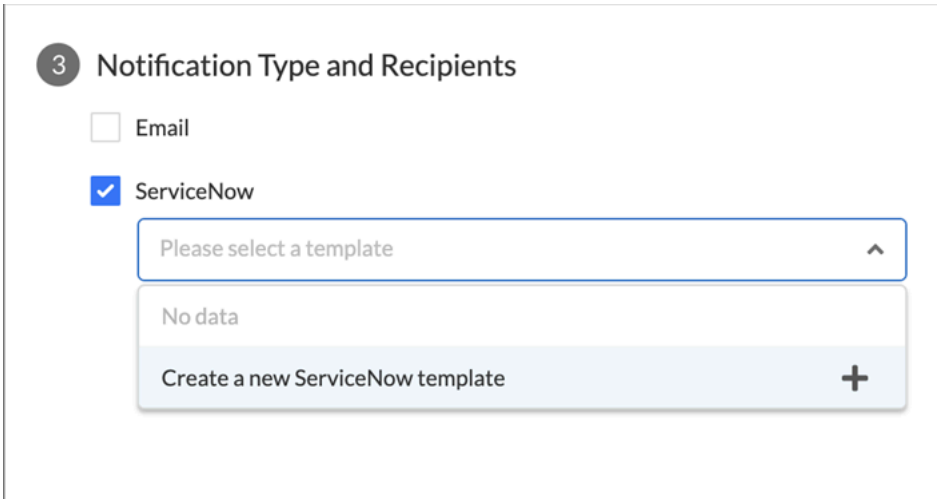


2. Füllen Sie Felder wie **Regelname** und **Benachrichtigungsbedingung** aus und aktivieren Sie dann unter **Benachrichtigungstyp und Empfänger** das Kontrollkästchen **ServiceNow**.
3. Klicken Sie unten in der Seitenleiste auf **ServiceNow-Kontoeinstellungen**. Geben Sie in das folgende Formular die zuvor gespeicherten Informationen ein. **ServiceNow-Benutzer** und **ServiceNow-Passwort** aus Schritt 1, wo Sie den Rest-Benutzer eingerichtet haben. **Client-ID** und **geheimen Client-Schlüssel** aus Schritt 2 zur Einrichtung der Anwendungsregistrierung. Lassen Sie die Version unverändert. Klicken Sie auf **Test**, um die Konfiguration zu speichern und einen Testvorfall an Ihre ServiceNow-Instanz

zu senden. Dieser muss erfolgreich sein, damit Sie fortzufahren können. Klicken Sie auf **Next (Weiter)**.



4. Erweitern Sie das Dropdown-Menü **Bitte wählen Sie eine Vorlage aus** und klicken Sie auf **Neue ServiceNow-Vorlage erstellen**.

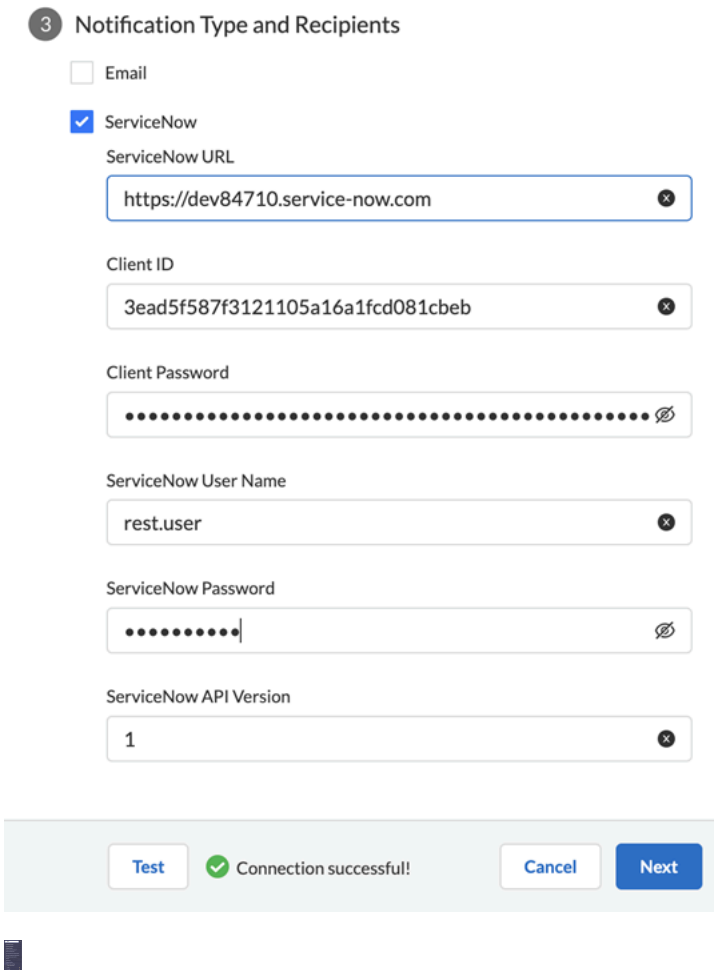


5. Geben Sie den **Namen der ServiceNow-Vorlage** ein und wählen Sie dann eine Gruppe aus der Dropdown-Liste **Zuweisungsgruppe** aus. Wählen Sie eine verantwortliche

Person aus der Dropdown-Liste **Verantwortlicher** aus. Beachten Sie, dass diese Dropdown-Listen mit Werten gefüllt werden, indem Sie die folgenden Tabellen von Ihrer ServiceNow-Instanz aus aufrufen:

- **Systemsicherheit > Benutzer und Gruppen > Benutzer**
- **Systemsicherheit > Benutzer und Gruppen > Gruppen**

Wenn keine Gruppen definiert sind, wird die Dropdown-Liste **Zuweisungsgruppe** nicht ausgefüllt. Wenn einer bestimmten Gruppe keine Benutzer zugewiesen sind, wird die Dropdown-Liste **Verantwortliche** nicht ausgefüllt. Klicken Sie auf **Weiter** und dann auf **Regel speichern**.



AIOps for NGFW-Benachrichtigungsreferenz

Willkommen bei der AIOps for NGFW-Benachrichtigungsreferenz. Zustandsbenachrichtigungen überwachen den Zustand und die Leistung Ihrer Plattform aktiv und in Echtzeit. Mit diesem Ansatz können Sie Probleme leichter erkennen, potenzielle Probleme vorhersagen und Abhilfemaßnahmen implementieren, um eine optimale Funktion Ihrer Geräte zu gewährleisten. Im Folgenden sind einige wichtige Aspekte aufgeführt:

- Überwachung von Metriken: Überwachen Sie kontinuierlich verschiedene Metriken der NGFWs, einschließlich CPU-Auslastung, Arbeitsspeicherauslastung, Festplattenspeicher, Netzwerkdurchsatz und andere relevante Leistungsindikatoren. Durch diese ständige Überwachung wird sichergestellt, dass Abweichungen von der normalen Leistung schnell erkannt werden.
- Anomalieerkennung: Generieren Sie Benachrichtigungen, die basierend auf dem historischen Wert der Metrik und Ihren Nutzungstrends dynamisch angepasst werden. Durch die Nutzung historischer Daten kann das System Anomalien erkennen, die auf potenzielle Probleme hinweisen könnten, und so ein proaktives Management ermöglichen.
- Prädiktive Analyse: Sagen Sie durch die Analyse historischer Daten und Muster voraus, wann bestimmte Schwellenwerte überschritten werden oder wann bestimmte Ereignisse eintreten. Dadurch können potenzielle Probleme vorhergesehen werden, bevor sie eskalieren.

Auf den folgenden Seiten sind die Benachrichtigungen aufgeführt, die AIOps for NGFW auslösen kann.

- Premium-Zustandsbenachrichtigungen: Lassen Sie sich die Premium-Benachrichtigungen zum Zustand Ihrer Plattform anzeigen, die Strata Cloud Manager auslösen kann.
- Kostenlose Zustandsbenachrichtigungen: Lassen Sie sich die kostenlosen Benachrichtigungen zum Zustand Ihrer Plattform anzeigen, die AIOps for NGFW auslösen kann.
- Benachrichtigungen zu Diensten: Lassen Sie sich die Benachrichtigungen zu verbundenen Diensten anzeigen, die AIOps for NGFW auslösen kann.
- Durch den Einsatz von maschinellem Lernen ausgelöste Benachrichtigungen: Lassen Sie sich die Benachrichtigungen anzeigen, die Strata Cloud Manager durch den Einsatz von maschinellem Lernen auslösen kann.

Informationen zu den Sicherheitsstatusprüfungen, die AIOps for NGFW auslösen kann, finden Sie in der Tabelle **Verwalten > Sicherheitsstatus > Einstellungen > Sicherheitsprüfungen**, in der die Prüfungen aufgeführt sind.

Premium-Zustandsbenachrichtigungen

In der folgenden Tabelle sind die Premium-Benachrichtigungen zum Zustand Ihrer Plattform aufgeführt, die Strata Cloud Manager auslösen kann.

Damit Strata Cloud Manager diese Benachrichtigungen auslösen kann, ist eine Premium-Lizenz für AIOps for NGFW erforderlich.

Benachrichtigen	Beschreibung
ACC-Abfragefehler (Premium-Benachrichtigung)	Diese Benachrichtigung informiert darüber, dass die Abfrage des Application Command Center (ACC) fehlgeschlagen ist. Klasse: Zustand Kategorie: Berichterstattung In-App-Support-Ticket: Nein
Unerwünschte Nutzung von Ressourcen für verschlüsselten Datenverkehr (Premium-Benachrichtigung)	Die Ressourcen für verschlüsselten Datenverkehr werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Unerwünschte Nutzung von Ressourcen (Premium-Benachrichtigung)	Die Firewall weist ungewöhnliche Werte für Verbindungen pro Sekunde (CPS), Durchsatz oder Anzahl der Sitzungen auf. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – ARP-Tabelle (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass die Einträge in der ARP-Tabelle bald die maximale Kapazität der Firewall ausgeschöpft haben werden. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Adressgruppen (Premium-Benachrichtigung)	Die Anzahl der Adressgruppenobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität

Benachrichtigen	Beschreibung
	In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Adressobjekte (Premium-Benachrichtigung)	Die Anzahl der Adressobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – CPU auf Datenebene (Premium-Benachrichtigung)	Die CPU-Auslastung auf Datenebene (Dataplane, DP) war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Entschlüsselungsnutzung (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass SSL-Entschlüsselungssitzungen bald die maximale Kapazität der Firewall ausgeschöpft haben werden. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – FQDN-Adressen (Premium-Benachrichtigung)	Die Anzahl der FQDN-Adressobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – GlobalProtect-Tunnel (clientlos) (Premium-Benachrichtigung)	Die Anzahl der clientlosen GlobalProtect-VPN-Tunnel nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – IKE-Peers (Premium-Benachrichtigung)	Die Anzahl der IKE-Peers war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität

Benachrichtigen	Beschreibung
	In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – CPU auf Verwaltungsebene (Premium-Benachrichtigung)	Die CPU-Auslastung auf Verwaltungsebene (Management Plane, MP) war konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Arbeitsspeicher auf Verwaltungsebene (Premium-Benachrichtigung)	Die Arbeitsspeichernutzung auf Verwaltungsebene (Management Plane, MP) war konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – NAT-Richtlinien (Premium-Benachrichtigung)	Die Anzahl der NAT-Richtlinienregeln war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Sicherheitsrichtlinien (Premium-Benachrichtigung)	Die Anzahl der Sicherheitsrichtlinienregeln war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Dienstgruppen (Premium-Benachrichtigung)	Die Anzahl der Dienstgruppenobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Dienstobjekte	Die Anzahl der Dienstobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand

Benachrichtigen	Beschreibung
(Premium-Benachrichtigung)	Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Sitzungstabellenauslastung (Premium-Benachrichtigung)	Die Auslastung der Sitzungstabelle (%) war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die die Firewall oder die VM-Lizenz unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Site-to-Site-VPN-Tunnel (Premium-Benachrichtigung)	Die Anzahl der Site-to-Site-VPN-Tunnel, bestehend aus IPsec-Tunneln und Proxy-IDs, war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an die maximale Kapazität – URLs oder IPs innerhalb von EDLs (Premium-Benachrichtigung)	Die Anzahl der URLs, IPs oder Domänen innerhalb der konfigurierten EDL(s), die in der Richtlinie dieser Firewall verwendet werden, nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Virtuelle Systeme (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass die Konfiguration virtueller Systeme bald die von der Lizenz der Firewall unterstützte maximale Kapazität erreichen wird. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an die maximalen Konfigurationsgrenzwerte (Premium-Benachrichtigung)	Firewallobjekte wie Regeln, Gruppen und Sicherheitsprofile nähern sich den Gerätegrenzwerten. Klasse: Zustand Kategorie: Konfigurationslimits In-App-Support-Ticket: Nein
Zertifikatablauf	Mindestens ein Zertifikat in der Firewall wurde gesperrt oder läuft bald ab.

Benachrichtigen	Beschreibung
(Premium-Benachrichtigung)	Klasse: Zustand Kategorie: Zertifikat In-App-Support-Ticket: Nein
Commit und Push fehlgeschlagen (Premium-Benachrichtigung)	Die Übertragung der Konfiguration per Push ist fehlgeschlagen. Klasse: Zustand Kategorie: Configuration (Konfiguration) In-App-Support-Ticket: Nein
Konfigurationsspeicherauslastung nähert sich den maximalen Grenzwerten (Premium-Benachrichtigung)	Die Konfiguration der Firewall nähert sich ihrem maximalen Speicherauslastungslimit. Während Commits muss der gesamte Konfigurationsspeicher der Firewall Platz für zwei Kopien bieten: die aktuell verwendete Konfiguration und die neue zu verwendende Konfiguration. Wenn der pro Konfiguration zugewiesene Speicher 50 % überschreitet, erreicht die Firewall ihr Kapazitätslimit, was zu einem Commit-Fehler führt. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
DP-Paketverlust (Premium-Benachrichtigung)	Die Benachrichtigung informiert darüber, dass anormale Paketverluste aus verschiedenen Gründen erkannt wurden Klasse: Zustand Kategorie: Leistung In-App-Support-Ticket: Nein
Status der HA-Links (Premium-Benachrichtigung)	Der Zustand eines Links, der mit der Firewall verbunden ist. Die Firewall ist mit verschiedenen Systemen für verschiedene Dienste verbunden. Diese Benachrichtigung gibt Auskunft über den Zustand dieser Verbindungen. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein
Hohe Protokollerfassungsrate (Premium-Benachrichtigung)	Ein Protokollkollektor nähert sich seiner maximal unterstützten Erfassungsrate. Klasse: Zustand Kategorie: Protokollierung In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
Hohe Protokollabfrageaktivität (Premium-Benachrichtigung)	Der Protokollkollektor nähert sich seiner Kapazität für Abfragejobs oder Berichte. Klasse: Zustand Kategorie: Protokollierung In-App-Support-Ticket: Nein
Erhöhte Datenverkehrslatenz – Paketpuffer (Premium-Benachrichtigung)	Die Ressourcen für den Paketpuffer auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Erhöhte Datenverkehrslatenz – Paketdeskriptor (Premium-Benachrichtigung)	Die Ressourcen des Paketdeskriptors auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Erhöhte Datenverkehrslatenz – unbekanntes TCP oder UDP (Premium-Benachrichtigung)	Die Firewall hat eine große Menge an Datenverkehr empfangen, dessen Anwendung als „unknown-tcp“ oder „unknown-udp“ kategorisiert ist. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Verbindung zum Protokollweiterleitungsziel ist verloren (Premium-Benachrichtigung)	Das Gerät kann keine Verbindung zu seinem Protokollweiterleitungsziel herstellen. Klasse: Zustand Kategorie: Protokollierung In-App-Support-Ticket: Nein
Mindestaufbewahrungsdauer für Protokolle ist überschritten (Premium-Benachrichtigung)	Der Protokollkollektor enthält Protokolle, die älter als die definierte Mindestaufbewahrungsdauer sind. Klasse: Zustand Kategorie: Protokollierung In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
Fehler bei der NAT-Zuweisung (Premium-Benachrichtigung)	Mindestens eine NAT-Regel kann nicht genügend Ressourcen für die Übersetzung zuweisen. Klasse: Zustand Kategorie: NAT-Poolressource In-App-Support-Ticket: Ja
NAT-Pool-Nutzung (Premium-Benachrichtigung)	Mindestens eine NAT-Regel weist eine hohe Ressourcennutzung auf. Klasse: Zustand Kategorie: NAT-Poolressource In-App-Support-Ticket: Nein
NGFW SD-WAN-Anwendungsleistungsbenachrichtigung (Premium-Benachrichtigung)	Zeigt die Liste der Anwendungen an, die von einer schlechten Verbindungsleistung betroffen sind. Klasse: Zustand Kategorie: SD-WAN-Leistung In-App-Support-Ticket: Nein
NGFW SD-WAN-Verbindungsleistungsbenachrichtigung (Premium-Benachrichtigung)	Gibt an, was zu Leistungseinbußen bei Ihren Apps und Diensten in Ihrem Link führt. Klasse: Zustand Kategorie: SD-WAN-Leistung In-App-Support-Ticket: Nein
Vom Standard abweichende Protokollierungsstufe (Premium-Benachrichtigung)	Diese Benachrichtigung wird ausgelöst, wenn die Protokollierungsstufe eines Dienstes nicht auf die Standardkonfiguration eingestellt ist. Diese Benachrichtigung stellt sicher, dass die Dienste ihre angegebenen Protokollierungseinstellungen konsistent beibehalten. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Verbindungsunterbrechung des vom in PAN-OS integrierten Benutzer-ID-Agenten überwachten Servers	Diese Benachrichtigung wird ausgelöst, wenn der Server, der vom in PAN-OS integrierten Benutzer-ID-Agenten (Benutzer-ID ohne Agent) überwacht wird, die Verbindung zur Firewall verliert. Dieser überwachte Server ist eine wichtige Komponente für die Zuordnung von Benutzeridentitäten zu Netzwerkaktivitäten. Klasse: Zustand

Benachrichtigen	Beschreibung
(Premium-Benachrichtigung)	Kategorie: In-App-Support-Ticket: Nein
Speicherauslastung der Richtlinienkonfiguration nähert sich den maximalen Grenzwerten (Premium-Benachrichtigung)	Diese Benachrichtigung informiert darüber, dass die Speicherauslastung der Richtlinienkonfiguration einen kritischen Schwellenwert überschreitet. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Datenverkehrslatenz – Paketdeskriptoren (On-Chip) (Premium-Benachrichtigung)	Ressourcen für den Paketdeskriptor (On-Chip) auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Flood/DoS In-App-Support-Ticket: Nein
Tunnel inaktiv (Premium-Benachrichtigung)	Mindestens ein Site-to-Site-VPN-Tunnel ist ausgefallen. Klasse: Zustand Kategorie: Site-to-Site-VPN In-App-Support-Ticket: Ja
Zonenschutzprofil – Flood-Erkennung (Premium-Benachrichtigung)	Die in der Zone hergestellten Verbindungen oder die eingehende Paketrate sind zu hoch oder ungewöhnlich. Klasse: Zustand Kategorie: Flood/DoS In-App-Support-Ticket: Ja
Zonenschutzprofil – Schwellenwertempfehlung (Premium-Benachrichtigung)	In einer Zone fehlt ein Zonenschutzprofil oder die Schwellenwerte in einem Zonenschutzprofil müssen angepasst werden. Klasse: Zustand Kategorie: Flood/DoS In-App-Support-Ticket: Nein

Kostenlose Zustandsbenachrichtigungen

In der folgenden Tabelle sind die kostenlosen Benachrichtigungen zum Zustand Ihrer Plattform aufgeführt, die AIOps for NGFW auslösen kann.

Damit AIOps for NGFW diese Benachrichtigungen auslösen kann, ist keine Premium-Lizenz erforderlich.

Benachrichtigen	Beschreibung
Stromausfall einer Karte (Kostenlose Benachrichtigung)	Es wurde ein Kartenausfall erkannt, was auf ein mögliches Problem mit der Karte oder ihrem Sitz im Chassis hindeutet. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Konfigurationsgröße erreicht Gerätekapazitätsgrenze (Kostenlose Benachrichtigung)	Die Konfigurationsgröße dieses Geräts hat ihre Kapazitätsgrenze erreicht. Klasse: Zustand Kategorie: Configuration (Konfiguration) In-App-Support-Ticket: Nein
Beeinträchtigtes Systemlaufwerk (Kostenlose Benachrichtigung)	Ein beeinträchtigtes Systemlaufwerk wurde durch Überwachung seiner Attributwerte erkannt. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Verzögerte Telemetrie (Kostenlose Benachrichtigung)	Die Analyse-Engines haben keine neuen Telemetriewerte von dieser NGFW/diesem Panorama erhalten. Klasse: Zustand Kategorie: Telemetrie In-App-Support-Ticket: Ja
FE100-Ausfall (Kostenlose Benachrichtigung)	Auf dem FE100-Chip in der Firewall wurde ein Kalibrierfehler erkannt. Dieses Problem weist normalerweise auf einen Hardwarefehler hin. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
Probleme mit Lüftern (Kostenlose Benachrichtigung)	Ein Lüfter oder eine Lüfterschale hat einen Alarm am Gerät ausgelöst. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Schwerwiegender Computerfehler (Kostenlose Benachrichtigung)	Es wurde ein schwerwiegender Computerfehler erkannt. Dieses Problem weist normalerweise auf einen Hardwarefehler in der CPU hin. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Firewall von Cortex Data Lake getrennt (Kostenlose Benachrichtigung)	Die Verbindung zwischen FW und Strata Logging Service wurde unterbrochen. Klasse: Zustand Kategorie: SLS-Konnektivität In-App-Support-Ticket: Nein
Firewall wurde von Panorama getrennt (Kostenlose Benachrichtigung)	Die Verbindung zwischen Firewall und Panorama wurde unterbrochen. Klasse: Zustand Kategorie: Verbindungsfehler In-App-Support-Ticket: Nein
HA-Backup (Kostenlose Benachrichtigung)	Die HA-Backup-Links sind derzeit nicht konfiguriert. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein
HA-Peer-Verbindungsstatus (Kostenlose Benachrichtigung)	Eine der Firewalls im HA-Paar ist nicht funktionsfähig. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Ja
Hohe Speicherplatznutzung – pancfg-Partition	Die Festplattenpartition nähert sich der Kapazitätsgrenze oder ist voll ausgelastet. Klasse: Zustand

Benachrichtigen	Beschreibung
(Kostenlose Benachrichtigung)	Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Hohe Speicherplatznutzung – panlogs-Partition (Kostenlose Benachrichtigung)	Die Festplattenpartition nähert sich der Kapazitätsgrenze oder ist voll ausgelastet. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Hohe Speicherplatznutzung – Root-Partition (Kostenlose Benachrichtigung)	Die Festplattenpartition nähert sich der Kapazitätsgrenze oder ist voll ausgelastet. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Hohe Verarbeitungsaktivität (Kostenlose Benachrichtigung)	Mindestens eine Rechenressource auf dem Gerät wird knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
IPQ-Fehler (Kostenlose Benachrichtigung)	Auf einem der FE100-Chips in der Firewall wurde ein IPQ-Fehler (Ingress Packet Queue) festgestellt. Dieser Fehler zeigt normalerweise an, dass eine Komponente aus ihrem Steckplatz herausgenommen und erneut eingesetzt werden muss oder dass ein Hardwarefehler vorliegt. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Unregelmäßige Eingangsleistung (Kostenlose Benachrichtigung)	Die Leistungswerte des Geräts liegen außerhalb des normalen Bereichs. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Lizenzablauf (Kostenlose Benachrichtigung)	Mindestens eine Ihrer Lizenzen steht kurz vor dem Ablauf oder ist bereits abgelaufen. Klasse: Zustand Kategorie: PanOS und Abonnement

Benachrichtigen	Beschreibung
	In-App-Support-Ticket: Nein
Ausfall des Protokolllaufwerks (Kostenlose Benachrichtigung)	Durch die Überwachung des Festplattenstatus der Firewall wurde ein ausgefallenes Protokolllaufwerk erkannt. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
MPC-Karte – CPLD-Ausfall (Kostenlose Benachrichtigung)	Die Management Processor Card (MPC) ist eine wesentliche Komponente des PA-5450, die Verwaltungs-, Protokollierungs- und Hochverfügbarkeitsfunktionen bereitstellt. Die MPC-Karte ist aufgrund eines Problems mit einer ihrer Komponenten, dem komplexen programmierbaren Logikbaustein (Complex Programmable Logic Device, CPLD), ausgefallen. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Ablauf des NGFW/ Panorama-Verwaltungszertifikats (Kostenlose Benachrichtigung)	Bei dieser Benachrichtigung wurde der Ablauf des NGFW/ Panorama-Verwaltungszertifikats erkannt. Klasse: Zustand Kategorie: Zertifikat In-App-Support-Ticket: Nein
NPC-Karte – FE100-Ausfall (Kostenlose Benachrichtigung)	NPC-Karten (Network Processing Cards) bieten Netzwerkkonnektivität und sind für die Verarbeitung des Netzwerkverkehrs unerlässlich. Bei einer NPC-Karte ist ein Problem mit ihrer FE100-Komponente aufgetreten, das zu deren Ausfall führte. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Nicht synchrone Peers – Konfiguration (Kostenlose Benachrichtigung)	Die Systemkonfigurationen auf den HA-Peers stimmen nicht überein. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
Nicht synchrone Peers – Dynamischer Inhalt (Kostenlose Benachrichtigung)	Dynamische Inhalte wie Virenschutz oder Anwendungen und Bedrohungen stimmen bei den HA-Peers nicht überein. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein
Nicht synchrone Peers – Sitzungen (Kostenlose Benachrichtigung)	Die Sitzungen bei den HA-Peers stimmen nicht überein oder sind nicht aktuell. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein
Nicht synchrone Peers – Software (Kostenlose Benachrichtigung)	Die PAN-OS-Softwareversionen auf den HA-Peers stimmen nicht überein. Klasse: Zustand Kategorie: Hochverfügbarkeit In-App-Support-Ticket: Nein
Veralteter dynamischer Inhalt (Kostenlose Benachrichtigung)	Der auf dem Gerät installierte dynamische Inhalt ist im Vergleich zu den Inhalten, die auf dem Updateserver verfügbar sind, veraltet. Klasse: Zustand Kategorie: Dynamischer Inhalt In-App-Support-Ticket: Nein
Ende der Lebensdauer von PAN-OS (Kostenlose Benachrichtigung)	Ihre aktuelle Version von PAN-OS wird nicht mehr unterstützt. Klasse: Zustand Kategorie: PanOS und Abonnement In-App-Support-Ticket: Nein
Bekannte Sicherheitslücken in PAN-OS (Kostenlose Benachrichtigung)	Ihre aktuelle PAN-OS-Version weist bekannte Sicherheitslücken auf. Klasse: Zustand Kategorie: Dynamischer Inhalt In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
Ablauf des Stamm- und Standardzertifikats von PAN-OS – Szenario 1 (Kostenlose Benachrichtigung)	Das Stammzertifikat und das Standardzertifikat auf der Firewall sind abgelaufen. Klasse: Zustand Kategorie: Zertifikat In-App-Support-Ticket: Nein
PCI-Fehler (Kostenlose Benachrichtigung)	Die Verbindung einer Peripheriekomponente (Peripheral Component Interconnect, PCI) ist für die Verbindung der Verwaltungsebene (Management Plane, MP) mit der Kontrollebene (Control Plane, CP) zuständig. Ein bestimmter Fehler im Zusammenhang mit dieser Komponente deutet auf einen Ausfall ihrer Funktionalität hin. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Pfadüberwachungsfehler – Karte (Kostenlose Benachrichtigung)	Auf einer Karte, die sich in den Slots der Firewall befindet, wurde ein Fehler bei der Pfadüberwachung festgestellt. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Portausfall (Kostenlose Benachrichtigung)	Es wurde ein Ausfall im Zusammenhang mit dem physischen Verwaltungsport oder einem der physischen Hochverfügbarkeitsports erkannt. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein
Erschöpfung des Prozessspeichers – Configd (Kostenlose Benachrichtigung)	Die Prozesse auf Verwaltungsebene des Geräts erschöpfen den verfügbaren Arbeitsspeicher. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Erschöpfung des Prozessspeichers – Geräteserver	Die Prozesse auf Verwaltungsebene des Geräts erschöpfen den verfügbaren Arbeitsspeicher. Klasse: Zustand Kategorie: Ressourcennutzung

Benachrichtigen	Beschreibung
(Kostenlose Benachrichtigung)	In-App-Support-Ticket: Ja
Erschöpfung des Prozessspeichers – Protokollempfänger (Kostenlose Benachrichtigung)	Die Prozesse auf Verwaltungsebene des Geräts erschöpfen den verfügbaren Arbeitsspeicher. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Erschöpfung des Prozessspeichers – Verwaltungsserver (Kostenlose Benachrichtigung)	Die Prozesse auf Verwaltungsebene des Geräts erschöpfen den verfügbaren Arbeitsspeicher. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Erschöpfung des Prozessspeichers – Benutzer-ID (Kostenlose Benachrichtigung)	Die Prozesse auf Verwaltungsebene des Geräts erschöpfen den verfügbaren Arbeitsspeicher. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja
Ausfall der redundanten Stromversorgung (Kostenlose Benachrichtigung)	Die Redundanz der Stromversorgung wird nicht erreicht, weil sie nicht eingefügt wurde, die Stromversorgung nicht funktioniert hat oder keine vollständige Redundanz erreicht wurde. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Ja
Protokollweiterleitungslatenz des Strata-Protokollierungsdienstes (Kostenlose Benachrichtigung)	Die Weiterleitungslatenz des Strata-Protokollierungsdienstes überschreitet einen akzeptablen Wert. Klasse: Zustand Kategorie: SLS-Status In-App-Support-Ticket: Nein
Protokollweiterleitung des Strata-Protokollierungsdienstes ist offline	Der Protokollweiterleitungsdienst des Strata-Protokollierungsdienstes funktioniert nicht Klasse: Zustand Kategorie: SLS-Status

Benachrichtigen	Beschreibung
(Kostenlose Benachrichtigung)	In-App-Support-Ticket: Nein
Protokollerfassungslatenz des Strata-Protokollierungsdienstes (Kostenlose Benachrichtigung)	Die Erfassungslatenz des Strata-Protokollierungsdienstes überschreitet einen akzeptablen Wert. Klasse: Zustand Kategorie: SLS-Status In-App-Support-Ticket: Nein
Protokollerfassung des Strata-Protokollierungsdienstes ist offline (Kostenlose Benachrichtigung)	Der Erfassungsdienst des Strata-Protokollierungsdienstes funktioniert nicht. Klasse: Zustand Kategorie: SLS-Status In-App-Support-Ticket: Nein
Der Protokollspeicher des Strata-Protokollierungsdienstes nähert sich den Grenzwerten (Kostenlose Benachrichtigung)	Die Protokolltypen nähern sich dem konfigurierten maximalen Speicherlimit. Klasse: Zustand Kategorie: Protokollierung In-App-Support-Ticket: Nein
Thermische Probleme (Kostenlose Benachrichtigung)	Die Gerätetemperatur liegt außerhalb des normalen Bereichs. Klasse: Zustand Kategorie: Hardware In-App-Support-Ticket: Nein

Benachrichtigungen zu Diensten

In der folgenden Tabelle sind die Benachrichtigungen aufgeführt, die AIOps for NGFW im Zusammenhang mit den damit verbundenen Diensten auslösen kann.

Benachrichtigen	Beschreibung
Firewall von Strata Logging Service getrennt (Kostenlose Benachrichtigung)	Die Verbindung zwischen FW und SLS ist seit über 5 Minuten unterbrochen. Kategorie: SLS-Konnektivität In-App-Support-Ticket: Nein
Protokollerfassung des Strata-Protokollierungsdienstes ist offline (Kostenlose Benachrichtigung)	Der SLS-Erfassungsdienst funktioniert seit über 5 Minuten nicht mehr. Kategorie: SLS-Status In-App-Support-Ticket: Nein
Protokollweiterleitung des Strata-Protokollierungsdienstes ist offline (Kostenlose Benachrichtigung)	Der SLS-Protokollweiterleitungsdienst funktioniert seit über 5 Minuten nicht mehr. Kategorie: SLS-Status In-App-Support-Ticket: Nein
Protokollerfassungslatenz des Strata-Protokollierungsdienstes (Kostenlose Benachrichtigung)	Die Latenz bei der Erfassung für SLS lag in den letzten 15 Minuten bei mehr als 10 Minuten. Kategorie: SLS-Status In-App-Support-Ticket: Nein
Protokollweiterleitungslatenz des Strata-Protokollierungsdienstes (Kostenlose Benachrichtigung)	Die Weiterleitungslatenz auf SLS lag in den letzten 15 Minuten bei mehr als 10 Minuten. Kategorie: SLS-Status In-App-Support-Ticket: Nein
Der Protokollspeicher des Strata-Protokollierungsdienstes nähert sich den Grenzwerten	Die Protokolltypen nähern sich dem konfigurierten maximalen Speicherlimit. Kategorie: Protokollierung In-App-Support-Ticket: Nein

Benachrichtigen	Beschreibung
(Kostenlose Benachrichtigung)	

Durch den Einsatz von maschinellem Lernen ausgelöste Benachrichtigungen

In der folgenden Tabelle sind die Benachrichtigungen aufgeführt, die AIOps for NGFW durch den Einsatz von maschinellem Lernens auslösen kann.

Benachrichtigen	Beschreibung
Unerwünschte Nutzung von Ressourcen für verschlüsselten Datenverkehr (Premium-Benachrichtigung)	Die Ressourcen für verschlüsselten Datenverkehr werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein Erkennungstyp: Anomalie
Unerwünschte Nutzung von Ressourcen (Premium-Benachrichtigung)	Die Firewall weist ungewöhnliche Werte für Verbindungen pro Sekunde (CPS), Durchsatz oder Anzahl der Sitzungen auf. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein Erkennungstyp: Anomalie
Annäherung an die maximalen Konfigurationsgrenzwerte (Premium-Benachrichtigung)	Firewallobjekte wie Regeln, Gruppen und Sicherheitsprofile nähern sich den Gerätegrenzwerten. Klasse: Zustand Kategorie: Konfigurationslimits In-App-Support-Ticket: Nein Erkennungstyp: Anomalie
Hohe Verarbeitungsaktivität (Kostenlose Benachrichtigung)	Mindestens eine Rechenressource auf dem Gerät wird knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Nein
Erhöhte Datenverkehrslatenz – Paketpuffer (Premium-Benachrichtigung)	Die Ressourcen für den Paketpuffer auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja

Benachrichtigen	Beschreibung
	Erkennungstyp: Anomalie
Erhöhte Datenverkehrslatenz – Paketdeskriptor (Premium-Benachrichtigung)	Die Ressourcen des Paketdeskriptors auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Ressourcennutzung In-App-Support-Ticket: Ja Erkennungstyp: Anomalie
Datenverkehrslatenz – Paketdeskriptoren (On-Chip) (Premium-Benachrichtigung)	Ressourcen für den Paketdeskriptor (On-Chip) auf dem Gerät werden knapp. Klasse: Zustand Kategorie: Flood/DoS In-App-Support-Ticket: Nein Erkennungstyp: Anomalie
Annäherung an maximale Kapazität – ARP-Tabelle (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass die Einträge in der ARP-Tabelle bald die maximale Kapazität der Firewall ausgeschöpft haben werden. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Adressgruppen (Premium-Benachrichtigung)	Die Anzahl der Adressgruppenobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Adressobjekte (Premium-Benachrichtigung)	Die Anzahl der Adressobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – CPU auf Datenebene	Die CPU-Auslastung auf Datenebene (Dataplane, DP) war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann.

Benachrichtigen	Beschreibung
(Premium-Benachrichtigung)	Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Entschlüsselungsnutzung (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass SSL-Entschlüsselungssitzungen bald die maximale Kapazität der Firewall ausgeschöpft haben werden. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – FQDN-Adressen (Premium-Benachrichtigung)	Die Anzahl der FQDN-Adressobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – GlobalProtect-Tunnel (clientlos) (Premium-Benachrichtigung)	Die Anzahl der clientlosen GlobalProtect-VPN-Tunnel nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – IKE-Peers (Premium-Benachrichtigung)	Die Anzahl der IKE-Peers war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – CPU auf Verwaltungsebene (Premium-Benachrichtigung)	Die CPU-Auslastung auf Verwaltungsebene (Management Plane, MP) war konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein

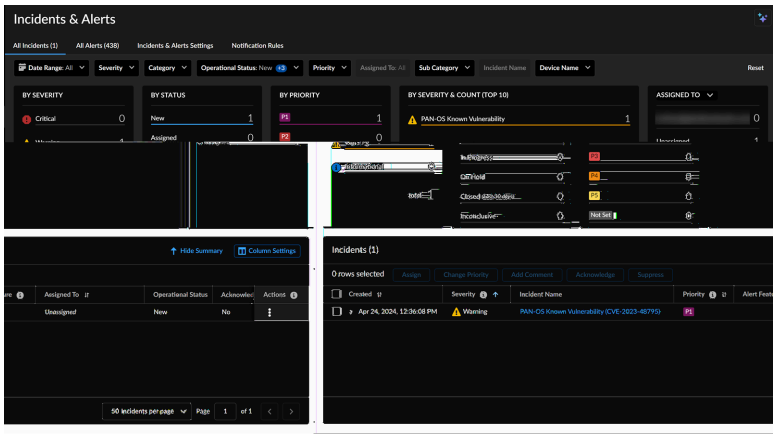
Benachrichtigen	Beschreibung
Annäherung an maximale Kapazität – Arbeitsspeicher auf Verwaltungsebene (Premium-Benachrichtigung)	Die Arbeitsspeichernutzung auf Verwaltungsebene (Management Plane, MP) war konstant hoch und nähert sich der maximalen Kapazität, die das Gerät unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – NAT-Richtlinien (Premium-Benachrichtigung)	Die Anzahl der NAT-Richtlinienregeln war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Sicherheitsrichtlinien (Premium-Benachrichtigung)	Die Anzahl der Sicherheitsrichtlinienregeln war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Dienstgruppen (Premium-Benachrichtigung)	Die Anzahl der Dienstgruppenobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Dienstobjekte (Premium-Benachrichtigung)	Die Anzahl der Dienstobjekte war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Sitzungstabellenauslastung (Premium-Benachrichtigung)	Die Auslastung der Sitzungstabelle (%) war über längere Zeit konstant hoch und nähert sich der maximalen Kapazität, die die Firewall oder die VM-Lizenz unterstützen kann. Klasse: Zustand Kategorie: Kapazität

Benachrichtigen	Beschreibung
	In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Virtuelle Systeme (Premium-Benachrichtigung)	Die Datenprognoseanalyse zeigt, dass die Konfiguration virtueller Systeme bald die von der Lizenz der Firewall unterstützte maximale Kapazität erreichen wird. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
Annäherung an maximale Kapazität – Site-to-Site-VPN-Tunnel (Premium-Benachrichtigung)	Die Anzahl der Site-to-Site-VPN-Tunnel, bestehend aus IPsec-Tunneln und Proxy-IDs, war konstant hoch und nähert sich der maximalen Kapazität, die die Firewall unterstützen kann. Klasse: Zustand Kategorie: Kapazität In-App-Support-Ticket: Nein
NGFW SD-WAN-Anwendungsleistungsbenachrichtigung (Premium-Benachrichtigung)	Zeigt die Liste der Anwendungen an, die von einer schlechten Verbindungsleistung betroffen sind. Klasse: Zustand Kategorie: SD-WAN-Leistung In-App-Support-Ticket: Nein Erkennungstyp: Anomalie
NGFW SD-WAN-Verbindungsleistungsbenachrichtigung (Premium-Benachrichtigung)	Gibt an, was zu Leistungseinbußen bei Ihren Apps und Diensten oder Links führt. Klasse: Zustand Kategorie: SD-WAN-Leistung In-App-Support-Ticket: Nein Erkennungstyp: Anomalie

Verwalten von NGFW-Vorfällen

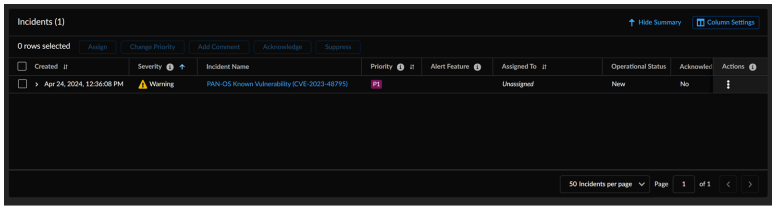
Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Erhalten Sie einen Überblick über die NGFW-Vorfälle, indem Sie **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Vorfälle** auswählen. Informieren Sie sich auf der Seite „Vorfälle“, um über Änderungen in Ihrer Bereitstellung auf dem Laufenden zu bleiben, sodass Sie diese untersuchen und bei Bedarf vorbeugende Maßnahmen ergreifen können. Sie haben direkten Zugriff auf eine detaillierte Liste der Vorfälle und wichtige visuelle Zusammenfassungen. Sie können die **Zusammenfassung ausblenden**, um die Widgets auszublenden und nur die Vorfälle in tabellarischer Form anzuzeigen.



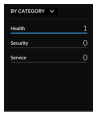
Unter **Alle Vorfälle** werden die folgenden Daten angezeigt.

- **Vorfälle**: Es werden alle Vorfälle angezeigt.



  In dieser Tabelle können Sie die folgenden Aufgaben ausführen:

  - **Zusammenfassung ausblenden**, um die Widgets auszublenden und nur die Vorfälle in tabellarischer Form anzuzeigen.
  - Erweitern Sie einen Vorfall, um seine Beschreibung und Auswirkung anzuzeigen.
  - Unter „Aktionen“ können Sie die folgenden Aktionen ausführen:
    - Sie können einem Benutzer oder sich selbst einen Vorfall **zuweisen** oder die Zuweisung eines Vorfalls aufheben.
    - Mit **Priorität ändern** können Sie die Priorität eines Vorfalls ändern. Oder wählen Sie „Nicht gesetzt“ aus, um die Priorität zu entfernen.
    - Indem Sie in der Spalte **Anerkennen** die Option **Ja** auswählen, bestätigen Sie, dass Sie den Vorfall gesehen haben.
    - Mit **Unterdrücken** können Sie einem Vorfall den Betriebsstatus „In der Warteschleife“ zuweisen, wenn Sie nicht vorhaben, ihn aktiv aufzulösen.
    - Hier können Sie für einen Vorfall einen **Kommentar hinzufügen**.
  - Klicken Sie auf einen Vorfall, um seine Details anzuzeigen.
  - Verwenden Sie die **Spalteneinstellungen**, um bestimmte Spalten für Vorfälle ein- oder auszublenden und die Standardreihenfolge der Spalten neu anzuordnen. Diese Änderungen bleiben in zukünftigen Sitzungen beibehalten.
- **ZUGEWIESEN ZU**: Zeigt die Anzahl der Vorfälle nach der Person oder Entität an, die für deren Auflösung zuständig ist. Ganz oben werden die dem aktuell angemeldeten Benutzer zugewiesenen Vorfälle sowie die nicht zugewiesenen Vorfälle angezeigt. Sie können die Anzahl der Vorfälle auch **NACH KATEGORIE** anzeigen, indem Sie diese Option in der Dropdown-Liste auswählen.



- **NACH SCHWEREGRAD UND ANZAHL (TOP 10):** Zeigt die nach Schweregrad kategorisierten Vorfälle zusammen mit der Anzahl der Vorfälle in jeder Kategorie an. Kritische Vorfälle

erhalten oberste Priorität, gefolgt von Vorfällen mit Warnungen und schließlich Vorfällen mit informativen Benachrichtigungen.

- **NACH STATUS:** Zeigt die Gesamtzahl der Vorfälle nach Status an.
  - „Neu“ gibt an, wie viele Vorfälle nicht zugewiesen wurden.
  - „Zugewiesen“ gibt an, wie viele Vorfälle einem Benutzer zugewiesen wurden.
  - „In Bearbeitung“ gibt an, an wie vielen Vorfällen gearbeitet wird.
  - „In der Warteschleife“ gibt an, dass Sie nicht vorhaben, einen Vorfall aktiv aufzulösen.
  - „Geschlossen“ gibt die Anzahl der Vorfälle an, die in den letzten 30 Tage geschlossen wurden.
  - „Uneindeutig“ gibt an, dass es für diese Vorfälle keine Lösung gibt.

- **NACH SCHWERGRAD:** Zeigt die Gesamtzahl der Vorfälle an, denen die Kategorie „Kritisch“, „Warnung“ und „Information“ zugewiesen wurde.

- **NACH PRIORITÄT:** Zeigt die Vorfälle entsprechend ihrer Priorität an, wobei P1 den Vorfällen mit der höchsten Priorität entspricht.

Anzeigen von Vorfalldetails

Wo kann ich das verwenden?	Was brauche ich?
• , einschließlich derer, die durch Software-NGFW-Credits finanziert werden	Eine der folgenden Komponenten: ❑ oder ❑ oder

Unter **Alle Vorfälle** können Sie einen Vorfall auswählen, um eine Seite mit Details zu diesem Vorfall zu öffnen. Auf der Registerkarte **Zusammenfassung** werden die folgenden Details angezeigt:

1. Zusammenfassung des Vorfalls mit Details. Sie können die Priorität des Vorfalls ändern oder ihn einem Benutzer zuweisen.
2. Auswirkung des Vorfalls, d. h. die Anzahl der betroffenen NGFWs.
3. Empfohlene Maßnahmen zur Behebung des Problems.

Sie können auch auf den CVE klicken, um dessen Details in den Sicherheitshinweisen von Palo Alto Networks und die Schwachstellen in der PAN-OS-Version anzuzeigen.

Auf der Registerkarte **Korrelierte Benachrichtigungen und Aktivitäten** werden die folgenden Details angezeigt:

- Korrelierte Benachrichtigungen für den ausgewählten Vorfall
- Aufgezeichnete Aktivität für den Vorfall