paloalto TECHDOCS

# Cloud NGFW für AWS-Verwaltung

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

December 5, 2024

# Table of Contents



# Verwalten

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • | ❑ |

Die Cloud NGFW für AWS unterstützt Dienste, die die Einrichtung und Einbindung einfach und unkompliziert machen. Umfassende digitale Services, technischer Support und Education Services unterstreichen unser Engagement für den kontinuierlichen Erfolg Ihrer Palo Alto Networks Bereitstellung. Sie können über die LIVE-Community und das Customer Support Portal auf Unterstützung zugreifen.

Cloud NGFW für AWS ist so konzipiert, dass Sie schnell einsatzbereit sind. Sie überspringen den langwierigen Bereitstellungsprozess, indem Sie unverzichtbare Regelstapel und automatisierte Sicherheitsprofile einrichten und gleichzeitig wie gewohnt mit AWS arbeiten können: vollständige Integration mit AWS-Einbindung, -Überwachung, -Protokollierung und mehr. Laden Sie ganz einfach zusätzliche Benutzer ein, Ihnen bei der Verwaltung Ihrer Cloud NGFW-Bereitstellung zu helfen, oder verwalten Sie Rollen für bestehende Benutzer.

# Benutzer zu Cloud NGFW für AWS einladen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Als Mandantenadministrator können Sie zusätzliche Benutzer einladen, die Ihnen bei der Verwaltung Ihrer Cloud NGFW-Bereitstellung helfen. Anschließend können Sie diesen neuen Benutzern die Rollen zuweisen, die für ihre Zugriffsebene erforderlich sind. Wenn Sie einen Benutzer zum Cloud NGFW-Mandanten einladen, geben Sie die E-Mail-Adresse des Benutzers an und weisen Sie eine oder mehrere Cloud NGFW-Rollen zu. Der Cloud NGFW-Mandant sendet dem Benutzer eine E-Mail mit einem Registrierungslink und einem temporären Passwort. Nach der ersten Anmeldung erstellt der neue Benutzer ein neues Passwort. Bis der eingeladene Benutzer die Einladung angenommen und sich beim Mandanten angemeldet hat, gilt die Einladung als ausstehend.

| Cloud NGFW-Rolle | Berechtigungen |
|---|---|
| Admin | • AWS-Konten hinzufügen<br>• Benutzer einladen und Rollen zuweisen<br>• NGFW erstellen<br>• Globale und lokale Regelstapel erstellen und verwalten |
| Mandantenadministrator | • AWS-Konten hinzufügen<br>• Benutzer einladen und Rollen zuweisen |
| Mandanten-Reader | • Alle Firewall-Ressourcen und ihre Einstellungen lesen<br>• Alle globalen und lokalen Regelstapel lesen<br>• Alle Mandantenbenutzer und Mandanteneinstellungen lesen |
| Administrator für globalen Regelstapel | Globalen Regelstapel erstellen |
| Lokaler Firewall-Administrator | • NGFW erstellen<br>• Lokalen Regelstapel mit NGFWs verknüpfen |

| Cloud NGFW-Rolle | Berechtigungen |
| --- | --- |
| | *Lokale Firewall-Administratoren können nur innerhalb eines bestimmten AWS-Kontos NGFWs erstellen und Regelstapel zuordnen.* |
| Administrator für lokale Regelstapel | • Lokale Regelstapel erstellen<br>• Lokale Regelstapel mit NGFWs verknüpfen<br>Mit jedem Administrator für lokale Regelstapel ist eine Konto-ID verknüpft. Dadurch ist es diesem Administrator möglich, lokale Regelstapel mit NGFWs in demselben Konto zu erstellen. |

*Die E-Mail-Domäne der vom Mandantenadministrator eingeladenen Benutzer muss mit der E-Mail-Domäne der Anmeldeinformationen des Mandantenadministrators übereinstimmen.*

**STEP 1 |** Melden Sie sich beim Cloud NGFW-Mandanten an.

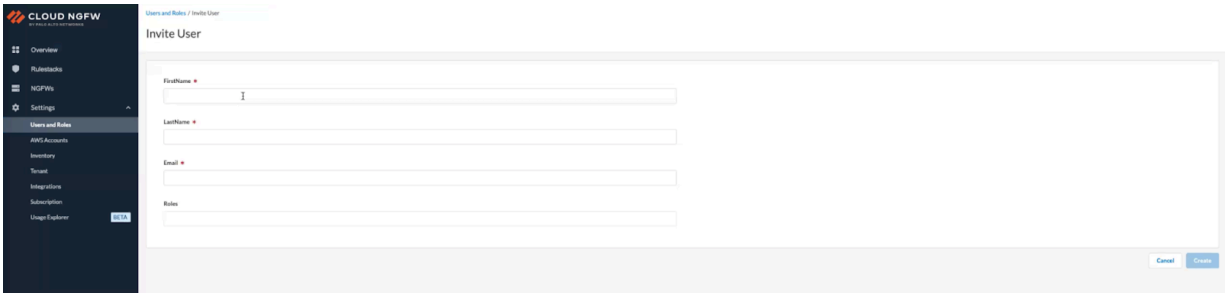
**STEP 2 |** Wählen Sie **Settings (Einstellungen)** > **Users and Roles (Benutzer und Rollen)** > **Invite User (Benutzer einladen)** aus.

**STEP 3 |** Geben Sie den **Vornamen**, **Nachnamen** und die **E-Mail-Adresse** des Eingeladenen ein.

**STEP 4 |** Wählen Sie die Rolle bzw. Rollen des neuen Benutzers aus der Dropdown-Liste **Roles (Rollen)** aus. Sie können jetzt einen vorhandenen Benutzer zu einem Cloud NGFW-Mandanten einladen.

**STEP 5 |** Klicken Sie auf **Create (Erstellen)**.




*Nach der Anmeldung werden Sie aufgefordert, einen Mandanten auszuwählen und auf **Continue (Weiter)** zu klicken. Wenn Sie ein neuer Benutzer sind, erhalten Sie eine Aktivierungs-E-Mail, über die Sie sich für SSO registrieren und beim Mandanten anmelden können. Vorhandene Benutzer können sich mit Ihrem SSO direkt beim Mandanten anmelden.*

## Überlegungen zu Anwendungsfällen mit mehreren Konten

Wenn einem Mandanten über die CNGFW-Konsole bereits ein AWS-Client-Konto hinzugefügt wurde, hat der Benutzer während des Abonnementvorgangs die Wahl, sich mit einem bestehenden Mandanten anzumelden oder einen neuen zu erstellen. In der folgenden Tabelle sind diese Anwendungsfälle veranschaulicht:

| Anwendungsfall | Schritte |
|---|---|
| Sie sind bereits für SSO registriert. | Sie erhalten keine Aktivierungs-E-Mail. |

| Anwendungsfall | Schritte |
| --- | --- |
| Sie sind ein bestehender Benutzer, der nicht für SSO registriert ist | Sie erhalten eine Aktivierungs-E-Mail, um die Registrierung für SSO abzuschließen. Sie können sich jedoch weiterhin wie zuvor anmelden, bis Sie die Registrierung abgeschlossen haben. |

Verwenden Sie eine einzelne E-Mail-ID, um sich bei verschiedenen Mandanten anzumelden. Verwenden Sie dazu die Option **Login with an Existing Tenant (Anmelden mit einem bestehenden Mandanten)**.


Nach der Anmeldung werden Sie aufgefordert, einen Mandanten auszuwählen und auf **Continue (Weiter)** zu klicken. Wenn Sie ein neuer Benutzer sind, erhalten Sie eine Aktivierungs-E-Mail, über die Sie sich für SSO registrieren und beim Mandanten anmelden können. Vorhandene Benutzer können sich mit Ihrem SSO direkt beim Mandanten anmelden.

# Benutzer in Cloud NGFW für AWS verwalten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Sie können jederzeit die Rolle bzw. Rollen eines Benutzers ändern, um seinen Zugriff und seine Berechtigungen zu erweitern oder einzuschränken. Sie können einen Benutzer auch löschen. Einzelne Benutzer können ihre Rollen anzeigen und bei Bedarf ihren Namen oder ihr Passwort ändern.

## Verwalten von Benutzerrollen

**STEP 1 |** Wählen Sie **Settings (Einstellungen)** > **User and Roles (Benutzer und Rollen)** aus.

**STEP 2 |** Klicken Sie auf den Namen des Benutzers.

**STEP 3 |** Ändern Sie bei Bedarf **First Name (Vorname)** und **Last Name (Nachname)**.

**STEP 4 |** Ändern Sie **Roles & Scope (Rollen und Umfang)** für den Benutzer.

- So fügen Sie eine Rolle hinzu:
  1. Klicken Sie auf **Add Role (Rolle hinzufügen)**.
  2. Wählen Sie Einträge für **Role (Rolle)** und **Scope (Umfang)** aus den jeweiligen Dropdown-Listen aus.
- So löschen Sie eine Rolle:
  1. Klicken Sie auf das Löschsymbol ( ) rechts neben der Regel.

**STEP 5 |** Klicken Sie auf **Save (Speichern)**.

## Löschen eines Benutzers

Wenn Sie den Zugriff und die Berechtigungen eines Benutzers vollständig entfernen müssen, können Sie diesen Benutzer löschen.

**STEP 1 |** Wählen Sie **Settings (Einstellungen)** > **User and Roles (Benutzer und Rollen)** aus.

**STEP 2 |** Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.

**STEP 3 |** Wählen Sie **Actions (Aktionen)** > **Delete (Löschen)** aus.

# Bearbeiten von Benutzerinformationen

Ein Nicht-Mandantenadministrator kann bei Bedarf seinen Namen aktualisieren oder sein Passwort ändern. Die zugewiesenen Rollen können jedoch nicht geändert werden.

**STEP 1 |** Wählen Sie **Settings (Einstellungen)** > **User and Roles (Benutzer und Rollen)** aus.

**STEP 2 |** Klicken Sie auf den Benutzernamen.

**STEP 3 |** Ändern Sie bei Bedarf **First Name (Vorname)** und **Last Name (Nachname)**.

**STEP 4 |** So ändern Sie ein Passwort:

1. Klicken Sie auf **Change Password (Passwort ändern)**.
2. Geben Sie das aktuelle Passwort in das Feld **Current Password (Aktuelles Passwort)** ein.
3. Geben Sie das neue Passwort in das Feld **New Password (Neues Passwort)** ein und geben Sie es dann noch einmal ein.
4. Klicken Sie auf **Change (Ändern)**.

*Durch das Ändern des Passworts werden Sie vom Cloud NGFW-Mandanten abgemeldet. Melden Sie sich mit dem neuen Passwort erneut an.*

**STEP 5 |** Klicken Sie auf **Save (Speichern)**.

# Hilfe anfordern

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Verwenden Sie diese Informationen, um Ihre Cloud NGFW-Ressource einzubinden. Informationen zum Auffinden Ihrer Cloud NGFW-Seriennummer und wie Sie einen Supportfall erstellen können, sind ebenfalls enthalten.

## Ihren Cloud NGFW-Mandanten bei der ersten Anmeldung registrieren

Cloud NGFW fordert Sie auf, ein Supportkonto für Ihren Cloud NGFW-Mandanten zu registrieren, nachdem Sie Ihr Passwort erfolgreich zurückgesetzt haben und bevor Sie sich zum ersten Mal bei Ihrer Cloud NGFW-Mandantenkonsole anmelden. Wenn Sie registrierter Benutzer eines oder mehrerer bestehender Palo Alto Networks Supportkonten sind, können Sie Ihren Cloud NGFW-Mandanten bei der ersten Anmeldung bei einem dieser Konten registrieren.

Möglicherweise haben Sie für die Anmeldung bei Cloud NGFW eine andere E-Mail-Adresse verwendet als für den Zugriff auf das Palo Alto Networks Supportkonto. Alternativ können Sie ein dediziertes Palo Alto Networks Supportkonto für Cloud NGFW erstellen. In beiden Fällen überspringen Sie die Registrierungsoption bei der ersten Anmeldung, **registrieren Ihren Cloud NGFW-Mandanten jedoch im Customer Support Portal**.

Gehen Sie wie folgt vor, um Ihren Cloud NGFW-Mandanten bei Ihrem bestehenden Supportkonto zu registrieren:

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

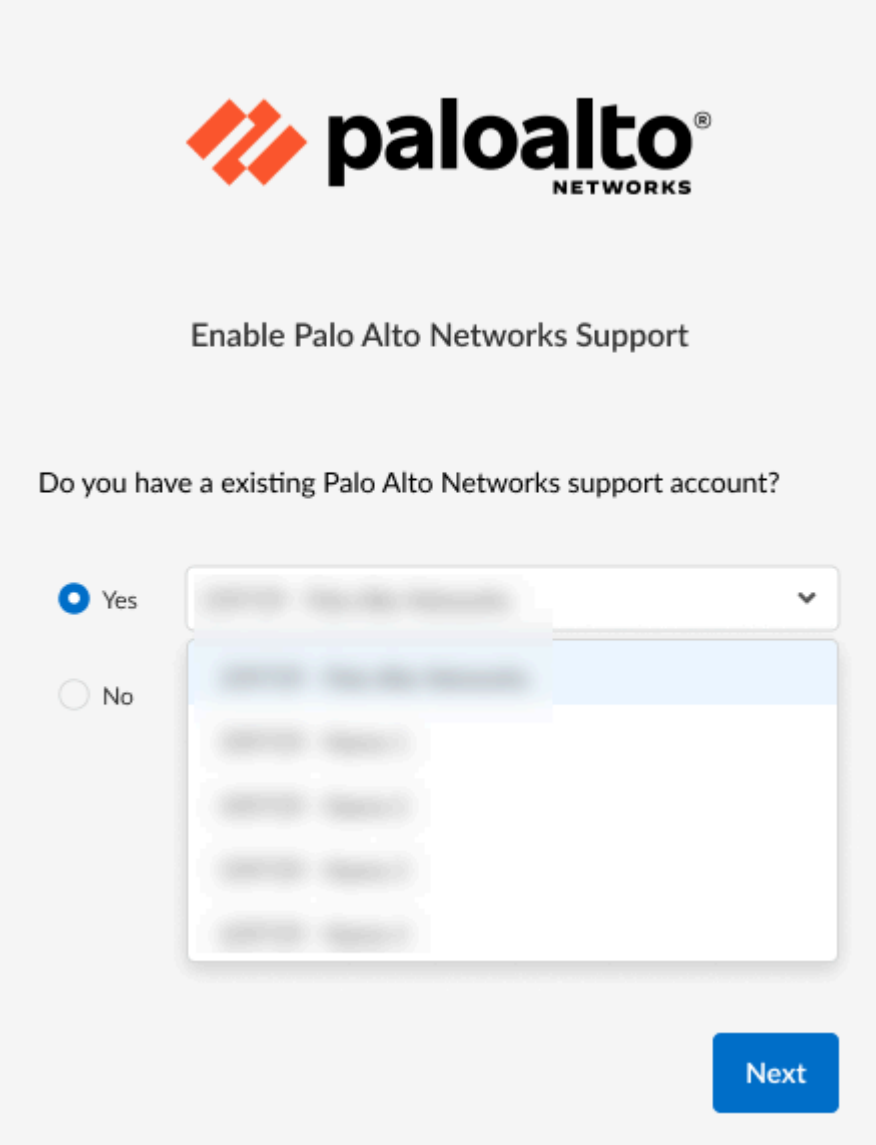
**STEP 2 |** Wählen Sie im Bildschirm **Enable Palo Alto Networks Support (Palo Alto Networks Support aktivieren)** die Option **Yes (Ja)** aus.

> *Wenn Sie im Bildschirm **Enable Palo Alto Networks (Palo Alto Networks aktivieren)** die Option **No (Nein)** auswählen, müssen Sie das Customer Support Portal (CSP) verwenden, um Ihren Cloud NGFW-Mandanten zu registrieren, oder verwenden Sie die Cloud NGFW-Konsole, um sich beim CSP zu registrieren.*

**STEP 3 |** Wählen Sie im Dropdown-Menü das Supportkonto aus.

**STEP 4 |** Klicken Sie auf **Next**.




*Wenn Sie sich bereits beim Customer Support Portal (CSP) registriert haben, werden in der Dropdown-Liste die vorhandenen Konten angezeigt. Wenn Sie jedoch ein neuer Benutzer sind und noch kein Konto haben, verwenden Sie die CSP-Seite, um ein Konto zu erstellen. Weitere Informationen finden Sie unter* Ihren Cloud NGFW-Mandanten über das Customer Support Portal registrieren *und* Ihren Cloud NGFW-Mandanten mithilfe der Cloud NGFW-Konsole im Customer Support Portal registrieren.

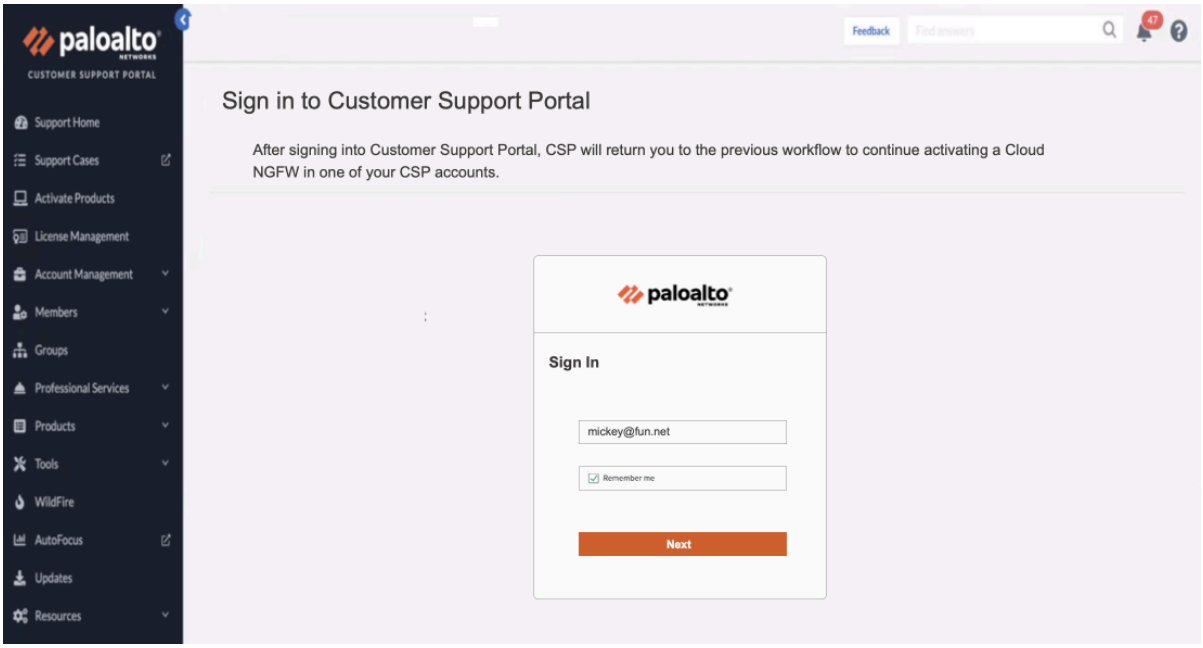
## Ihren Cloud NGFW-Mandanten über das Customer Support Portal registrieren

Sie können das Customer Support Portal verwenden, um Ihren Cloud NGFW-Mandanten zu registrieren.

*Sie benötigen ein Konto, um sich beim CSP anzumelden. Weitere Informationen finden Sie unter* Kundensupportkonto erstellen.

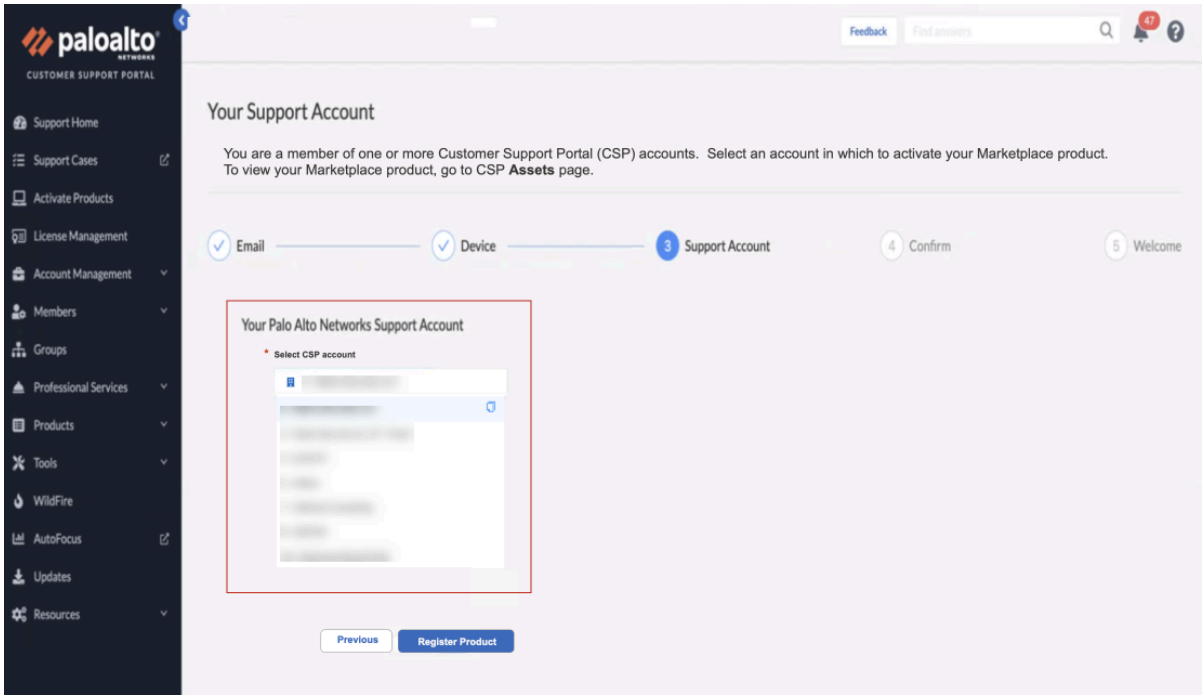
 

**STEP 1 |** Geben Sie im Customer Support Portal Ihre Anmeldeinformationen ein und klicken Sie dann auf **Next (Weiter)**.



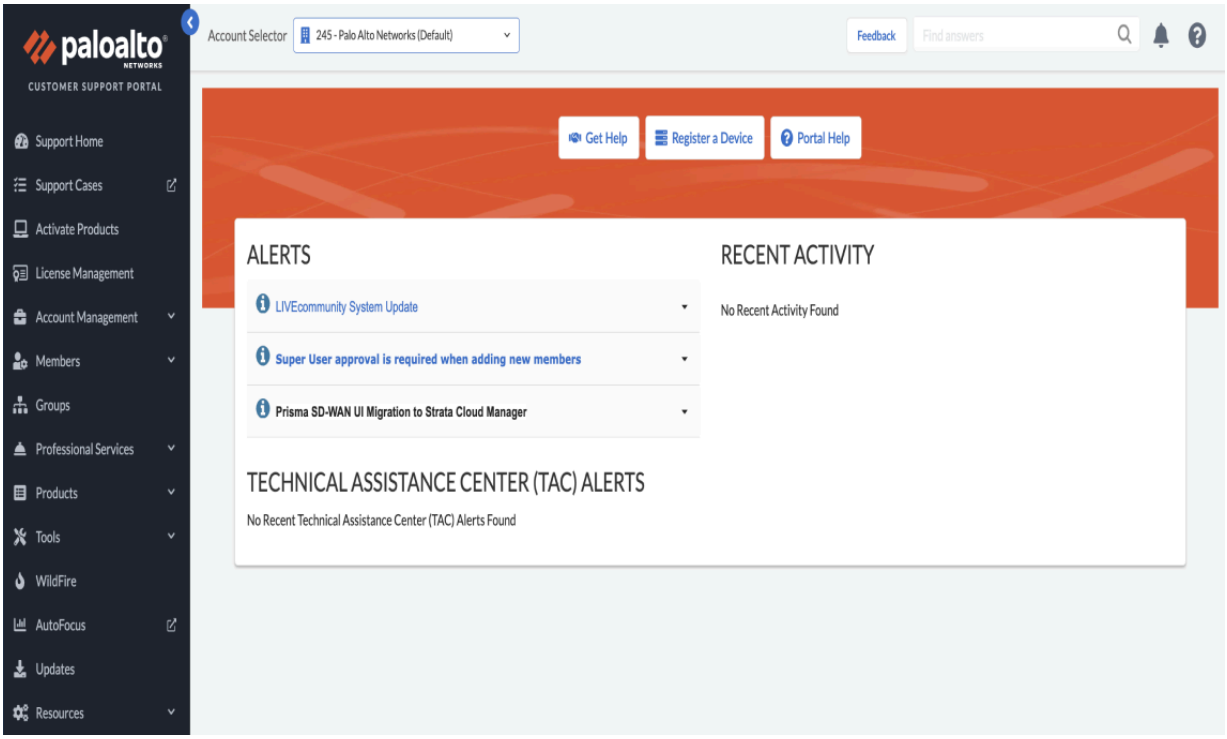

 

**STEP 2 |** Auf der Seite **Your Support Account (Ihr Supportkonto)** werden Informationen zu Ihren Anmeldedaten angezeigt. Wählen Sie das Palo Alto Networks Supportkonto aus und klicken Sie dann auf **Register Product (Produkt registrieren)**.




Sobald die Registrierung abgeschlossen ist, wird ein Bestätigungsfenster und anschließend die Seite des Customer Support Portals angezeigt:




# Ihren Cloud NGFW-Mandanten mithilfe der Cloud NGFW-Konsole im Customer Support Portal registrieren

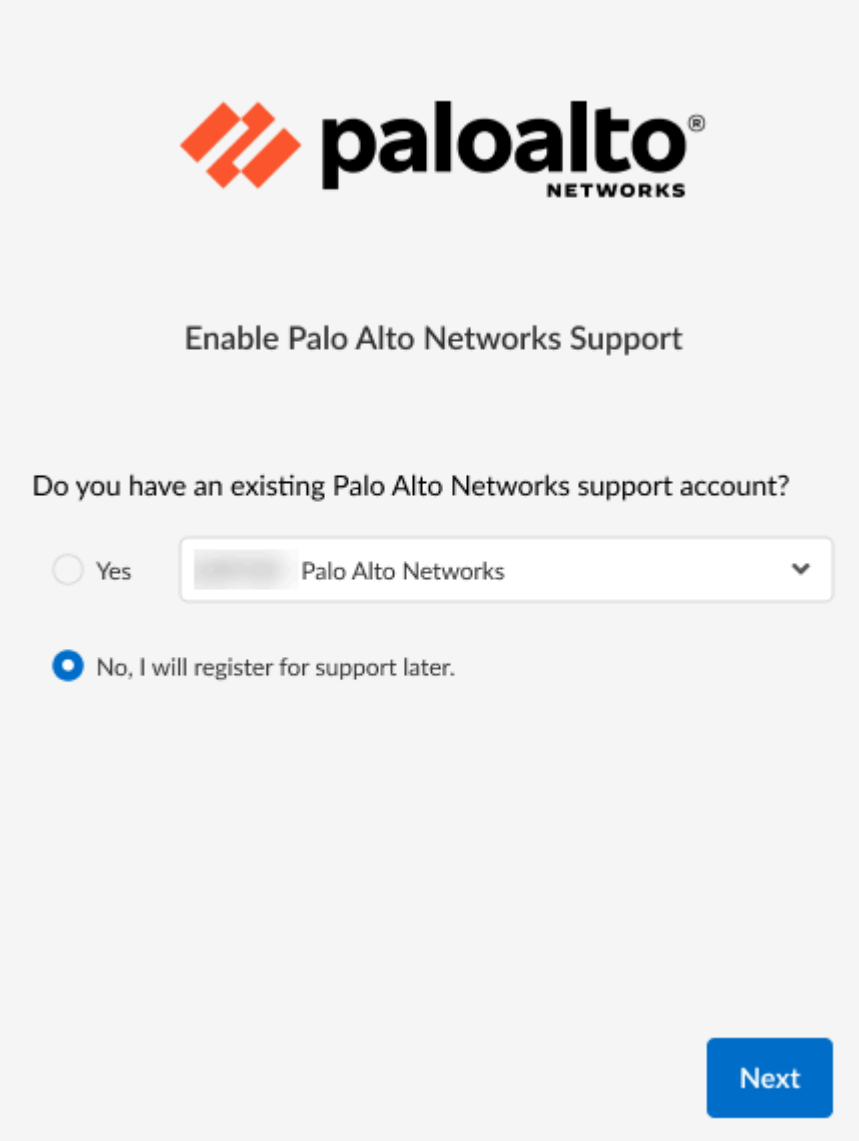
Wenn Sie noch kein Palo Alto Networks Supportkonto haben, werden Sie aufgefordert, eines zu erstellen, bevor Sie Ihren Cloud NGFW-Mandanten verwenden.

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Ressource an.

**STEP 2 |** Wählen Sie auf der Seite **Enable Palo Alto Networks Support (Palo Alto Networks Support aktivieren)** die Option **No (Nein)** aus.

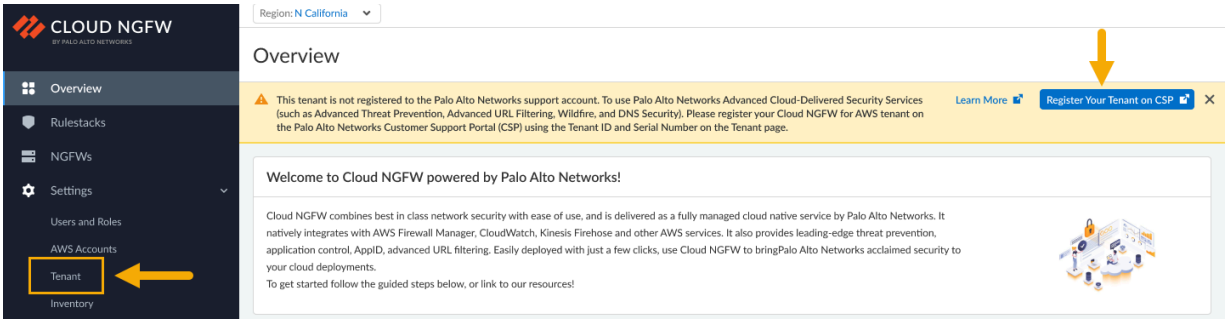
**STEP 3 |** Klicken Sie auf **Next**.



**STEP 4 |** Klicken Sie in der Cloud NGFW-Konsole auf **Register Your Tenant on CSP (Ihren Mandanten im CSP registrieren)**.

*Um Ihren Cloud NGFW-Mandanten einem Customer-Support-Portal-Konto zuzuordnen, benötigen Sie Ihre Geräteregistrierungsinformationen, einschließlich Ihrer **Mandanten-ID** und der **Seriennummer** für Ihre Cloud NGFW-Ressource. Sie finden diese Informationen auf der Seite **Tenant (Mandant)** in der Cloud NGFW-Konsole. Weitere Informationen finden Sie auf der Seite* Supportfall erstellen.

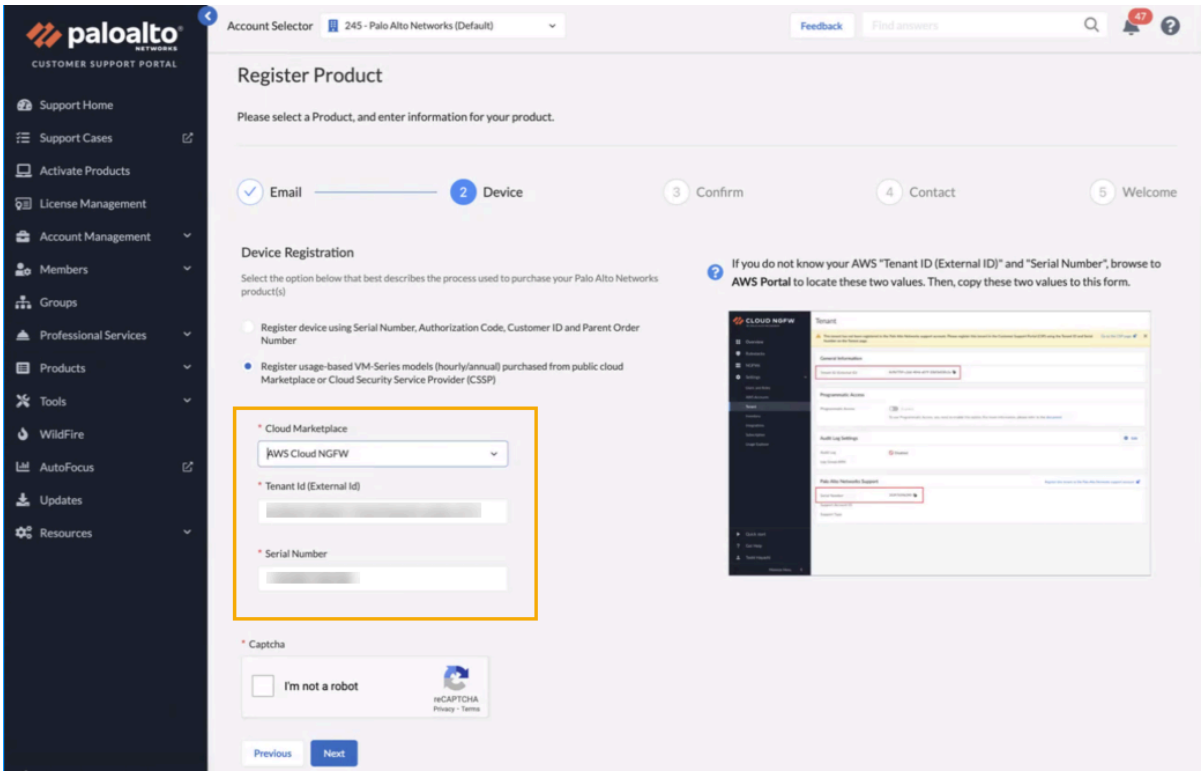



**STEP 5 |** Wählen Sie im Customer Support Portal auf der Seite **Register Product (Produkt registrieren)** im Dropdown-Menü die Option **AWS Cloud NGFW** für den **Cloud-Marketplace** aus. Geben Sie die **Mandanten-ID** und die **Seriennummer** ein und lösen Sie das Captcha.

*Informationen zur Mandanten-ID und zur Seriennummer finden Sie auf der Seite* Supportfall erstellen.

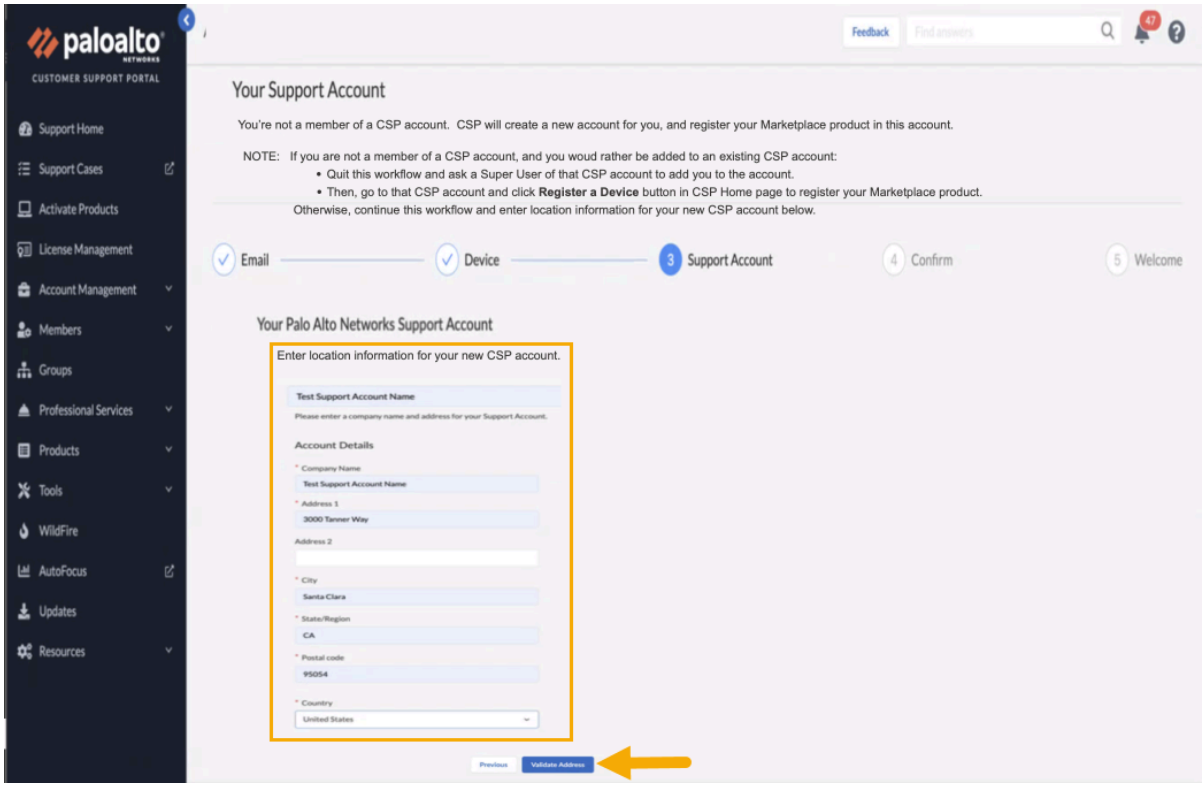
 

**STEP 6 |** Klicken Sie auf **Next (Weiter)**.



**STEP 7 |** Erstellen Sie Ihr Supportkonto. Geben Sie die **Kontodetails** ein und klicken Sie dann auf **Validate Address (Adresse überprüfen)**.

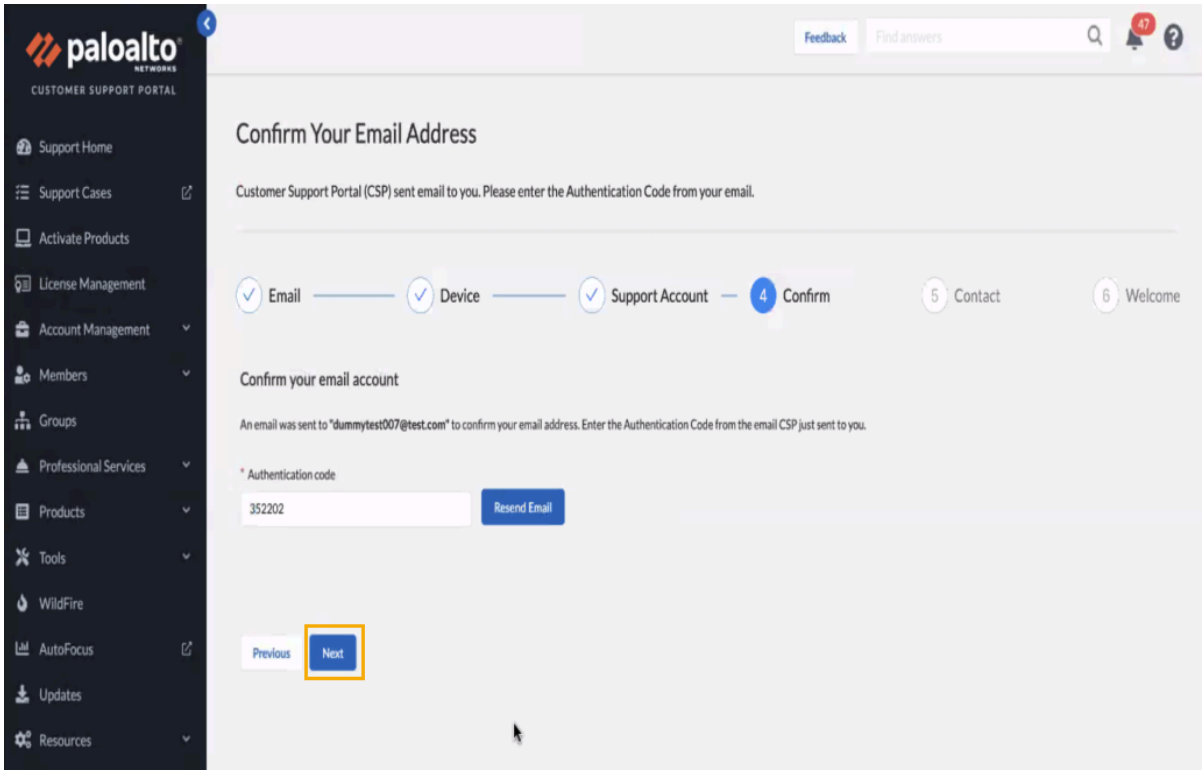



Möglicherweise werden Sie aufgefordert, Ihre Adresse für das neue Supportkonto zu bestätigen. Bestätigen Sie gegebenenfalls Ihre Adresse und klicken Sie auf **OK**, um eine Authentifizierungsanfrage an die angegebene E-Mail-Adresse zu senden.

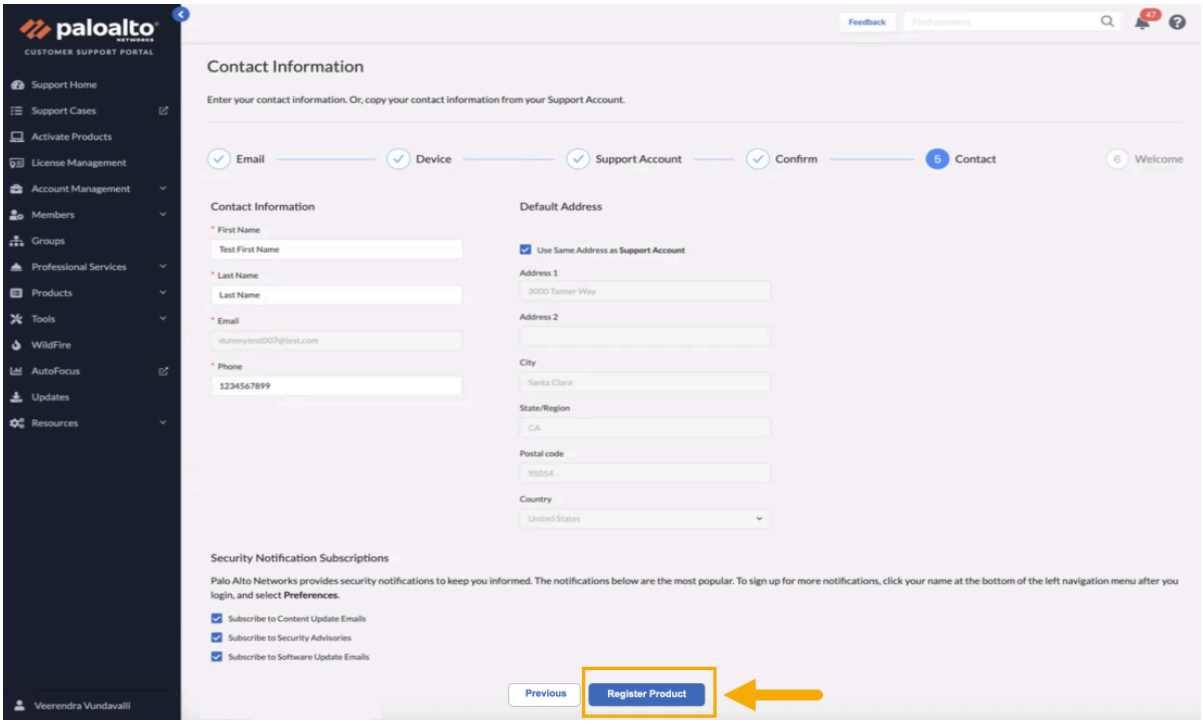
**STEP 8 |** Suchen Sie in Ihrer E-Mail nach dem Authentifizierungscode. Geben Sie den **Authentifizierungscode** ein und klicken Sie dann auf **Next (Weiter)**.




**STEP 9 |** Bestätigen Sie Ihre E-Mail-Adresse für Ihr Customer-Support-Portal-Konto und klicken Sie dann auf **Next (Weiter)**.

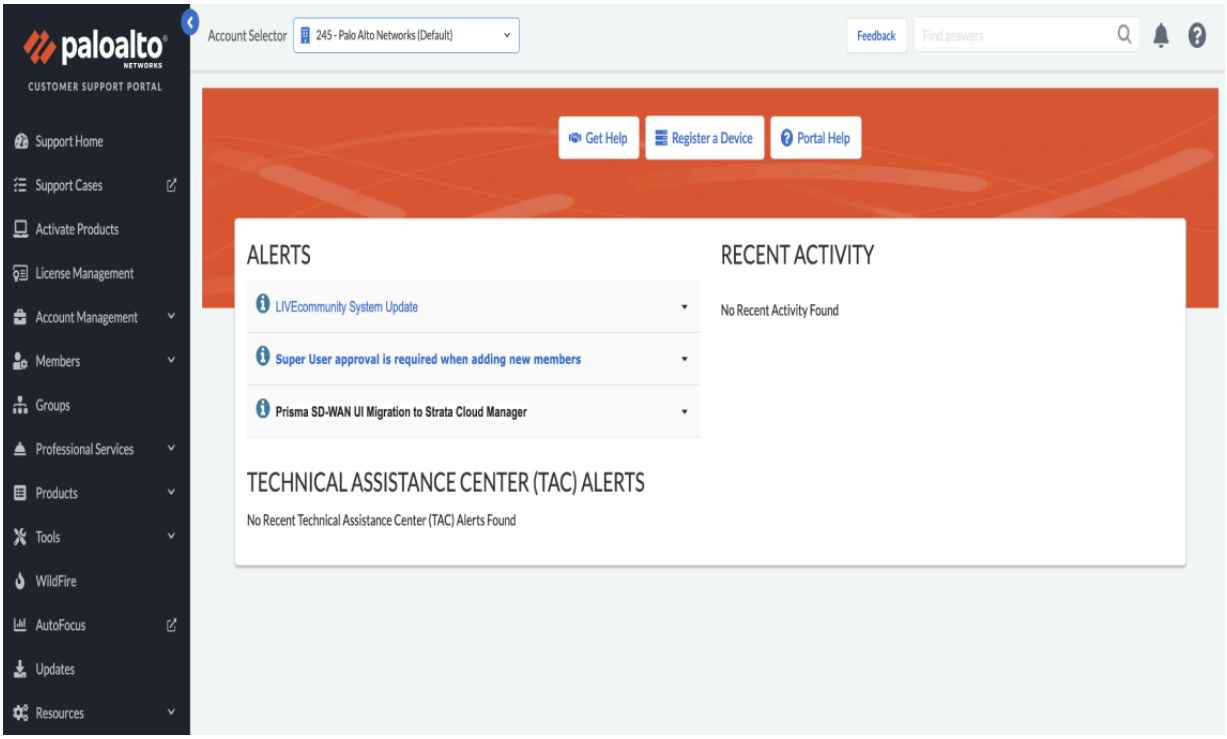
 

**STEP 10 |** Bestätigen Sie Ihre **Kontaktinformationen**. Wählen Sie Ihre **Abonnements für Sicherheitsbenachrichtigungen** aus und klicken Sie dann auf **Register Product (Produkt registrieren)**




Sobald die Registrierung abgeschlossen ist, wird ein Bestätigungsfenster und anschließend die Seite des Customer Support Portals angezeigt:



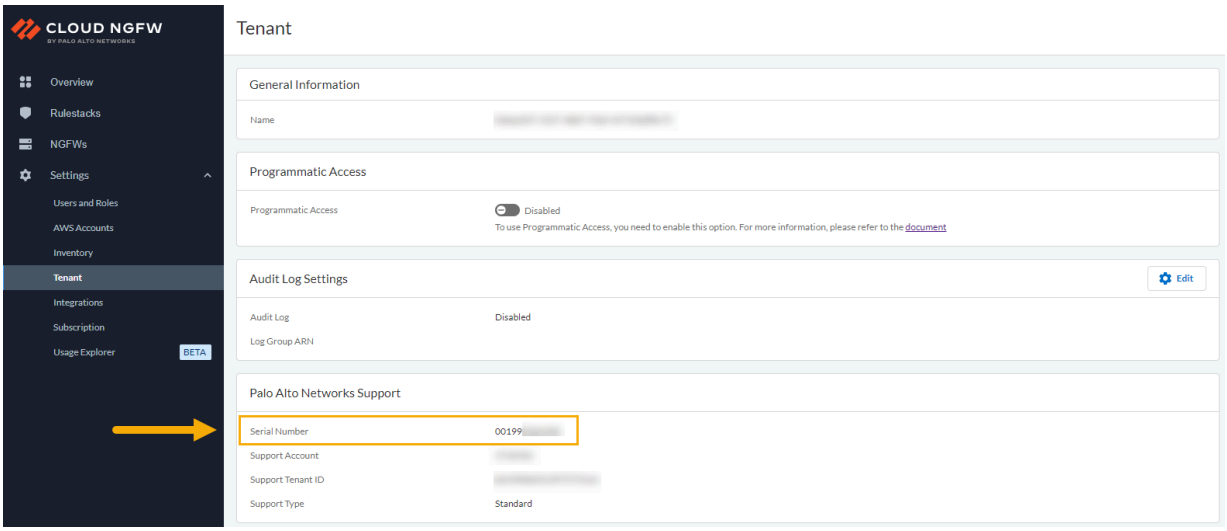

# Ihre Seriennummer für Cloud NGFW für AWS suchen

So finden Sie die Cloud NGFW-Seriennummer:

**STEP 1 |** Melden Sie sich beim Cloud NGFW-Mandanten an.

**STEP 2 |** Klicken Sie auf **Tenant (Mandant)**. Auf der Seite „Tenant“ (Mandant) werden die **Seriennummer** und zusätzliche Informationen im Abschnitt **Palo Alto Networks Support** angezeigt.

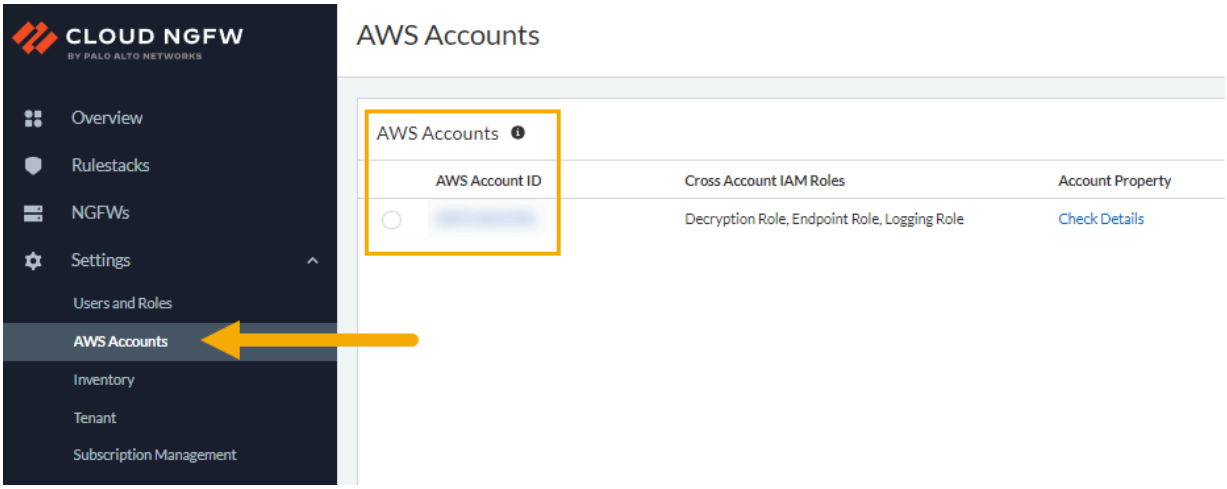



## Supportfall erstellen

So erstellen Sie einen Supportfall mithilfe der Cloud NGFW-Konsole:

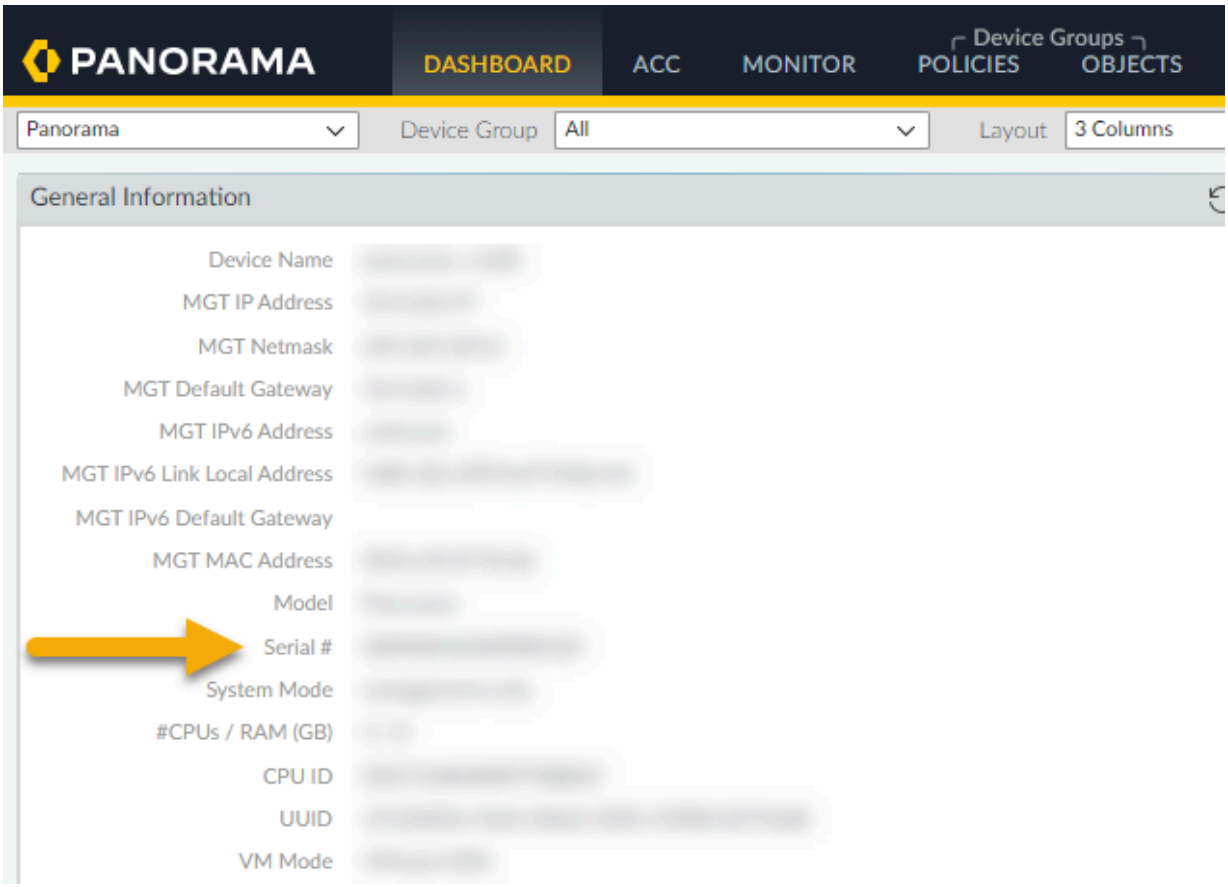
**STEP 1 |** Suchen Sie Ihre **AWS-Konto-ID**. Wählen Sie **AWS Accounts (AWS-Konten)** aus.



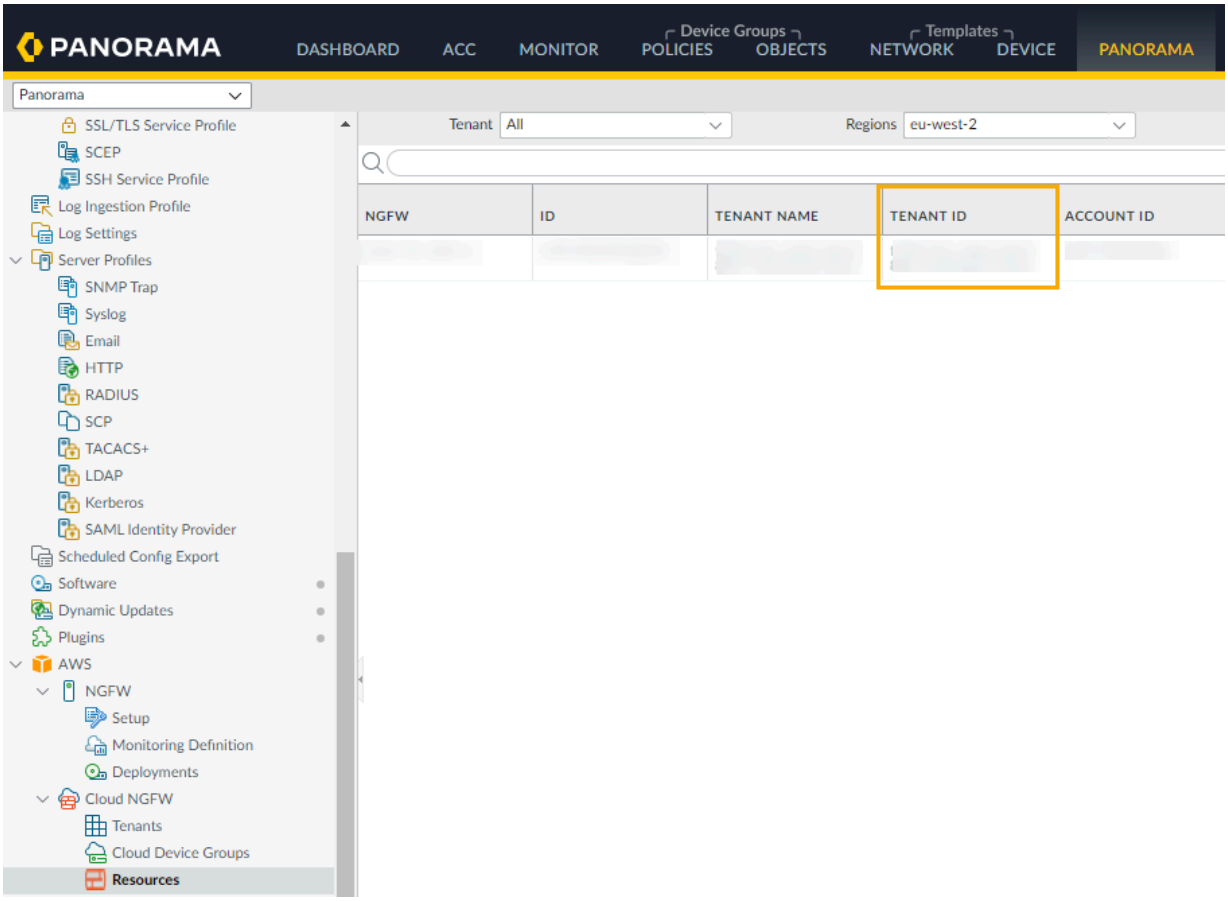
**STEP 2 |** Verwenden Sie bei Bedarf die Panorama-Konsole, um zusätzliche Informationen für den Supportfall zu ermitteln, beispielsweise die Mandanten-ID oder die Panorama-Seriennummer.

Suchen Sie die **Panorama-Seriennummer** mithilfe des **Dashboards**:




Suchen Sie die **Mandanten-ID** für die Cloud NGFW-Ressource:

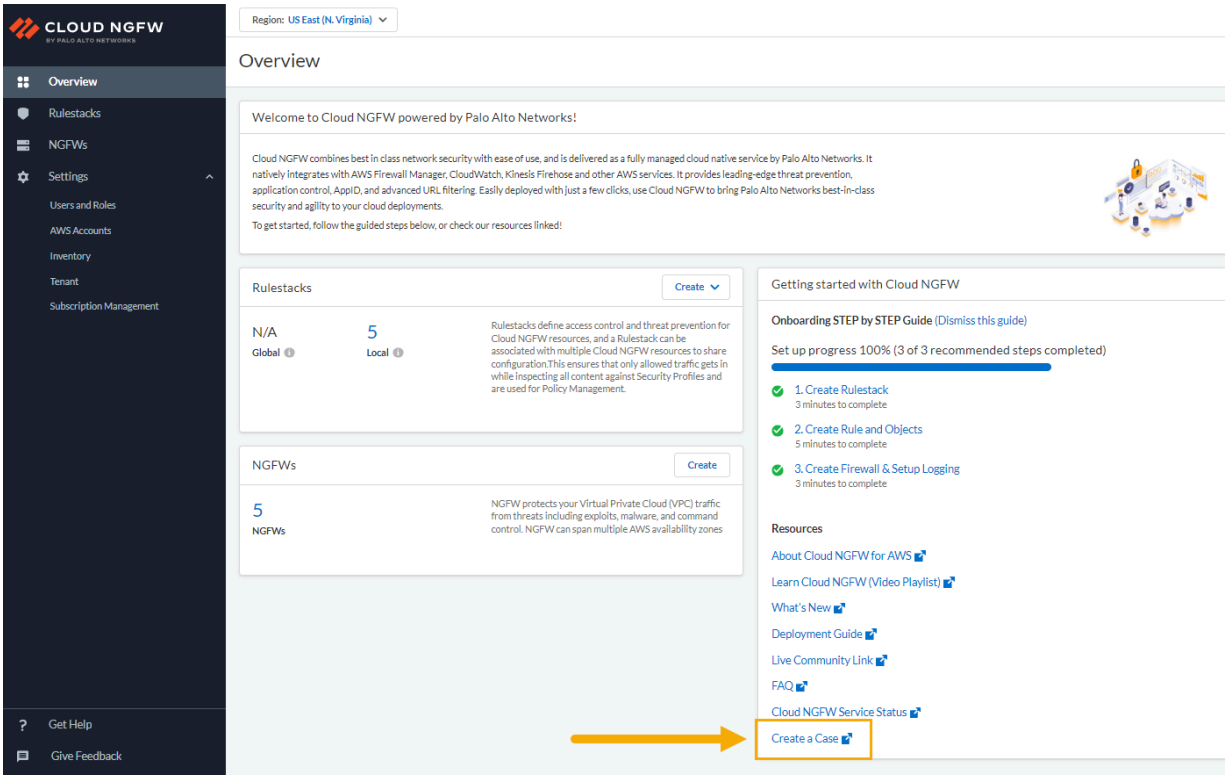
 



**STEP 3 |** Klicken Sie auf der Seite **Overview (Übersicht)** in der Cloud NGFW-Konsole auf **Create a case (Fall erstellen)**.



# Usage Explorer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

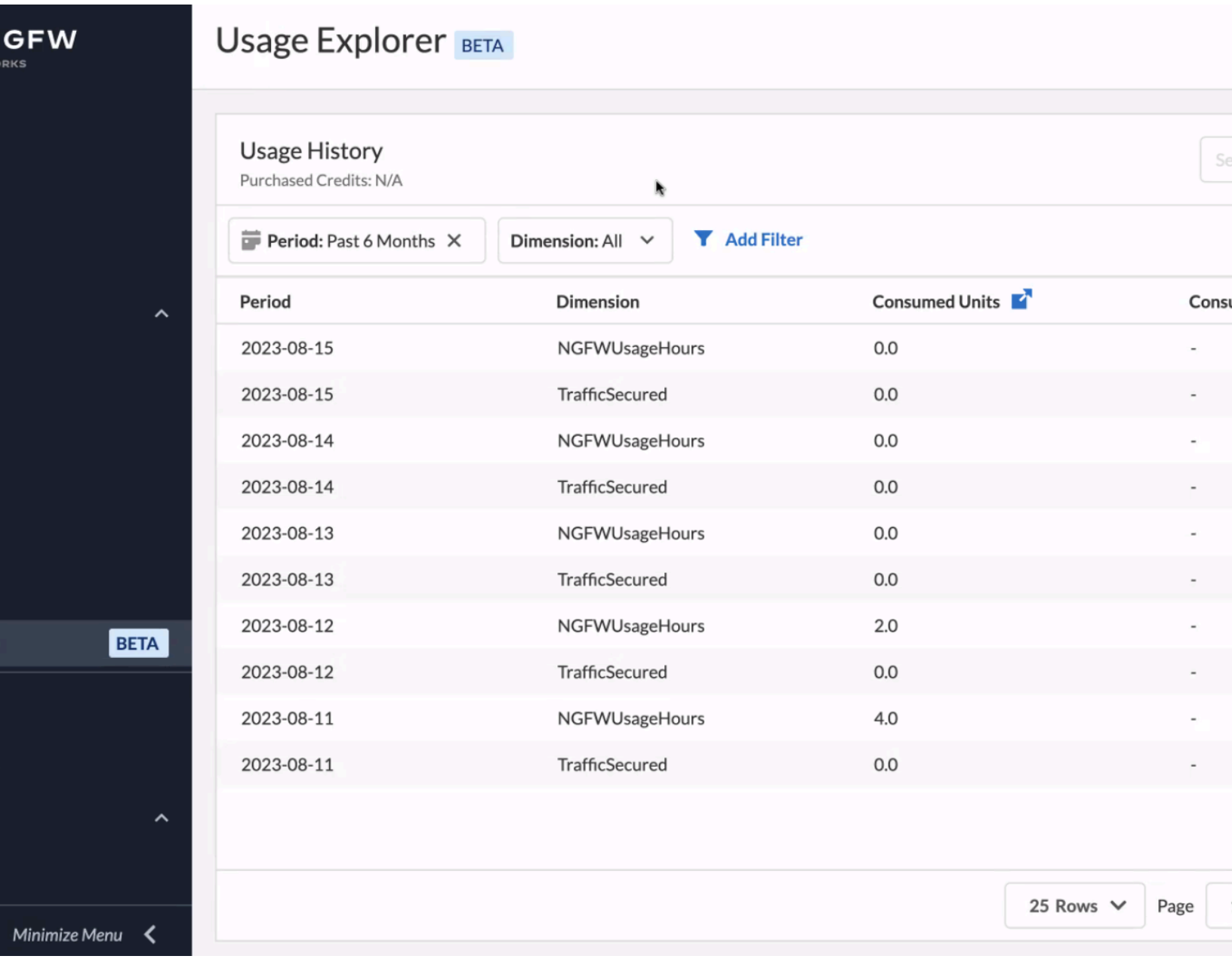
Das Dashboard von Usage Explorer bietet eine schnelle und komfortable Möglichkeit, den Cloud NGFW-Verbrauch für einen Mandanten für nutzungsbasierte Bezahlung (Pay-as-you-go, PAYG) und kreditbasierte Abonnements (die über einen Vertrag erworben wurden) zu ermitteln. Diese Informationen zeigen einen täglichen Verbrauch an, der Einblicke in Ihren durchschnittlichen Verbrauch und die Korrelation mit Cloud NGFW-Credits enthält, die dem Mandanten zugeordnet sind.

*Die Funktion Usage Explorer ist derzeit als Vorschau verfügbar.*

So greifen Sie auf den Usage Explorer zu:

1. Stellen Sie eine Verbindung zur Cloud NGFW-Konsole her.
2. Wählen Sie in der Konsole die Option **Usage Explorer** aus.




Der Usage Explorer enthält Optionen zum Anzeigen des Verbrauchs über einen bestimmten Zeitraum und ermöglicht es Ihnen, eine CSV-Datei herunterzuladen, um relevante Daten für zukünftige Überprüfungen zu erfassen. Der tägliche Verbrauchsverlauf wird in einer Tabelle bereitgestellt, die die folgenden Felder enthält:

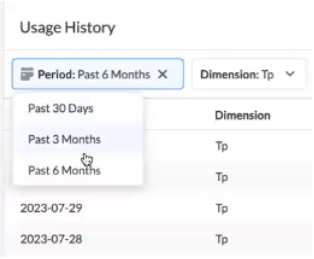
- Period (Zeitraum): Stellt den Zeitrahmen für den Cloud NGFW-Verbrauch dar.
- Dimension: Wird verwendet, um die Abrechnung für eine Cloud NGFW zu identifizieren. Eine Dimension bezieht sich auf ein Add-on (z. B. Threat Prevention).
- Consumed Units (Verbrauchte Einheiten): Die Menge der Ressource, die vom Mandanten während des Abrechnungszeitraums verbraucht wurde. Dieses Feld ist für das PAYG-Abonnementmodell relevant.

- Consumed as Credits (Als Credits verbraucht): Die Menge der Ressource, die vom Mandanten während des Abrechnungszeitraums verbraucht wurde. Dieses Feld ist für das PAYG-Abonnementmodell relevant.

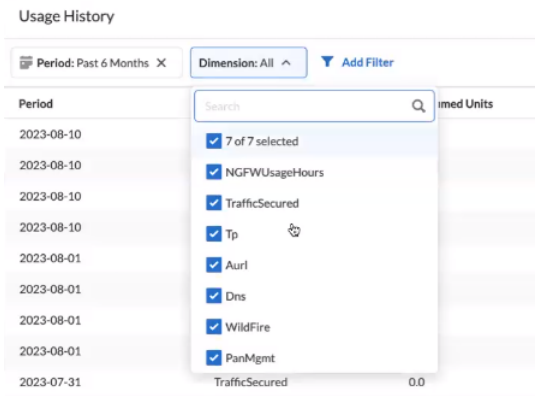
*Sie können nur nach unterstützten Dimensionen filtern. Die Option **Add filter (Filter hinzufügen)** funktioniert derzeit nicht in dieser Vorschauversion.*

Verwenden Sie die Schaltfläche **Period (Zeitraum)**, um den Verbrauch über einen bestimmten Zeitraum anzuzeigen. Wenn Sie diese Option verwenden, beachten Sie, dass das Filtern des Verbrauchs über längere Zeiträume zu Verzögerungen bei der Anzeige von Daten führen kann:




*Standardmäßig zeigt Usage Explorer Verbrauchsdaten für die letzten 30 Tage an.*

Mit der Option **Dimensions (Dimensionen)** können Sie die Anzeige von Usage Explorer so ändern, dass nur die Add-on-Dimensionen angezeigt werden, die Teil Ihres Abonnements sind. Sie können nach allen Dimensionen filtern oder im Dropdown-Menü eine Dimension auswählen:



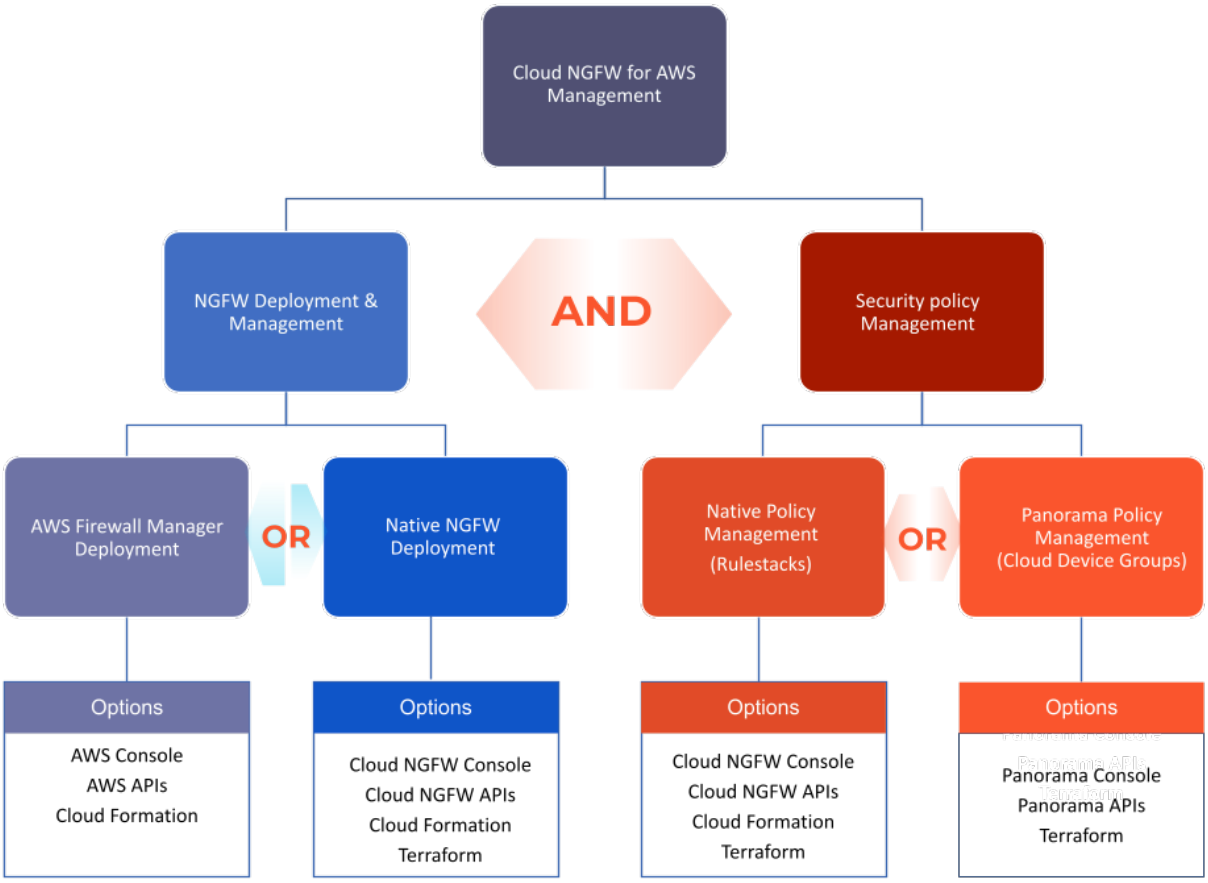

*Die Anzeige von Usage Explorer unterscheidet sich je nach Modell des Cloud NGFW-Mandantenabonnements (entweder PAYG oder als Vertrag).*

# Bereitstellen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW für AWS bietet mehrere Optionen zum Bereitstellen von NGFW-Ressourcen und Verwalten von Sicherheitsrichtlinienregeln.



**NGFW-Bereitstellung und -Verwaltung**

- **Native NGFW-Bereitstellung** – Wenn Sie Cloud NGFW über AWS Marketplace abonnieren, erwerben Sie einen Mandanten. Anschließend können Sie Cloud NGFW-Ressourcen mit wenigen Klicks auf der Cloud NGFW-Konsole oder mithilfe von APIs für Ihre VPCs bereitstellen. Diese Ressourcen bieten integrierte Ausfallsicherheit, Skalierbarkeit und Lebenszyklusverwaltung. Sie können zum Erstellen dieser Ressourcen auch Infrastructure-as-Code-Tools wie CloudFormation oder Terraform verwenden. Nach dem Erstellen können Sie Sicherheitsrichtlinienregeln für diese Cloud NGFW-Ressourcen mithilfe der nativen Richtlinienverwaltung (Regelstapel) oder der Panorama-Richtlinienverwaltung (Gerätegruppen) verfassen.
- **Bereitstellung von AWS Firewall Manager** – Wenn Sie derzeit AWS Firewall Manager zum Verwalten von Sicherheitsgruppen oder anderen Netzwerksicherheitsfunktionen in Ihrer AWS-Organisation verwenden, können Sie denselben AWS Firewall Manager zum Bereitstellen von NGFWs in mehreren Konten und VPCs in einer AWS-Organisation verwenden. Sie können die AWS-Konsole, AWS-APIs oder CloudFormation verwenden, um die Richtlinienkonfiguration für Firewall Manager zu erstellen, die alle Cloud NGFW-Einstellungen bereitstellt und verwaltet.

  AWS Firewall Manager verwaltet außerdem die Endpunkt-Subnetze, Routentabellen und Gateway-Load-Balancer-Endpunkte innerhalb der VPC, in der die Cloud NGFW-Ressource bereitgestellt wird. Wenn Sie AWS Firewall Manager verwenden, nutzt die Cloud NGFW-Ressource globale Regelstapel in Ihrem Cloud NGFW-Mandanten für die Sicherheitseinstellungen und -regeln. Wenn Sie zuvor keinen globalen Regelstapel in Ihrem Mandanten konfiguriert haben (mithilfe der Panorama-Richtlinienverwaltung), leitet AWS Firewall Manager Sie zur Cloud NGFW-Konsole weiter, um den globalen Regelstapel mithilfe der nativen Richtlinienverwaltung zu erstellen und zu verwalten.

**Verwaltung von Sicherheitsrichtlinien**

- **Native Richtlinienverwaltung** – Sie können Sicherheitsrichtlinienregeln für die Cloud NGFW-Ressourcen verwalten, indem Sie Regelstapel nativ mithilfe der Cloud NGFW-Konsole oder mit APIs erstellen. Sie können zum Erstellen dieser Regelstapel auch Infrastructure-as-Code-Tools wie CloudFormation oder Terraform verwenden. Ein Regelstapel definiert die erweiterte Zugriffskontrolle (App-ID, URL-Filterung) und das Bedrohungspräventionsverhalten der NGFW. Ein Regelstapel enthält eine Reihe von Sicherheitsregeln sowie die verknüpften Objekte und Sicherheitsprofile.
- **Panorama-Richtlinienverwaltung** – Sie können Ihren Cloud NGFW-Mandanten mit einer Panorama-Appliance verknüpfen, um Richtlinienregeln für Ihre Cloud NGFW-Ressourcen zu erstellen und zu verwalten. Sie können die Panorama-Konsole, APIs oder Terraform verwenden, um diese Sicherheitsrichtlinien für die Cloud-Gerätegruppen zu erstellen. Die Richtlinie, die Sie in der Panorama Cloud-Gerätegruppe erstellen, wird als globaler Regelstapel in Ihrem Cloud NGFW-Mandanten manifestiert.
- **Strata Cloud Manager für die Richtlinienverwaltung** – Sie können Ihre Cloud NGFW-Ressource mit Strata Cloud Manager (SCM) für die Richtlinienverwaltung verknüpfen. Strata Cloud Manager bietet eine einheitliche Verwaltungslösung für Ihre gesamte Netzwerksicherheitsbereitstellung, sodass Sie Ihre Palo Alto Networks Sicherheitsinfrastruktur einfach von einer einzigen optimierten Weboberfläche aus verwalten können. Mit dieser Oberfläche erhalten Sie einen umfassenden Überblick über Benutzer, Zweigstellen, Anwendungen und Bedrohungen an allen Punkten zur Durchsetzung der Netzwerksicherheit. Diese Funktion bietet umsetzbare Erkenntnisse, höhere Sicherheit sowie einfache Fehlerbehebung und Problemlösung.

# NGFW-Ressource in AWS erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Nachdem Sie Regelstapel und Regeln erstellt haben, können Sie eine NGFW-Ressource erstellen und ihr einen lokalen Regelstapel zuordnen. Während der Konfiguration Ihrer NGFW müssen Sie auswählen, wie NGFW-Endpunkte erstellt werden: automatisch oder manuell. Wenn Sie NGFW-Endpunkte manuell erstellen, müssen Sie NGFW-Endpunkte in den von Ihnen angegebenen Verfügbarkeitszonen erstellen.

Führen Sie die folgenden Schritte aus, um eine NGFW zu erstellen.

**STEP 1 |** Wählen Sie **NGFWs** aus.

**STEP 2 |** Klicken Sie auf **Add Firewall (Firewall hinzufügen)**.

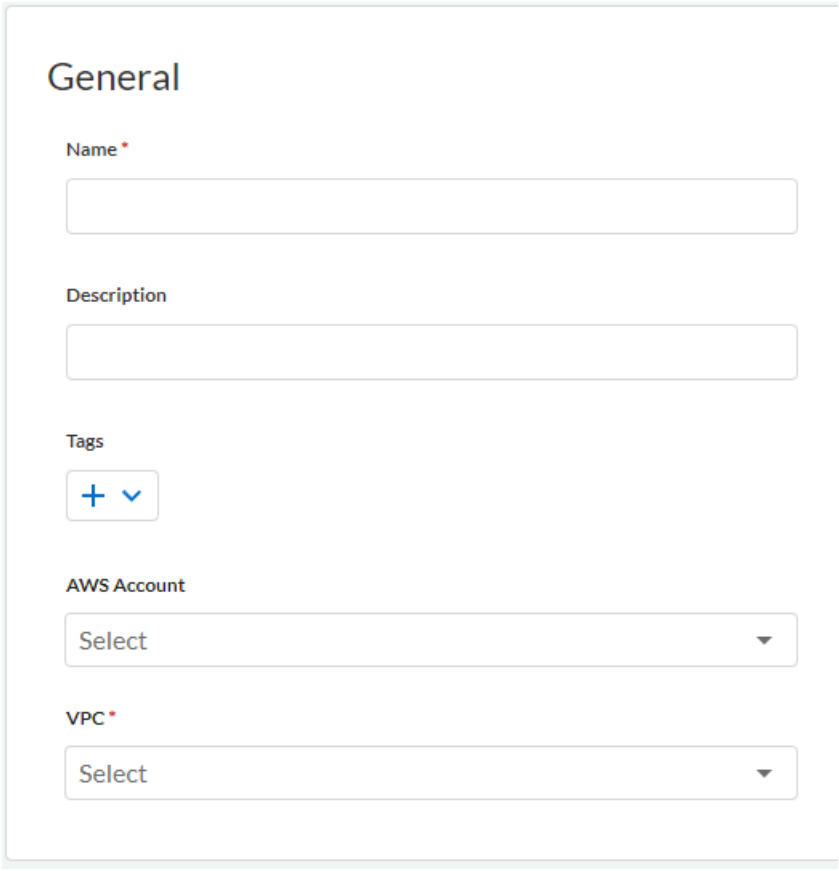
**STEP 3 |** Geben Sie einen beschreibenden **Namen** ein.

**STEP 4 |** (optional) Geben Sie eine **Beschreibung** ein.

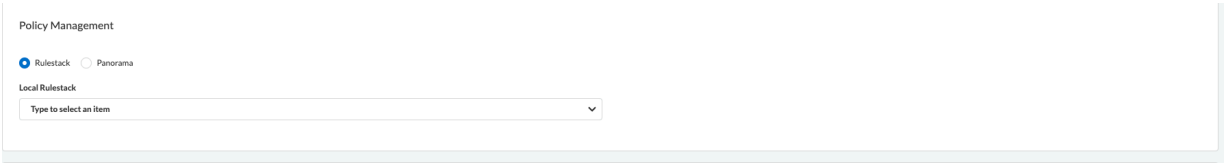
**STEP 5 |** Wählen Sie ein **AWS-Konto** aus der Dropdown-Liste aus, das dieser NGFW zugeordnet werden soll.

**STEP 6 |** Wählen Sie eine **VPC** aus der Dropdown-Liste aus.




**STEP 7 |** Wählen Sie im Abschnitt **Policy Management (Richtlinienverwaltung)** aus der Dropdown-Liste einen **lokalen Regelstapel** aus.




**STEP 8 |** Geben Sie AWS-Verfügbarkeitszonen oder Subnetze an. Geben Sie an, ob der Cloud NGFW-Mandant NGFW-Endpunkte bereitstellen wird (dienstverwalteter Modus) oder nicht (kundenverwalteter Modus).

- **Yes (Ja)** (dienstverwaltet): Im dienstverwalteten Modus erstellt der Cloud NGFW-Mandant automatisch NGFW-Endpunkte in den von Ihnen angegebenen VPC-Subnetzen. Führen Sie die Endpunktverwaltung für den dienstverwalteten Modus nur über die Cloud NGFW-Konsole durch.

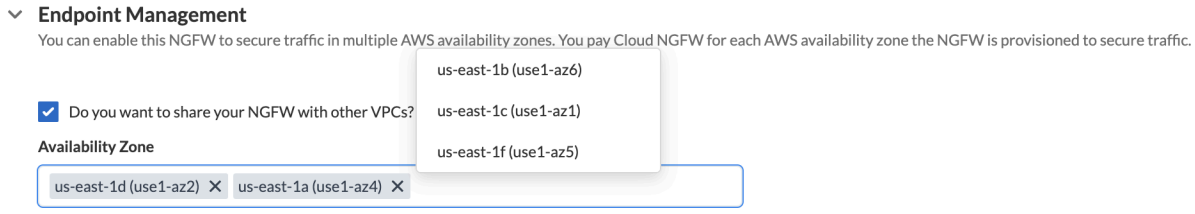
 

Die Endpunktverwaltung für den dienstverwalteten Modus kann nur durch Zuordnen oder Aufheben der Zuordnung eines Subnetzes erfolgen. Durch die Zuordnung eines Subnetzes wird der Endpunkt erstellt und durch die Aufhebung der Zuordnung eines Subnetzes wird der Endpunkt entfernt.

- **No (Nein)** (kundenverwaltet): Im kundenverwalteten Modus müssen Sie NGFW-Endpunkte in jeder von Ihnen angegebenen Verfügbarkeitszone manuell erstellen.

*Im Abschnitt **Endpoint Management (Endpunktverwaltung)** können Sie Ihre Cloud NGFW aktivieren, um den Datenverkehr in mehreren AWS-Verfügbarkeitszonen zu sichern. Sie zahlen für jede AWS-Verfügbarkeitszone, in der Ihre NGFW zur Sicherung des Datenverkehrs bereitgestellt wird. Sie können verwalten, wie die Endpunkte für Ihre NGFW in diesen Verfügbarkeitszonen erstellt werden. Sie zahlen AWS für jeden VPC-Endpunkt (Gateway Load Balancer), den Sie für Ihre NGFW erstellen.*

Die **Verfügbarkeitszone** zeigt die **Zonen-ID** und den entsprechenden **Verfügbarkeitszonennamen** in Ihrem Palo Alto Networks Konto an. Verwenden Sie diese Informationen, wenn Sie Ihre Verfügbarkeitszonen Ihren AWS-Konten zuordnen.




**STEP 9 |** Klicken Sie auf **Create (Erstellen)**.

# Cloud NGFW für AWS-Endpunkte erstellen

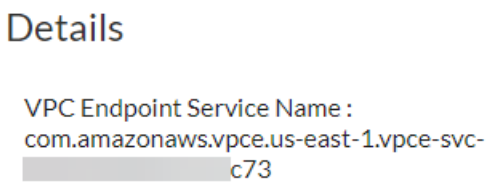
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Wenn Sie beim Erstellen einer NGFW den kundenverwalteten Modus ausgewählt haben, müssen Sie die NGFW-Endpunkte für Ihre ausgewählten Subnetze manuell erstellen. In der AWS-Konsole werden NGFW-Endpunkte als Gateway-Load-Balancer-Endpunkte angezeigt.

Die Subnetze, an die Sie NGFW-Endpunkte anfügen, müssen sich in der virtuellen privaten Cloud (VPC) befinden, die Sie während der NGFW-Erstellung angegeben haben.

**STEP 1 |** Wählen Sie im Cloud NGFW-Mandanten **NGFWs** aus und klicken Sie auf Ihre Firewall.

**STEP 2 |** Wählen Sie **Endpoints (Endpunkte)** aus und notieren Sie sich den Dienstnamen des VPC-Endpunkts.




**STEP 3 |** Melden Sie sich bei der AWS-Konsole an.

**STEP 4 |** Wählen Sie **Services (Dienste)** > **Networking & Content Delivery (Netzwerk- und Inhaltsbereitstellung)** > **VPC** aus.

**STEP 5 |** Wählen Sie im VPC-Dashboard **Endpoints (Endpunkte)** > **Create Endpoint (Endpunkt erstellen)** aus.

**STEP 6 |** Wählen Sie **Find service by name (Dienst anhand des Namens suchen)** aus, der dem oben notierten Dienstnamen des VPC-Endpunkts entspricht.

**STEP 7 |** Wählen Sie die **VPC**, die Sie während der Firewall-Erstellung angegeben haben, aus der Dropdown-Liste aus.

**STEP 8 |** Wählen Sie die Subnetze aus, in denen Sie NGFW-Endpunkte erstellen möchten.

**STEP 9 |** Klicken Sie auf **Create endpoint (Endpunkt erstellen)**.

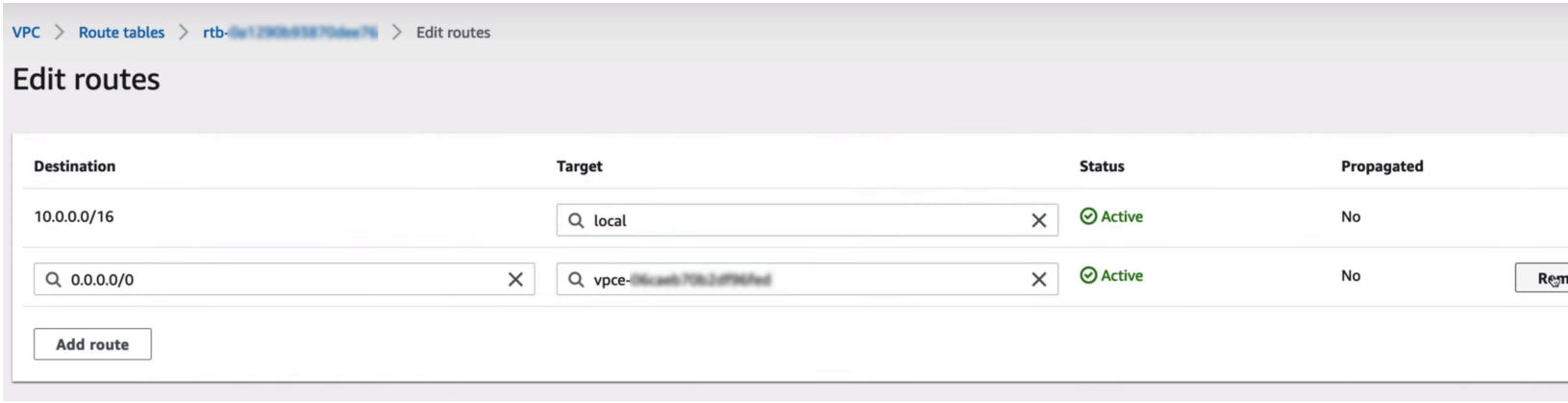
# Cloud NGFW-Ressource löschen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Wenn Sie eine Cloud NGFW-Ressource nicht mehr benötigen, gehen Sie wie folgt vor, um sie aus Ihrer AWS-Bereitstellung zu entfernen.

**STEP 1 |** Entfernen Sie zugeordnete Cloud NGFW-Endpunkte aus Ihren Routentabellen.

1. Melden Sie sich bei der AWS-Konsole an.
2. Wählen Sie **VPC** aus und suchen Sie die VPC, die den Cloud NGFW-Endpunkt enthält.
3. Wählen Sie **Route Tables (Routentabellen)** und anschließend die Routentabelle des zu entfernenden Endpunkts aus.




4. Klicken Sie auf **Edit Routes (Routen bearbeiten)**.
5. Klicken Sie auf **Remove (Entfernen)**, um die Route aus der Routentabelle zu löschen.
6. Klicken Sie auf **Save Changes (Änderungen speichern)**.

**STEP 2 |** (Nur kundenverwaltete Endpunkte) Wenn Sie Ihre eigenen Cloud NGFW-Endpunkte bereitgestellt haben, müssen Sie diese aus der AWS-Konsole löschen.

1. Wählen Sie in der AWS-Konsole **Endpoints (Endpunkte)** und dann Ihren Cloud NGFW-Endpunkt aus.
2. Wählen Sie **Actions (Aktionen)** > **Delete (Löschen)** aus und bestätigen Sie den Löschvorgang.

**STEP 3 |** Entfernen Sie die Cloud NGFW-Ressource aus dem Cloud NGFW-Mandanten.

1. Melden Sie sich bei der Cloud NGFW-Konsole an und wählen Sie **NGFWs** aus.
2. Wählen Sie die zu löschende Ressource aus.
3. Klicken Sie in der Dropdown-Liste **Actions (Aktionen)** auf **Delete (Löschen)**.
4. **Bestätigen** Sie den Löschvorgang.

   Nach einigen Minuten werden die Cloud NGFW-Ressource und alle ihre Endpunkte aus Ihrer Cloud NGFW-Bereitstellung gelöscht.

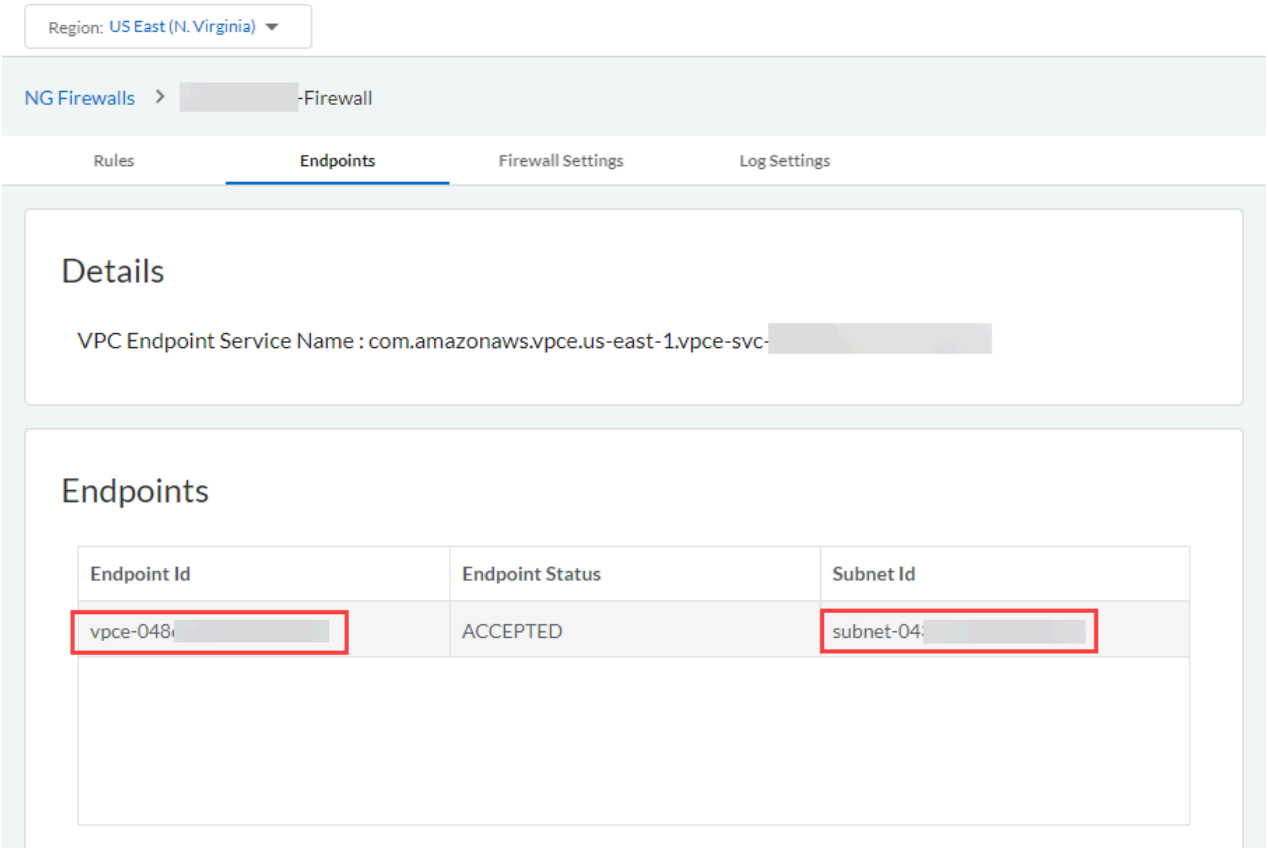
 

# Datenverkehr zu Cloud NGFW für AWS leiten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Nachdem Sie Cloud NGFW bereitgestellt und Endpunkte erstellt haben, müssen Sie Ihre Routing-Tabellen aktualisieren, um Datenverkehr an Ihre Firewall zu senden. Welche Routing-Tabellen aktualisiert werden und wie dies geschieht, hängt von Ihrer spezifischen Bereitstellung ab.

In der AWS-Konsole werden NGFW-Endpunkte als Gateway Load Balancer-Endpunkte angezeigt. Sie können die NGFW-Endpunkte in der AWS-Konsole anhand ihrer Endpunkt-ID identifizieren. Sie finden die Endpunkt-IDs für eine bestimmte Firewall in der Cloud NGFW-Konsole unter **NGFWs** > **firewall-name (Firewallname)** > **Endpoints (Endpunkte)**.




Nachfolgend sind Beispiele für Paketflüsse in verschiedenen Bereitstellungsmodi sowie Beispiele der aktualisierten Routen für diese Paketflüsse aufgeführt.

- Zentralisierte Bereitstellungen in Cloud NGFW für AWS
- Verteilte Bereitstellungen in Cloud NGFW für AWS

# Privaten Datenverkehrsbereich konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Mit Cloud NGFW können Sie den privaten Datenverkehrsbereich für jeden Endpunkt festlegen. Standardmäßig umfassen die Präfixe für den privaten Datenverkehrsbereich die für VPC zulässigen IP-Adressbereiche wie in IANA RFC 1918 angegeben. Ihr Hybrid-Cloud-Netzwerk könnte jedoch zusätzlich den freigegebenen Adressraum gemäß IANA RFC 6598 oder einen bestimmten Satz öffentlich routbarer CIDR-Blöcke in den Präfixen für den privaten Datenverkehrsbereich umfassen.

So konfigurieren Sie private Datenverkehrsbereiche:

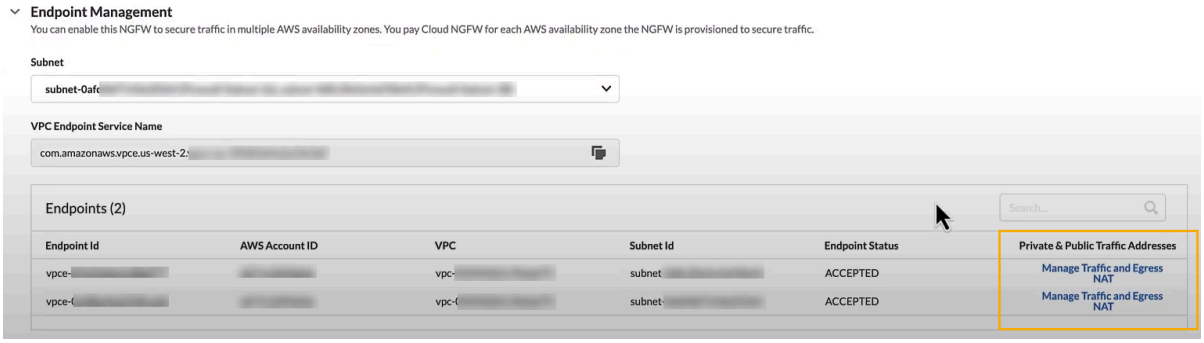
**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Klicken Sie auf **NGFWs**.

**STEP 3 |** Wählen Sie im Abschnitt „Endpoint Management“ (Endpunktverwaltung) das Subnetz aus dem Dropdown-Menü aus.

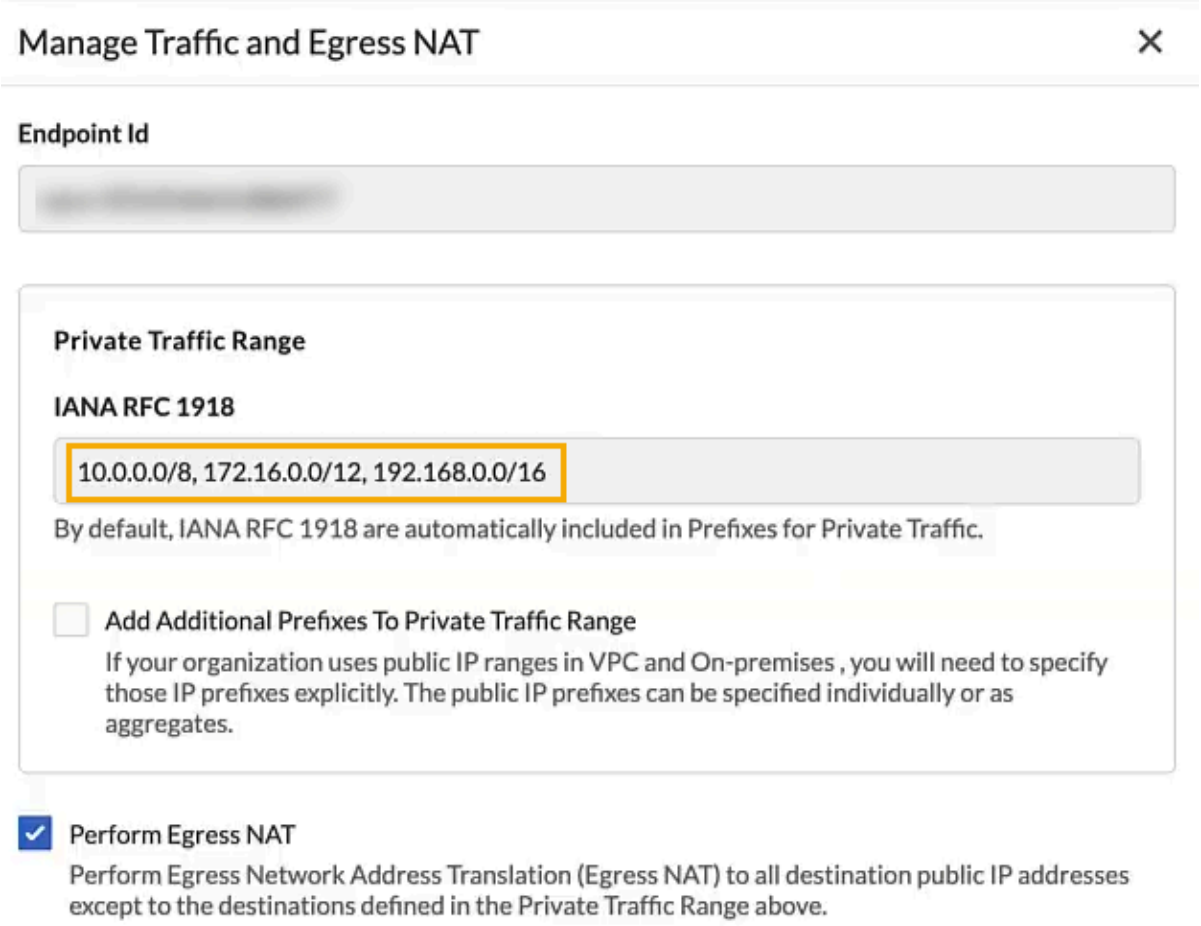
 

**STEP 4 |** Wählen Sie in der Tabelle **Endpoints (Endpunkte)** die Option **Manage Traffic and Egress NAT (Datenverkehr und Ausgangs-NAT)** für den entsprechenden Endpunkt aus:



**STEP 5 |** Geben Sie auf dem Bildschirm **Manage Traffic and Egress NAT (Datenverkehr und Ausgangs-NAT)** die IP-Adresse (oder die IP-Adressen) an, die Sie explizit einschließen möchten:




**STEP 6 |** Aktivieren Sie das Kontrollkästchen **Add Additional Prefixes to Private Traffic Range (Zusätzliche Präfixe zum privaten Datenverkehrsbereich hinzufügen)**.

**STEP 7 |** Aktivieren Sie das Kontrollkästchen **Perform Egress NAT (Ausgangs-NAT ausführen)**, um sicherzustellen, dass die Adressübersetzung für alle öffentlichen IP-Adressziele erfolgt, mit Ausnahme derjenigen, die im privaten Datenverkehrsbereich angegeben sind.

**STEP 8 |** Klicken Sie auf **Save (Speichern)**.

# Ausgangs-NAT konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW bietet zwei Möglichkeiten, Quell-NAT für ausgehenden Datenverkehr zu Zielen im öffentlichen Internet durchzuführen: AWS-NAT-Gateway und Cloud NGFW-Ausgangs-NAT.

*Ausgangs-NAT-Funktionalitäten werden auf vorhandenen Firewalls (die vor dieser Version von Cloud NGFW für AWS erstellt wurden) nicht unterstützt. Erstellen Sie eine neue Firewall, um Ausgangs-NAT verwenden zu können.*

## AWS-NAT-Gateway

Das Amazon-NAT-Gateway ermöglicht es Ihren VPC-Ressourcen in Ihren privaten Subnetzen, sicher auf Dienste außerhalb des Subnetzes zuzugreifen, einschließlich des öffentlichen Internets, während private Ressourcen für unerwünschten Datenverkehr zugänglich bleiben.

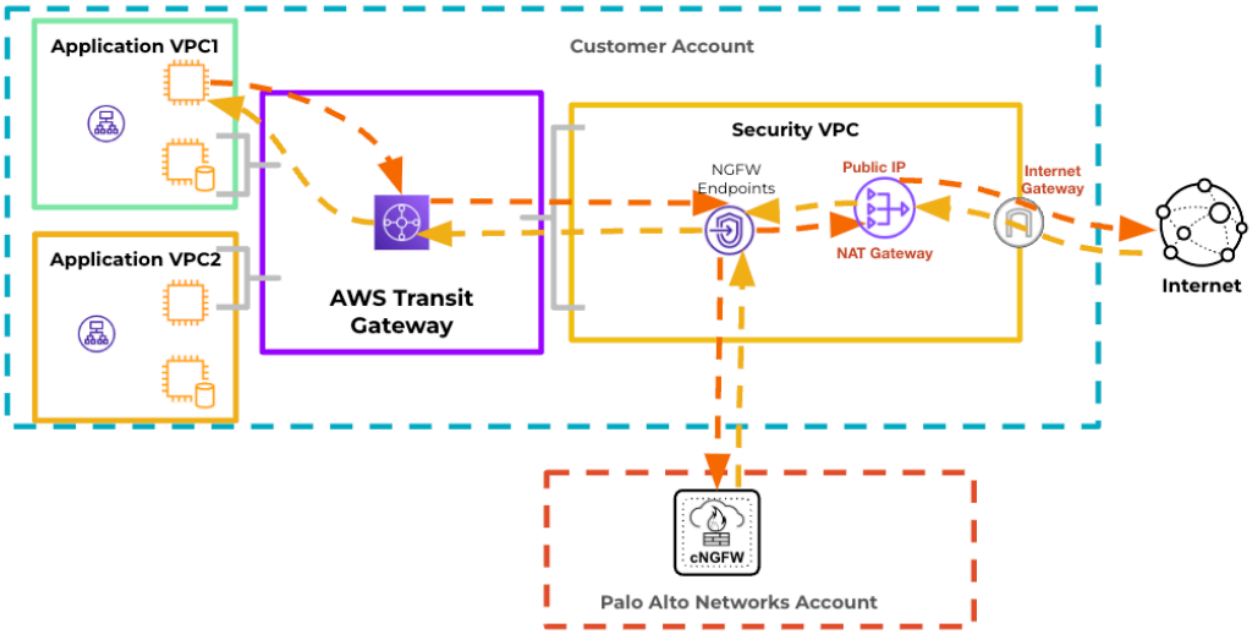
Sie können das AWS-NAT-Gateway in Ihrem VPC weiterhin verwenden. In diesem Szenario übernimmt die Cloud NGFW die Aufgabe eines Bump-in-the-Wire und leitet den gesamten geprüften Datenverkehr zurück an seinen Endpunkt.

*Sie bezahlen AWS für das NAT-Gateway und die damit verbundenen Ausgangs-Datenübertragungskosten.*

*Ausgangs-NAT wird auf Strata-Cloud-Manager(SCM)-Firewalls nicht unterstützt.*

Die folgende Abbildung veranschaulicht Quell-NAT auf internetgebundenem Datenverkehr mit dem AWS-NAT-Gateway:




*Informationen zur Verwendung von AWS zum Konfigurieren von NAT finden Sie im Abschnitt* Work with NAT Gateways.

## Cloud NGFW-Ausgangs-NAT

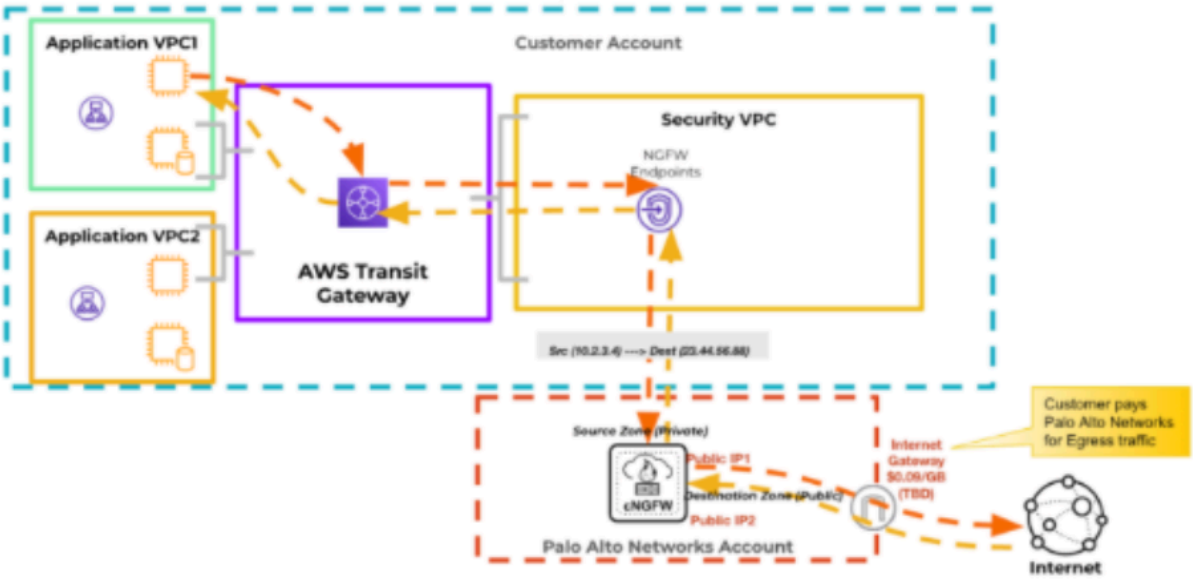
Alternativ konfigurieren Sie die Ausgangs-NAT-Funktion. In diesem Fall führt Cloud NGFW Quell-NAT für den gesamten ausgehenden Datenverkehr aus, mit Ausnahme derjenigen Sitzungen mit Ziel-IP-Adressen innerhalb der für den Endpunkt definierten Präfixe für privaten Datenverkehrsbereich, auf dem der Datenverkehr in die Cloud NGFW-Ressource eintritt. In diesem Fall leitet die Cloud NGFW-Ressource den geprüften Datenverkehr nicht zum Endpunkt zurück. Alternativ wird der geprüfte Ausgangsdatenverkehr direkt ins Internet gesendet. Es entstehen Ihnen keine AWS-NAT-Gateway-Kosten mehr, sondern Sie bezahlen Palo Alto Networks für die ausgehende Datenübermittlung. Sie ordnen der Cloud NGFW-Ressource jedoch öffentliche IP-Adressen auf zwei Arten zu:

1. Konfigurieren Sie die Cloud NGFW-Ressource so, dass die von Palo Alto Networks verwalteten AWS Elastic-IP-Address(EIP)-Adressen verwendet werden, um Quell-NAT für Ihren VPC durchzuführen. In diesem Fall entstehen Ihnen stündliche EIP-Verwaltungskosten.

2. Übertragen Sie Ihre BYOIPs von Ihrem AWS-Konto in die Cloud NGFW, um die stündlichen EIP-Verwaltungskosten zu vermeiden. Weitere Informationen finden Sie unter BYOIPs with AWS IPAM.

Die folgende Abbildung veranschaulicht, wie Quell-NAT auf internetgebundenem Datenverkehr mit Cloud NGFW-Ausgangs-NAT funktioniert. Quell-NAT auf internetgebundenem Datenverkehr mit Cloud NGFW-Ausgangs-NAT:



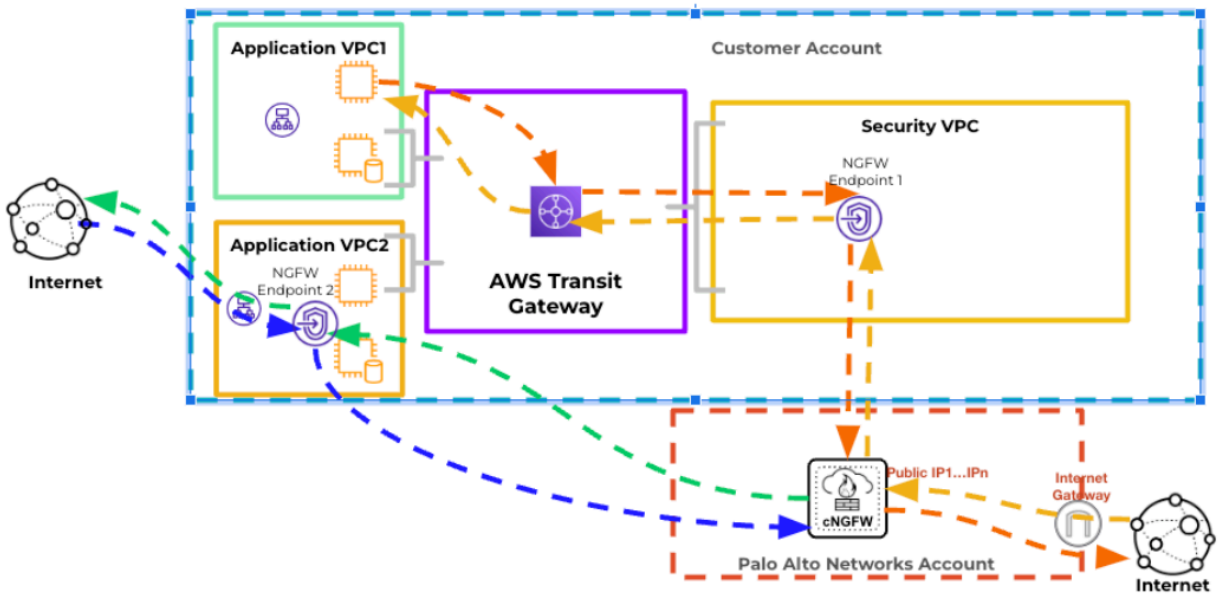

## Hybride NAT-Einstellungen

Sie können Ausgangs-NAT für eine NGFW-Ressource aktivieren, aber Sie können die Einstellung für Ausgangs-NAT auf einem oder mehreren Endpunkten als deaktiviert anpassen. In diesem Fall funktioniert Cloud NGFW wie folgt:

1. Wenn Sie Ausgangs-NAT auf einem Endpunkt deaktivieren, übernimmt Cloud NGFW die Rolle eines Bump-in-the-Wire und leitet den gesamten geprüften Datenverkehr zurück an seinen Endpunkt.
2. Wenn Sie Ausgangs-NAT auf einem Endpunkt aktiviert lassen, leitet Cloud NGFW den geprüften Datenverkehr direkt ins Internet um.

In der folgenden Abbildung ist Ausgangs-NAT für Endpunkt 1 aktiviert und für Endpunkt 2 deaktiviert:




# Ausgangs-NAT mit von Palo Alto Networks verwalteten AWS-EIPs konfigurieren

In AWS stellt eine elastische IP-Adresse (EIP) eine statische IPv4-Adresse dar, die für dynamisches Cloud-Computing verwendet wird. Eine elastische IP-Adresse ist aus dem öffentlichen Internet erreichbar, Sie können sie jedoch einer privaten Instanz zuordnen, um die Kommunikation mit dem Internet zu ermöglichen. Ausgangs-NAT wird nur für die Regelstapel- und Panorama-Richtlinienverwaltung unterstützt.

So konfigurieren Sie Ausgangs-NAT mit von Palo Alto Networks verwalteten AWS-EIPs:

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Klicken Sie auf **NGFWs**.

**STEP 3 |** Erstellen Sie eine neue NGFW-Ressource.

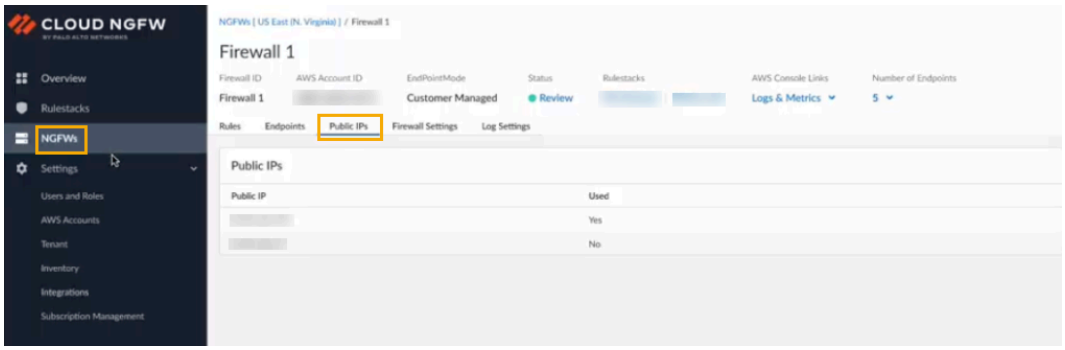
**STEP 4 |** Wählen Sie im Abschnitt **Policy Management (Richtlinienverwaltung)** die Option **Panorama** aus. Wählen Sie im Dropdown-Menü die integrierte Panorama-Instanz aus.

**STEP 5 |** Wählen Sie im Abschnitt **Egress NAT (Ausgangs-NAT)** die Option **Enable Egress NAT (Ausgangs-NAT aktivieren)** aus.

**STEP 6 |** Wählen Sie im Abschnitt **Public IPs (Öffentliche IPs)** die Option **AWS Service IPs (AWS-Dienst-IPs)** aus.

*Wählen Sie auf der Firewallseite die Registerkarte **Public IPs (Öffentliche IPs)** aus, um die Liste der unterstützten IP-Adressen für den Ausgangs-NAT-Datenverkehr anzuzeigen:*




Nachdem die Firewall erstellt wurde, überprüfen Sie deren Status.

# Ausgangs-NAT mit Bring Your Own IPs (BYOIPs) konfigurieren

In diesem Szenario übertragen Sie Ihre BYOIP-Adressen von Ihrem AWS-Konto, um stündliche EIP-Verwaltungskosten zu vermeiden.

Um BYOIPs verwenden zu können, müssen Sie einen IP-Adressverwaltungspool (IPAM) in Ihrem AWS-Konto erstellen und in Ihrem Cloud NGFW für AWS-Bereitstellungskonto freigeben. IPAM hilft Ihnen, Ihr IP-Adressierungsschema zu verwalten, um die Sicherheitsanforderungen zu erfüllen. Weitere Informationen finden Sie unter Bring your own IP addresses auf der AWS-Website. Ausgangs-NAT wird nur für die Regelstapel- und Panorama-Richtlinienverwaltung unterstützt.

*Wenn Sie einen IPAM-Pool in AWS erstellen, müssen Sie die AWS-Konto-ID von Palo Alto Networks für Cloud NGFW auf die Whitelist setzen, um IP-Adressen zwischen der Cloud NGFW-Datenebene und AWS freizugeben. Während des IPAM-Poolerstellungsprozesses wählen Sie die Option **Allow Amazon VPC IP Address Manager (Amazon VPC IP Address Manager zulassen)** aus. Dies ist ein obligatorischer Schritt zum Erstellen des IPAM-Pools. Geben Sie die Konto-ID der AWS-Datenebene für Ihre Cloud NGFW-Ressource an: 010510656586.*

*Das Erstellen eines IPAM-Pools kann etwa 10 Minuten dauern.*

### IPAM-Pool erstellen

So erstellen Sie einen IPAM-Pool:

**STEP 1 |** Melden Sie sich im AWS VPC IP Address Manager an.

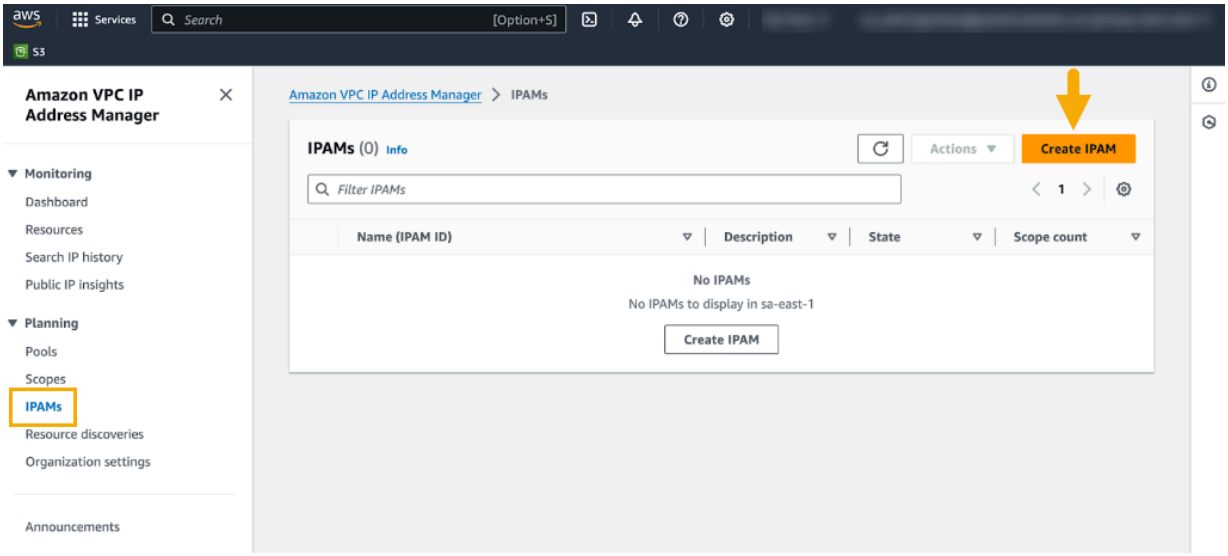
**STEP 2 |** Wählen Sie **Planning > IPAMs (Planung > IPAMs)** aus.

**STEP 3 |** Klicken Sie auf der Seite **IPAMs** auf **Create IPAM (IPAM erstellen)**.

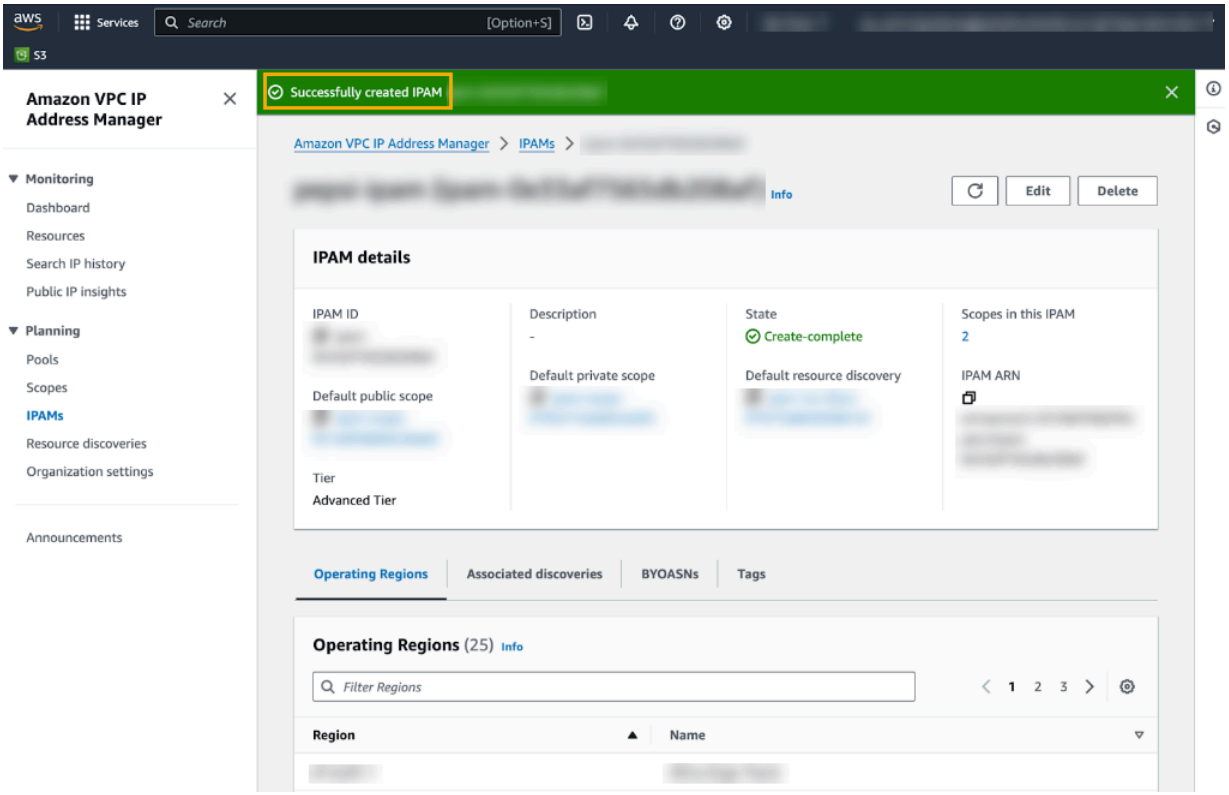
*Weitere Informationen finden Sie in den Anweisungen auf der AWS-Seite* Create an IPAM.

Nachdem Sie den IPAM erfolgreich erstellt haben, zeigt der **AWS VPC IP Address Manager** Details zum IPAM an:




Nachdem Sie den IPAM erfolgreich erstellt haben, zeigt der **AWS VPC IP Address Manager** Details zum IPAM an:

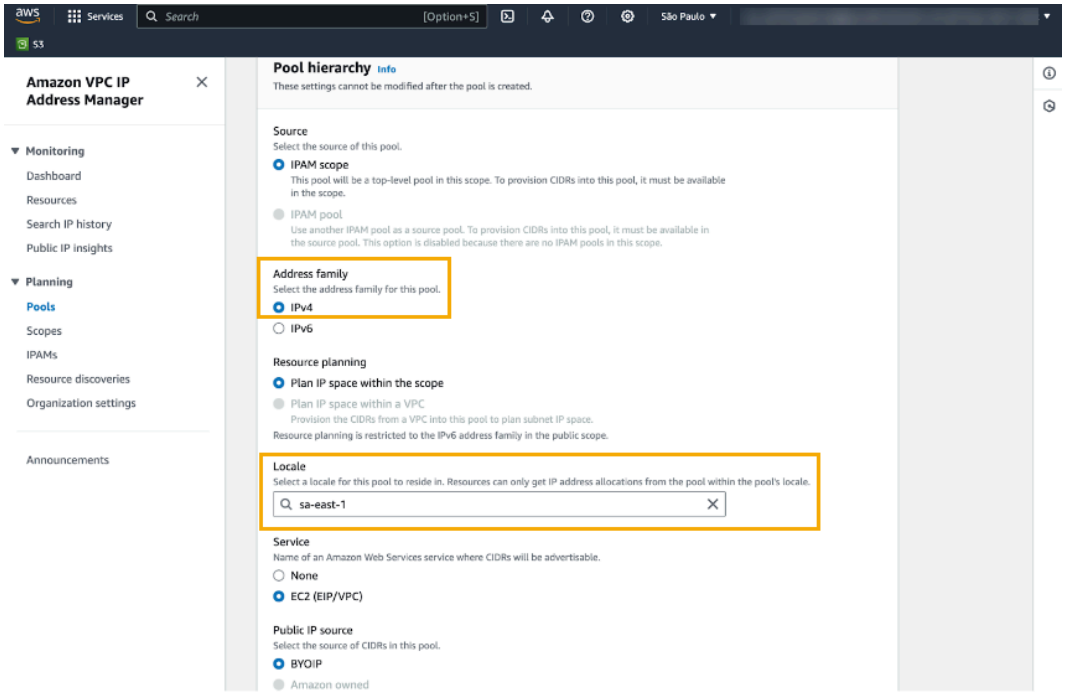
 



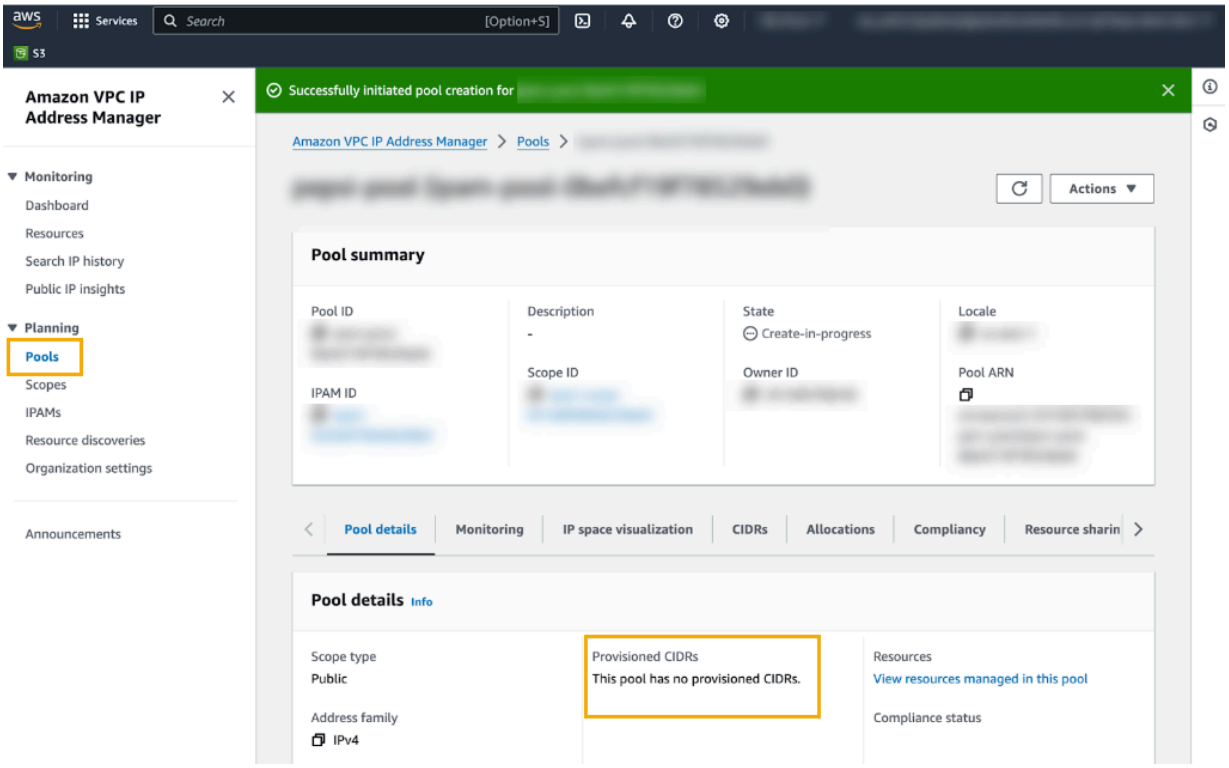
**STEP 4 |** Erstellen Sie einen IPAM-Pool, um die Bereitstellung von IP-Adressen zu planen. Wählen Sie **Planning > Pools (Planung > Pools)** aus und klicken Sie auf **Create Pool (Pool erstellen)**.

*Wenn Sie einen IPAM-Pool erstellen, müssen Sie **Address Family (Adressfamilie)** auf **IPv4** und **Locale (Gebietsschema)** auf den Ort festlegen, an dem Sie Ihre Cloud NGFW-Ressource bereitstellen möchten, wie im Bildschirm **Pool Hierarchy (Poolhierarchie)** dargestellt:*




Nachdem Sie das IPAM erfolgreich erstellt haben, zeigt der **AWS VPC IP Address Manager** Details zum neuen Pool an:




*Im neu erstellten Pool werden keine CIDRs bereitgestellt. Sie benötigen einen öffentlichen IP-CIDR-Bereich und den privaten Schlüssel des entsprechenden Zertifikats.*

**STEP 5 |** Stellen Sie CIDRs für den neu erstellten Pool aus dem vorherigen Schritt bereit. Wählen Sie **Planning > Pools (Planung > Pools)** und dann die Registerkarte **CIDR** unter der **Poolübersicht** aus.

**STEP 6 |** Wählen Sie **Actions > Provision CIDR (Aktionen > CIDR bereitstellen) aus.** Sie werden diesen Prozess verwenden, um einen öffentlichen IP-CIDR-Bereich und den privaten Schlüssel des entsprechenden Zertifikats abzurufen. Weitere Informationen finden Sie unter Provision CIDRS to a pool.

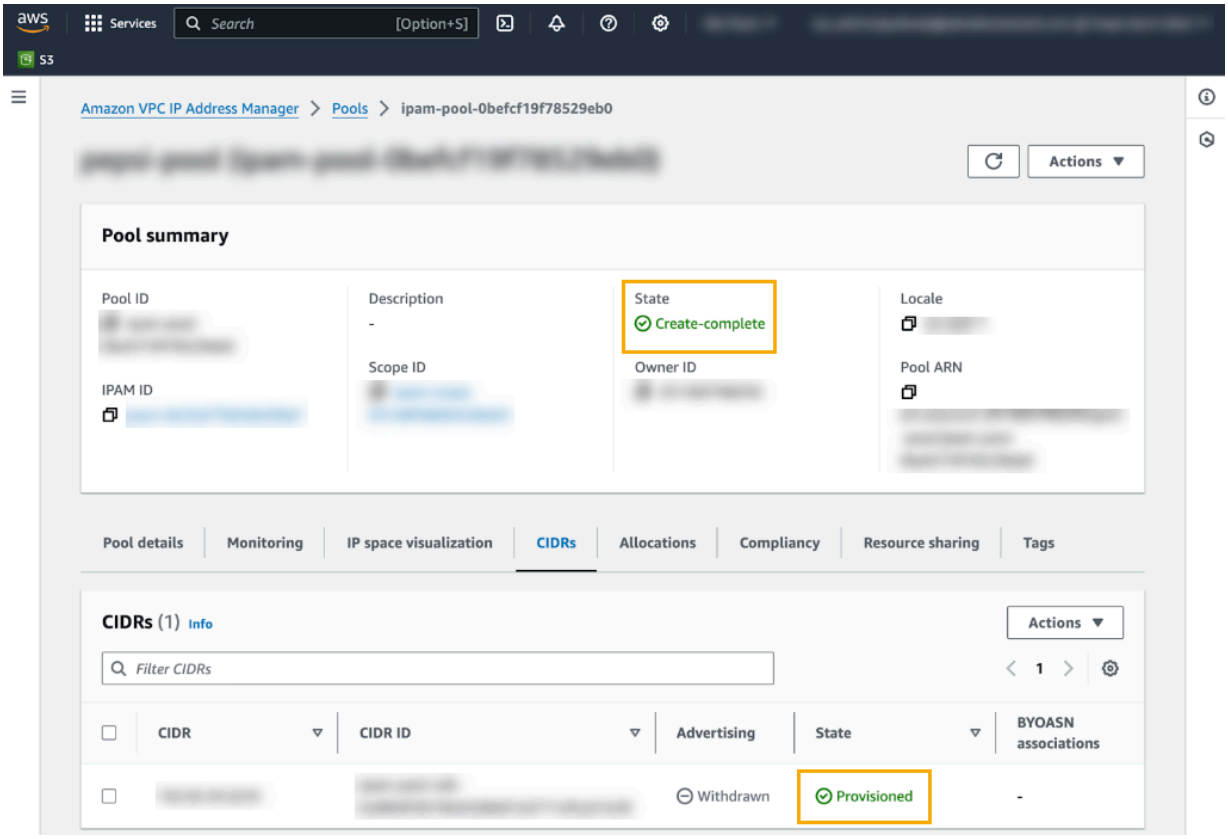
 

**STEP 7 |** Klicken Sie in den bereitzustellenden CIDRs auf **Input a CIDR with a X.509 Certificate (Eingabe eines CIDR mit einem X.509-Zertifikat)**.

**STEP 8 |** Kopieren Sie die **Signatur**.

**STEP 9 |** Klicken Sie auf **Provision (Bereitstellen)**.

Stellen Sie sicher, dass das CIDR erfolgreich bereitgestellt wurde und dass der Pool erfolgreich erstellt wurde:

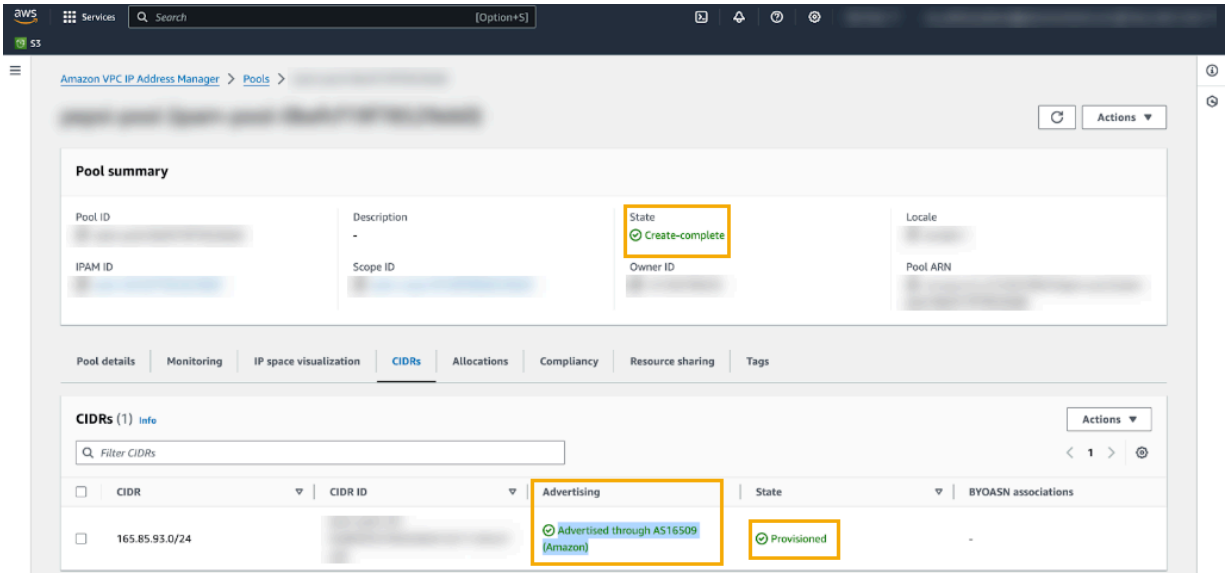


**STEP 10 |** Wenn Sie ein CIDR zu einem Pool hinzufügen, wird es standardmäßig nicht angekündigt. Kündigen Sie es an, um es öffentlich über das Internet zugänglich zu machen. So kündigen Sie das CIDR an:

1. Wählen Sie den Pool aus.
2. Klicken Sie auf die Registerkarte **CIDR**.
3. Wählen Sie im Menü **Actions (Aktionen)** die Option **Advertise (Ankündigen)** aus.
4. Wählen Sie im Menü **Advertise CIDR (CIDR ankündigen)** über das Dropdown-Menü die entsprechende ASN aus. Klicken Sie auf **Advertise CIDR (CIDR ankündigen)**. Weitere Informationen finden Sie unter Advertise your CIDR.

Bestätigen Sie, dass das CIDR erfolgreich angekündigt wird:



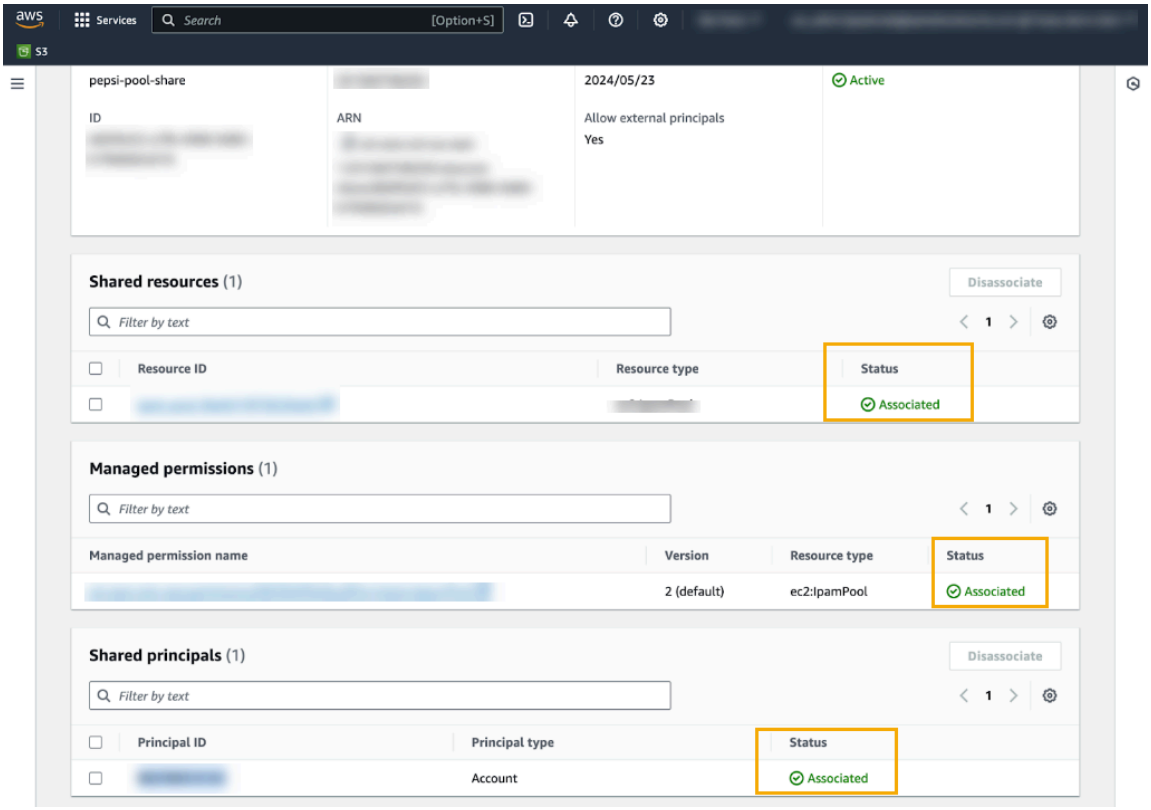

 

**STEP 11 |** Geben Sie nach der Ankündigung des CIDR den IPAM-Pool für Ihr Cloud NGFW-Bereitstellungskonto frei. Gehen Sie dazu wie folgt vor:

1. Wählen Sie den Pool aus.
2. Klicken Sie auf die Registerkarte **Resource sharing (Ressourcenfreigabe)**.
3. Wählen Sie im Menü **Resource sharing (Ressourcenfreigabe)** die Option **Create resource share (Ressourcenfreigabe erstellen)** aus.
4. Geben Sie im Menü **Resource share name (Ressourcenfreigabename)** den Namen des IPAM-Pools ein, den Sie freigeben möchten.
5. Fügen Sie optional die **ARN** zum Ressourcenfreigabenamen hinzu.
6. Klicken Sie auf **Next (Weiter)**.
7. Gewähren Sie den Principals Zugang.
8. Überprüfen Sie die Ressourcenfreigabeoptionen und Principals und klicken Sie dann auf **Create (Erstellen)**. Weitere Informationen finden Sie unter Share an IPAM pool.

   Bestätigen Sie, dass die mit dem IPAM-Pool verknüpften Ressourcen erfolgreich freigegeben wurden:




# Cloud NGFW-Ressource erstellen, Ausgangs-NAT aktivieren und BYOIPs festlegen

Nachdem Sie die Schritte zum Erstellen des IPAM-Pools abgeschlossen haben, erstellen Sie die Cloud NGFW-Ressource, aktivieren Sie Ausgangs-NAT und geben Sie BYOIPs an.

So konfigurieren Sie Ausgangs-NAT mithilfe von BYOIPs:

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Klicken Sie auf **NGFWs**.

**STEP 3 |** Erstellen Sie eine neue NGFW-Ressource.

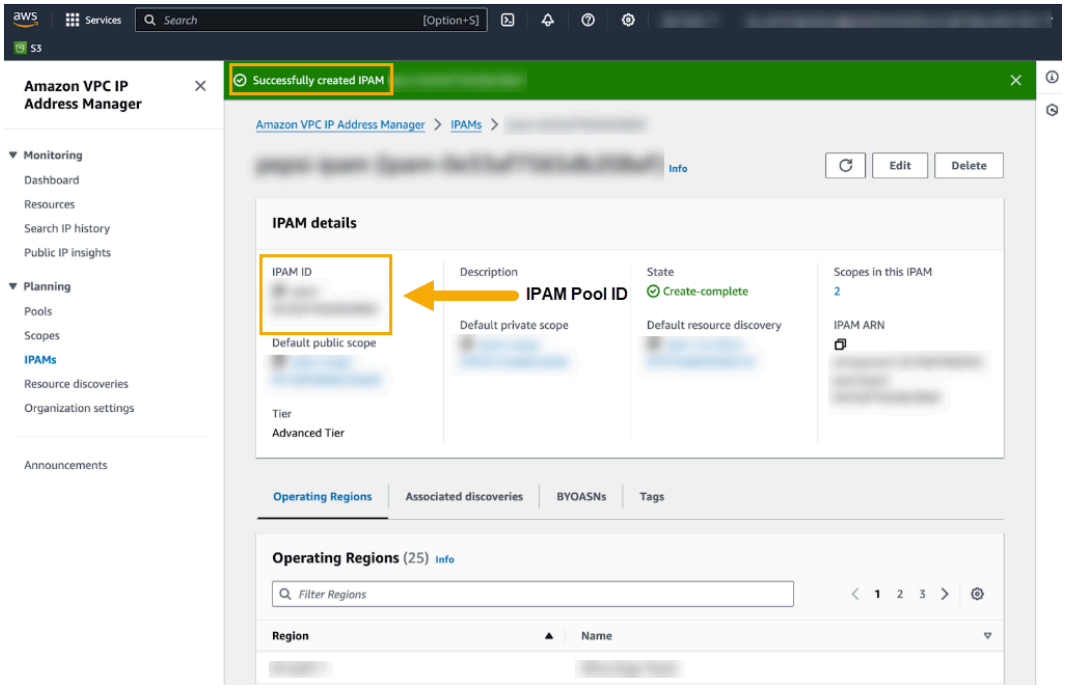
**STEP 4 |** Wählen Sie im Abschnitt **Policy Management (Richtlinienverwaltung)** die Option **Panorama** aus. Wählen Sie im Dropdown-Menü die integrierte Panorama-Instanz aus.

**STEP 5 |** Wählen Sie im Abschnitt **Egress NAT (Ausgangs-NAT)** die Option **Enable Egress NAT (Ausgangs-NAT aktivieren)** aus.

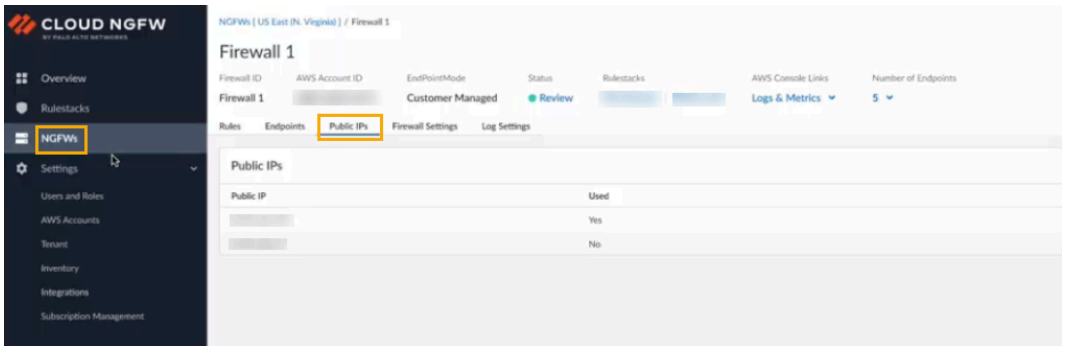
**STEP 6 |** Wählen Sie **Bring Your Public IPs (Öffentliche IPs mitbringen)** aus und geben Sie die IPAM-Pool-ID ein, die in Schritt 3 (oben) erstellt wurde.

*Die **IPAM-Pool-ID** befindet sich im Abschnitt **IPAM Pool Details (IPAM-Pool-Details)**.*



*Wählen Sie auf der Firewallseite die Registerkarte **Public IPs (Öffentliche IPs)** aus, um die Liste der unterstützten IP-Adressen für den Ausgangs-NAT-Datenverkehr anzuzeigen:*




Nachdem die Firewall erstellt wurde, überprüfen Sie deren Status.

*Wenn Sie keine BYOIPs verwenden möchten, wenden Sie sich an Palo Alto Networks, um einen Supportfall zu erstellen.*

# Schutz

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Sie können verschiedene Arten von Richtlinienregeln erstellen, um Ihr Netzwerk vor Bedrohungen und Störungen zu schützen. Das hilft bei der Optimierung der Netzwerkressourcenzuweisung und der Verwaltung Ihrer Netzwerkrichtlinienregeln, um den Datenverkehr zu priorisieren und Anwendungsklassifizierungen zu konfigurieren.

Cloud NGFW wertet Regeln von oben nach unten aus und wenn der Datenverkehr den definierten Regelkriterien entspricht, werden nachfolgende Regeln nicht ausgewertet. Um die bestmöglichen Übereinstimmungskriterien durchzusetzen, sollten Sie spezifischere Richtlinienregeln oberhalb von allgemeineren platzieren. Für den Datenverkehr, der einer Richtlinienregel entspricht, wird ein Protokoll generiert, wenn die Protokollierung für die Regel aktiviert ist. Protokollierungsoptionen sind für jede Regel konfigurierbar.

Für die meisten Richtlinientypen stehen Best-Practice-Richtlinienregeln zur Verfügung, die Ihnen einen schnellen und sicheren Einstieg ermöglichen. Diese Regeln können zwar nicht bearbeitet werden, um sicherzustellen, dass Ihnen immer ein Mindestmaß an Sicherheit zur Verfügung steht, Sie können sie jedoch klonen, wenn Sie sie als Grundlage für eigene Richtlinien verwenden möchten.

Die Cloud NGFW für AWS-Plattform schützt Ihr gesamtes Unternehmen, unabhängig von Größe oder Komplexität. Mit einer einheitlichen Netzwerksicherheitsarchitektur und der Fähigkeit, Deep Learning in Echtzeit zu nutzen, kann Cloud NGFW für AWS Ihnen helfen, alles zu sehen und zu sichern. Dieser Schutz umfasst Folgendes:

- Zweigstelle. Ermöglichen Sie Zero-Trust-Netzwerksicherheit mit vereinfachter Sicherheit für Tausende von Zweigstellen.
- Campus. Integrierte Funktionen schützen Ihre internen Ressourcen und die Außenwelt, sodass Ihre Benutzer überall auf Daten und Anwendungen zugreifen können.
- Rechenzentrum. Profitieren Sie von umfassender Transparenz und konsistenten, erstklassigen Sicherheitskontrollen in allen Cloud-Umgebungen.
- Öffentliche Cloud. Schützen Sie mehrere Umgebungen in öffentlichen Clouds mit dem gleichen Schutzniveau wie lokale Rechenzentren.
- 5G-Sicherheit. Nutzen Sie eine vereinfachte Lösung, um alle Facetten Ihres einzigartigen Mobilfunknetzes zu schützen.

Mit Cloud NGFW für AWS müssen Sie keine Infrastruktur verwalten. Komfortable Bereitstellung: Dank der Regelstapelkonfiguration und der automatisierten Sicherheitsprofile ist diese Firewall der nächsten

Generation von Palo Alto Networks so konzipiert, dass Sie die Anforderungen an die Netzwerksicherheit mühelos erfüllen können.

# Cloud-Delivered Security Services (CDSS)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Die Suite an Cloud-Delivered Security Services (CDSS) von Palo Alto Networks bietet Zugriff auf spezialisierte abonnementbasierte Sicherheitslösungen, die eigens zum Schutz vor bekannten, unbekannten und hochentwickelten Bedrohungen durch Sicherheitsumgehungstechniken entwickelt wurden. Die durch erweiterte Analysen generierten Bedrohungsdaten werden über die Sicherheitsplattformen von Palo Alto Networks hinweg geteilt, um eine vollständige Abdeckung aller Bedrohungsvektoren zu gewährleisten.

Um Ihren Datenverkehr mit CDSS zu sichern und zu schützen, bietet Cloud NGFW für AWS Schutzfunktionen von Palo Alto Networks wie:

- App-ID. Basierend auf der patentierten Layer-7-Datenverkehrs-Klassifizierungstechnologie ermöglicht Ihnen der App-ID-Dienst, die Anwendungen in Ihrem Netzwerk anzuzeigen, mehr über ihre Funktionsweise zu erfahren, ihre Verhaltensmerkmale zu beobachten und ihr relatives Risiko zu verstehen. Cloud NGFW für AWS identifiziert Anwendungen und Anwendungsfunktionen mithilfe mehrerer Techniken, darunter Anwendungssignaturen, Entschlüsselung, Protokolldekodierung und Heuristik. Diese Funktionen ermitteln die genaue Identität der Anwendungen, die Ihr Netzwerk durchlaufen, einschließlich derjenigen, die versuchen, der Erkennung zu entgehen, indem sie sich durch Port-Hopping oder Verwendung von Verschlüsselung als legitimer Datenverkehr tarnen.
- Threat Prevention. Der Threat Prevention-Dienst von Palo Alto Networks schützt Ihr Netzwerk, indem er mehrere Präventionsebenen bereitstellt, um jeder Phase eines Angriffs entgegenzuwirken. Zusätzlich zu den grundlegenden Funktionen des Intrusion Prevention Service (IPS) verfügt Threat Prevention über die einzigartige Fähigkeit, Bedrohungen auf allen Ports zu erkennen und zu blockieren – anstatt einfach Signaturen basierend auf einer begrenzten Anzahl vordefinierter Ports aufzurufen.
- Erweiterte URL-Filterung. Dieser wichtige, in Cloud NGFW für AWS integrierte Dienst stoppt unbekannte webbasierte Angriffe in Echtzeit, um Patient Zero mit der branchenweit einzigen ML-gestützten erweiterten URL-Filterung zu verhindern. Die erweiterte URL-Filterung kombiniert die bekannte Datenbank bösartiger URLs von Palo Alto Networks mit der ersten Echtzeit-Web-Schutz-Engine der Branche, sodass Unternehmen neue bösartige und gezielte webbasierte Bedrohungen automatisch und sofort erkennen sowie verhindern können.
- DNS. DNS Security bietet Ihnen Echtzeitschutz und wendet branchenweit einzigartige Schutzmechanismen an, um Angriffe, die DNS verwenden, zu unterbinden. Die nahtlose Integration in eine Next-Generation Firewall (NGFW) von Palo Alto Networks bietet Ihnen automatisierten Schutz, verhindert, dass Angreifer Sicherheitsmaßnahmen umgehen, und macht unabhängige Tools oder Änderungen am DNS-Routing überflüssig. Dank DNS Security steht Ihrem Unternehmen ein wichtiger neuer Kontrollpunkt zum Stoppen von Angriffen zur Verfügung.

- WildFire. Palo Alto Networks Advanced WildFire® ist die branchenweit größte cloudbasierte Malware-Präventions-Engine. Sie schützt Unternehmen mithilfe patentierter Erkennungs-Engines für maschinelles Lernen vor hochentwickelten Bedrohungen durch Sicherheitsumgehungstechniken und ermöglicht so automatisierten Schutz im gesamten Netzwerk, in der Cloud und an Endpunkten. Advanced WildFire analysiert jede unbekannte Datei auf bösartige Absichten und verteilt dann in Rekordzeit – 60-mal schneller als das Produkt des nächsten Wettbewerbers – Präventionsmaßnahmen, um das Risiko von Patient Zero zu reduzieren.

# Advanced Threat Prevention in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

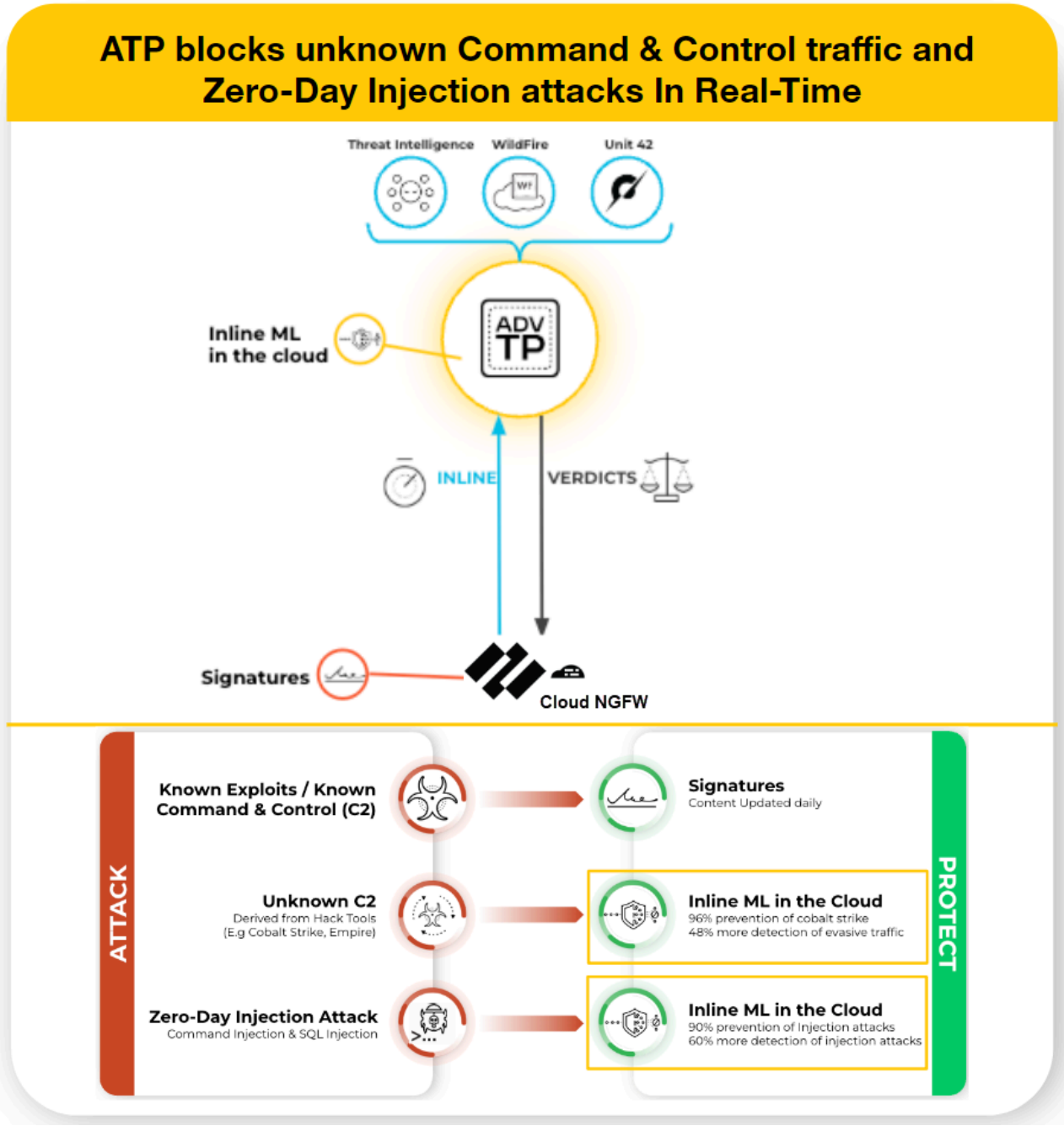
Advanced Threat Prevention (ATP) ist eine Intrusion-Prevention-System(IPS)-Lösung, die Malware, Sicherheitslücken-Exploits sowie Command-and-Control(C2)-Funktionen über alle Ports und Protokolle hinweg erkennen und blockieren kann. Dabei kommen mehrschichtige Abwehrmaßnahmen zum Einsatz. Die Threat-Prevention-Cloud betreibt eine Vielzahl von Erkennungsdiensten, die die kombinierten Bedrohungsdaten der Palo Alto Networks Dienste verwenden, um Signaturen zu erstellen, die jeweils spezifische identifizierbare Muster aufweisen. Sie werden von Cloud NGFW für AWS verwendet, um Regeln für Sicherheitsrichtlinien durchzusetzen, wenn übereinstimmende Bedrohungen und bösartiges Verhalten erkannt werden. Diese Signaturen werden anhand des Bedrohungstyps kategorisiert und mit eindeutigen Kennnummern versehen. Um Bedrohungen zu erkennen, die diesen Signaturen entsprechen, betreibt Cloud NGFW für AWS Analyse-Engines, die Netzwerkverkehr mit anomalen Merkmalen prüfen und klassifizieren.

*Nachdem Sie Advanced Threat Prevention aktiviert haben, verwenden Sie Panorama, um zugeordnete Advanced Threat Prevention-Richtlinien zu konfigurieren.*

Zusätzlich zum signaturbasierten Erkennungsmechanismus bietet Advanced Threat Prevention ein Inline-Erkennungssystem, um unbekannte und ausweichende C2-Bedrohungen, einschließlich solcher, die über das Empire-Framework erzeugt werden, sowie Befehlsinjektions- und SQL-Injektionssicherheitslücken zu verhindern. Die Advanced Threat Prevention-Cloud betreibt erweiterbare Deep-Learning-Modelle, die Inline-Analysefunktionen in Cloud NGFW für AWS auf Anfrage ermöglichen, um das Eindringen von Zero-Day-Bedrohungen in das Netzwerk zu verhindern und Schutzmaßnahmen zu verteilen. So können Sie unbekannte Bedrohungen durch Echtzeitüberprüfung des Datenverkehrs mit Inline-Detektoren verhindern. Zum Schutz vor Zero-Day-Bedrohungen analysieren diese ML-basierten Erkennungs-Engines mit Deep-Learning-Modellen in der Advanced Threat Prevention-Cloud den Datenverkehr auf unbekannte C2-Aktivität und Sicherheitslücken, die SQL-Injektionen und Befehlsinjektionen verwenden. Um einen Bedrohungskontext und umfassende Einzelheiten zur Erkennung bereitzustellen, werden Berichte erstellt, die die vom Angreifer verwendeten Tools und Techniken, den Umfang und die Auswirkungen

der Erkennung sowie die entsprechende Cyberangriffsklassifikation gemäß dem MITRE ATT&CK® Framework beinhalten können.




## Native Richtlinienverwaltung

Advanced Threat Prevention (ATP) wird automatisch konfiguriert, wenn Sie einen neuen lokalen Regelstapel erstellen. Für Regelstapel, die Sie vor März 2024 erstellt haben, aktivieren Sie ATP manuell über die Cloud NGFW für AWS-Konsole.

So aktivieren Sie ATP für einen Regelstapel:

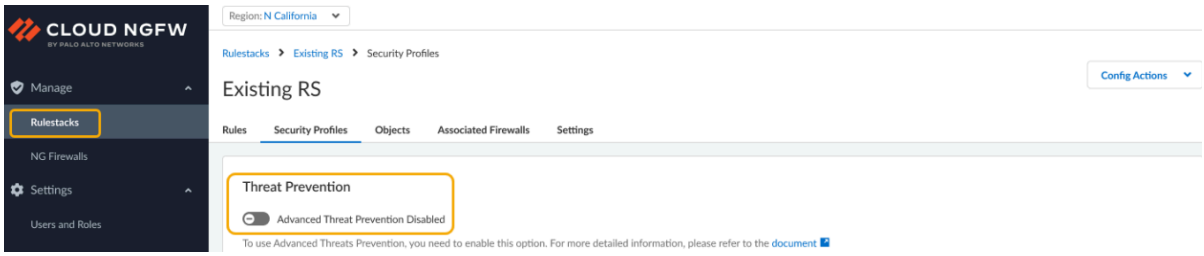
**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Wählen Sie **Rulestacks (Regelstapel)** aus.

**STEP 3 |** Wählen Sie **Security Profiles (Sicherheitsprofile)** aus.

**STEP 4 |** Aktivieren Sie im Abschnitt **Threat Prevention** mit dem Schalter die Option **Advanced Threat Prevention**.




**STEP 5 |** In einem Bestätigungsdialogfeld wird darauf hingewiesen, dass durch die ATP-Funktion möglicherweise Gebühren anfallen. Klicken Sie auf **Enable (Aktivieren)**. Weitere Details finden Sie in Ihrem AWS-Abrechnungsabonnement.

*Sie verwenden Panorama, um Ihr ATP-Abonnement innerhalb Ihrer Netzwerksicherheitsbereitstellung zu konfigurieren. Obwohl es möglicherweise nicht erforderlich ist, alle Prozesse von ATP zu implementieren, empfiehlt Palo Alto Networks, alle Aufgaben zu überprüfen, um sich mit den verfügbaren Optionen für eine erfolgreiche Bereitstellung vertraut zu machen.*

## Panorama-Richtlinienverwaltung

Advanced Threat Prevention (ähnlich wie andere Sicherheitsdienste von Palo Alto Networks) wird über Sicherheitsprofile verwaltet, die wiederum von der Konfiguration der in den Sicherheitsrichtlinienregeln definierten Netzwerkdurchsetzungsrichtlinien abhängig sind.

*Sie verwenden Cloud NGFW für AWS, um Advanced Threat Prevention für den Regelstapel zu aktivieren. Allerdings müssen Sie Panorama verwenden, um die Richtlinien zu konfigurieren, aus denen der Sicherheitsdienst besteht.*

So konfigurieren Sie mithilfe von Panorama erweiterte Richtlinienregeln für die URL-Filterung:

**STEP 1 |** Melden Sie sich bei Panorama an.

**STEP 2 |** Überprüfen Sie, ob Sie über das entsprechende Lizenzabonnement für die erweiterte URL-Filterung verfügen. Wählen Sie in Panorama **Device (Gerät) > Licenses (Lizenzen)** aus. Vergewissern Sie sich, dass das Ablaufdatum der Lizenz in der Zukunft liegt.

**STEP 3 |** Richten Sie Advanced Threat Prevention mithilfe von Panorama ein.

**STEP 4 |** Führen Sie einen Commit für Ihre Änderungen aus.

*Palo Alto Networks bietet mehrere Optionen zur Überwachung der vom Sicherheitsdienst Advanced Threat Prevention verarbeiteten Aktivitäten. Weitere Informationen finden Sie unter Advanced Threat Prevention überwachen.*

# Erweiterte URL-Filterung in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Palo Alto Networks bietet eine Reihe vordefinierter URL-Filterungskategorien. Sie können auch eigene URL-Filterungskategorien mithilfe eines benutzerdefinierten URL-Kategorieobjekts angeben. Erstellen Sie beispielsweise eine benutzerdefinierte Liste von URLs, die Sie als Übereinstimmungskriterien in einer Sicherheitsrichtlinienregel verwenden möchten. Dies ist eine gute Möglichkeit, Ausnahmen für URL-Kategorien anzugeben, bei denen Sie bestimmte URLs anders erzwingen möchten als die URL-Kategorie, zu der sie gehören.

## Benutzerdefinierte URL-Kategorie erstellen

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den eine benutzerdefinierte URL-Kategorie konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Objects (Objekte)** > **Custom URL Category (Benutzerdefinierte URL-Kategorie)** > **Create Custom URL Category (Benutzerdefinierte URL-Kategorie erstellen)** aus.

**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihre benutzerdefinierte URL-Kategorie ein.

**STEP 4 |** (optional) Geben Sie eine Beschreibung für Ihre benutzerdefinierte URL-Kategorie ein.

**STEP 5 |** Geben Sie mindestens eine **URL-Liste** ein, eine pro Zeile.

**STEP 6 |** Klicken Sie auf **Save (Speichern)**.

## Grundlegende Richtlinien für URL-Kategorie-Ausnahmelisten

- Geben Sie die URLs der Websites, die Sie erzwingen möchten, getrennt von der zugeordneten URL-Kategorie ein.
- Listeneinträge müssen genau übereinstimmen und die Groß-/Kleinschreibung muss beachtet werden.
- Geben Sie einen String ein, der genau mit der Website (und möglicherweise einer bestimmten Unterdomäne) übereinstimmt, für die Sie den Zugriff steuern möchten, oder verwenden Sie Platzhalterzeichen, damit ein Eintrag mit mehreren Website-Unterdomänen übereinstimmt. Weitere Informationen zur Verwendung von Platzhalterzeichen finden Sie unter Platzhalterrichtlinien für URL-Kategorie-Ausnahmelisten.
- Lassen Sie `http` und `https` in URL-Einträgen weg.
- Jeder URL-Eintrag kann bis zu 255 Zeichen lang sein.

## Platzhalterrichtlinien für URL-Kategorie-Ausnahmelisten

Sie können Platzhalter in URL-Kategorie-Ausnahmelisten verwenden, um einen einzelnen Eintrag einfach so zu konfigurieren, dass er mehreren Website-Unterdomänen und -Seiten zugeordnet wird, ohne genaue Unterdomänen und Seiten angeben zu müssen.

Befolgen Sie beim Erstellen von Platzhaltereinträgen die folgenden Richtlinien:

- Die folgenden Zeichen werden als Tokentrennzeichen betrachtet: . / ? & = ; +

  Jeder String, der durch ein oder zwei dieser Zeichen getrennt ist, ist ein Token. Verwenden Sie Platzhalterzeichen als Tokenplatzhalter, um anzugeben, dass ein bestimmtes Token einen beliebigen Wert enthalten kann.
- Verwenden Sie anstelle eines Tokens entweder ein Sternchen (*) oder ein Caretzeichen (^), um einen Platzhalterwert anzugeben.
- Platzhalterzeichen müssen das einzige Zeichen innerhalb eines Tokens sein. Beispielsweise wäre www.gmail*.com ungültig, da das Sternchen auf andere Zeichen folgt. Ein Eintrag kann jedoch mehrere Platzhalter enthalten.

## So verwenden Sie Sternchen (*) und Caretzeichen (^) als Platzhalter

| | |
|---|---|
| ***** | Verwenden Sie dieses Zeichen, um mindestens eine variable Unterdomäne anzugeben. Wenn Sie ***** verwenden, stimmt der Eintrag mit allen zusätzlichen Unterdomänen überein, unabhängig davon, ob es am Anfang oder am Ende der URL steht.<br>Beispiel:<br>• ***.paloaltonetworks.com** stimmt mit www.paloaltonetworks.com und www.paloaltonetworks.com.uk überein.<br>• ***.paloaltonetworks.com/** stimmt mit www.paloaltonetworks.com überein, aber nicht mit www.paloaltonetworks.com.uk. |
| **^** | Verwenden Sie dieses Zeichen, um eine variable Unterdomäne anzugeben.<br>Beispiel:<br>**mail.^.com** stimmt mit mail.company.com überein, aber nicht mit mail.company.sso.com. |

***Erstellen Sie keinen Eintrag mit fortlaufenden Sternchen (*) oder mehr als neun aufeinanderfolgenden Caretzeichen (^) als Platzhalter. Einträge wie diese können die Firewall-Leistung beeinträchtigen.***

*Fügen Sie beispielsweise keinen Eintrag wie* ***`mail.*.*.com`*** *hinzu. Geben Sie stattdessen je nach Bereich der Websites, für die Sie den Zugriff steuern möchten,* ***`mail.*.com`*** *oder* ***`mail.^.^.com`*** *ein. Ein Eintrag wie* ***`mail.*.com`*** *stimmt mit einer größeren Anzahl von Websites überein als* ***`mail.^.^.com`****.* ***`mail.*.com`*** *stimmt mit Websites mit beliebig vielen Unterdomänen überein und* ***`mail.^.^.com`*** *stimmt mit Websites mit genau zwei Unterdomänen überein.*

### URL-Kategorie-Ausnahmeliste – Beispiele für Platzhalter

Die folgende Tabelle enthält Beispiele für URL-Listeneinträge mit Platzhaltern und Websites, die mit diesen Einträgen übereinstimmen.

| Eintrag in URL-Ausnahmeliste | Übereinstimmende Seiten |
|---|---|
| **Beispielsatz 1** | |
| *.company.com | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| ^.company.com | tools.company.com<br>docs.company.com |
| ^.^.company.com | eng.tools.company.com<br>support.tools.company.com |
| **Beispielsatz 2** | |
| mail.google.* | mail.google.com<br>mail.google.co.uk<br>mail.google.example.org |
| mail.google.^ | mail.google.com<br>mail.google.info |
| mail.google.^.^ | mail.google.co.uk<br>mail.google.example.info |

| Eintrag in URL-Ausnahmeliste | Übereinstimmende Seiten |
|---|---|
| **Beispielsatz 3** | |
| site.*.com | site.yourname.com<br>site.abc.xyz.com |
| site.^.com | site.company.com<br>site.example.com |
| site.^.^.com | site.a.b.com |
| site.com/* | site.com/photos<br>site.com/blog/latest<br>beliebiges Unterverzeichnis von site.com |

# WildFire-Schutz in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW kann jetzt Dateien, ausführbare Dateien und schädliche Skripts (wie JScript und PowerShell) in Ihrem VPC-Datenverkehr erkennen und zur Analyse an den Cloud-Dienst WildFire™ weiterleiten. WildFire wendet dann Bedrohungsinformationen, Analysen und Korrelationen auf diese weitergeleiteten Dateien (ausführbare Dateien oder Skripte) an und stellt Urteile auf Grundlage der Analyse bereit. Wenn eine Bedrohung erkannt wird, erstellt WildFire Schutzmaßnahmen, um Malware zu blockieren und diesen Schutz vor dieser Bedrohung innerhalb weniger Minuten global zu verteilen.

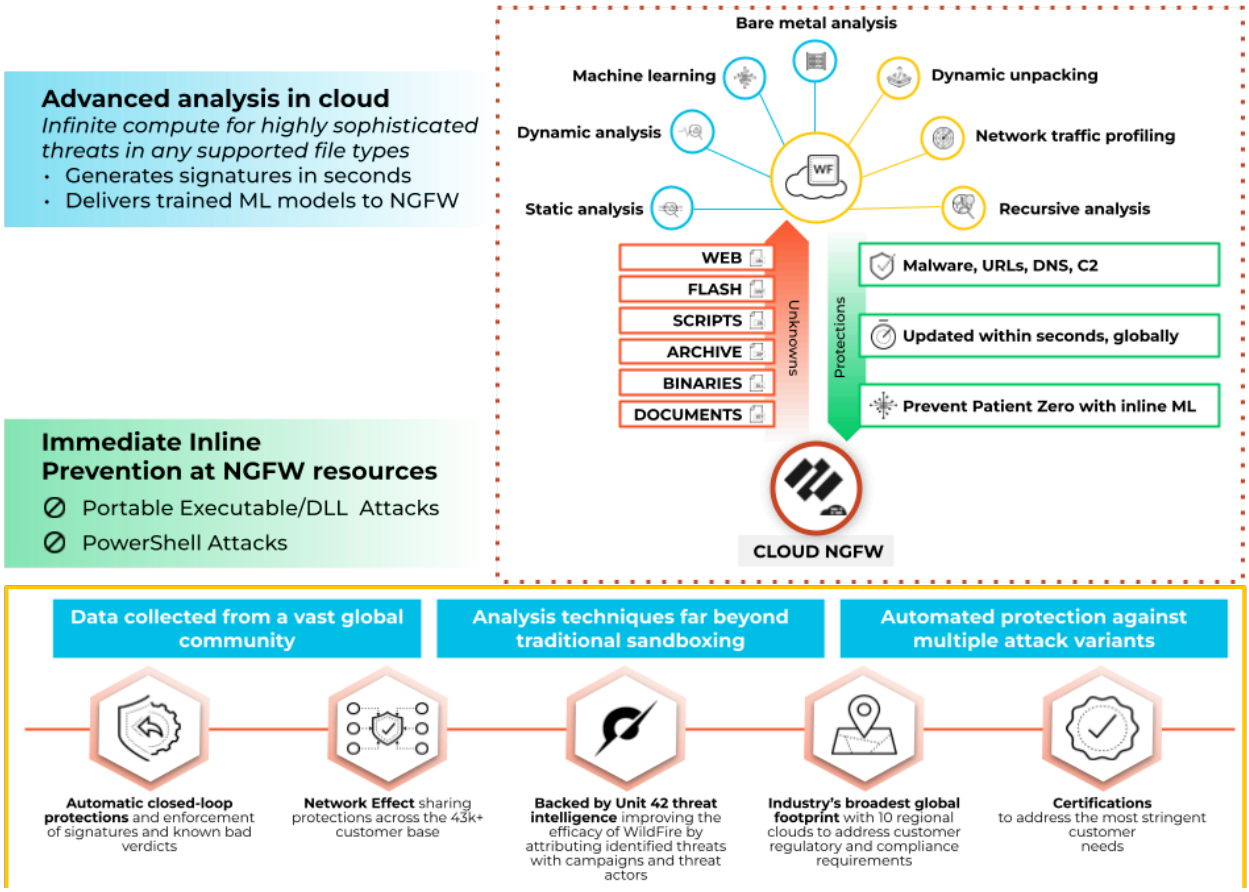
WildFire geht über herkömmliche Sandboxing-Ansätze hinaus und verwendet mehrere Techniken, um Dateien mit potenziell bösartigem Verhalten zu identifizieren. Zu diesen Techniken gehören:

- **Dynamische Analyse** – Dateien werden während ihrer Ausführung in einer speziell entwickelten, umgehungssicheren virtuellen Umgebung beobachtet, sodass bislang unbekannte Malware anhand hunderter Verhaltensmerkmale erkannt werden kann.
- **Statische Analyse** – Die dynamische Analyse wird durch eine effektive Erkennung von Malware ergänzt, sodass Malware-Varianten sofort erkannt werden können. Die statische Analyse nutzt darüber hinaus das dynamische Entpacken, um Bedrohungen zu analysieren, die durch den Einsatz von Packtool-Sätzen versuchen, der Erkennung zu entgehen.

- **Netzwerkverkehrsprofile** – Bösartige Verkehrsmuster basierend auf Malware-Varianten, wie etwa der Erstellung von Hintertüren, dem Download von Malware der nächsten Stufe, dem Zugriff auf Domänen mit geringer Reputation und der Netzwerkaufklärung, werden erkannt.
- **Maschinelles Lernen** – Aus jeder Datei werden tausende einzigartige Merkmale extrahiert und es wird ein prädiktives Modell für maschinelles Lernen trainiert, damit es neue Malware identifizieren kann, was mit einer rein statischen oder dynamischen Analyse nicht möglich ist.
- **Ein individuell entwickelter Hypervisor** – Mit einem robusten, proprietären Hypervisor, der nicht von Open-Source-Projekten oder proprietärer Software abhängig ist, auf die Angreifer Zugriff haben, werden von Angreifern verwendete Sicherheitsumgehungstechniken verhindert.



Um WildFire auf Ihrer Cloud NGFW AWS-Ressource zu konfigurieren, müssen Sie wie folgt vorgehen:

- WildFire-Profil konfigurieren
- Definieren Sie Sicherheitsregeln in der Cloud-Gerätegruppe, die Sie in Panorama erstellt haben
- WildFire-Übermittlungsprotokolle anzeigen

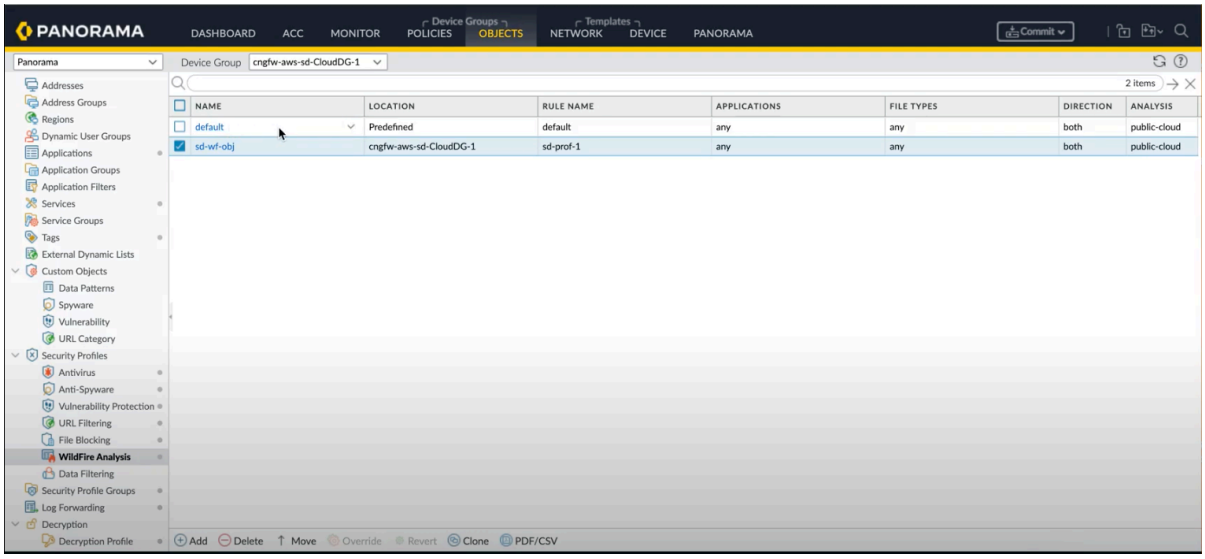
## WildFire-Profil konfigurieren

**STEP 1 |** Melden Sie sich bei **Panorama** an und klicken Sie auf **Objects (Objekte) > WildFire Analysis (WildFire-Analyse)**. Das Fenster „WildFire Analysis Profile“ (WildFire-Analyse-Profil) wird angezeigt.

**STEP 2 |** Wählen Sie im Dropdown-Menü die Gerätegruppe aus, in der Sie das Profil erstellen möchten.



**STEP 3 |** Klicken Sie auf **Add (Hinzufügen)**.

**STEP 4 |** Geben Sie einen **Namen** für das WildFire-Profil ein und klicken Sie auf **Add (Hinzufügen)**.

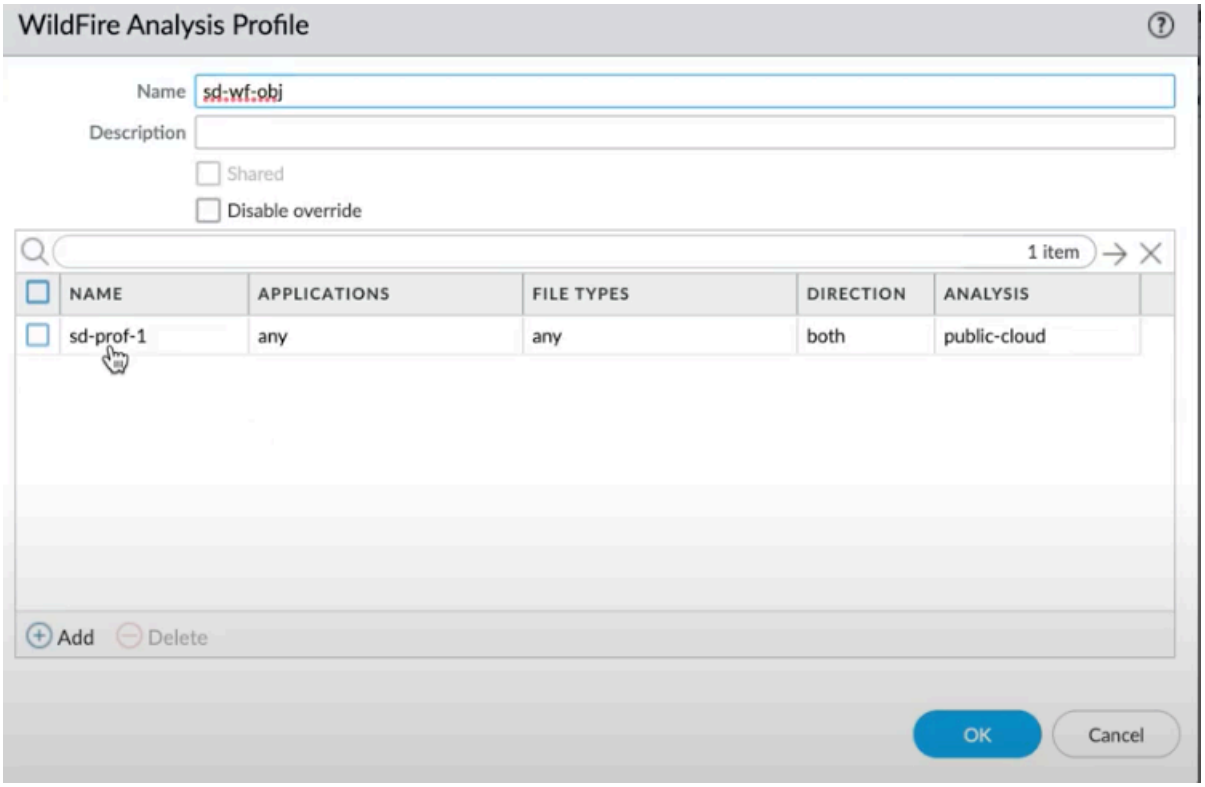
**STEP 5 |** Geben Sie einen beschreibenden **Namen** für alle Regeln ein, die Sie dem Profil hinzufügen.

**STEP 6 |** Klicken Sie im Abschnitt „Application“ (Anwendung) auf **Add (Hinzufügen)**, um aus der Liste der Anwendungen die Anwendung auszuwählen, der Sie über Ihr WildFire-Profil Zugriff gewähren möchten.

**STEP 7 |** Klicken Sie auf **FileTypes (Dateitypen)**, um die Dateitypen auszuwählen, die Sie zulassen möchten.

**STEP 8 |** Klicken Sie auf **Direction (Richtung)**, um den Download oder Upload oder beide Optionen zuzulassen.




**STEP 9 |** Wählen Sie das **Ziel** für Datenverkehr aus, der zur Analyse weitergeleitet werden soll: Wählen Sie **public cloud** aus, wenn der gesamte Datenverkehr, der der Regel entspricht, zur Analyse an die öffentliche WildFire-Cloud weitergeleitet werden soll.

**STEP 10 |** Wählen Sie **private cloud** aus, wenn der gesamte Datenverkehr, der der Regel entspricht, zur Analyse an die WildFire-Appliance weitergeleitet werden soll.

**STEP 11 |** Klicken Sie auf **OK**.

## Sicherheitsregeln definieren

**STEP 1 |** Melden Sie sich bei Panorama an und klicken Sie auf **Policy Rules (Richtlinienregeln)**.

**STEP 2 |** Wählen Sie die gewünschte Gerätegruppe aus und klicken Sie auf die vorkonfigurierte Sicherheitsregel („Vor-Regel“ oder „Nach-Regel“) oder erstellen Sie eine neue Regel.

**STEP 3 |** Klicken Sie auf **Actions (Aktionen)**.

**STEP 4 |** Wählen Sie in den Profileinstellungen unter dem Profiltyp die Option **Profiles (Profile)** aus.

**STEP 5 |** Wählen Sie aus der Dropdown-Liste **WildFire Analysis (WildFire-Analyse)** das gewünschte WildFire-Profil aus.

**STEP 6 |** Klicken Sie auf **OK**.

Führen Sie einen Commit aus und übertragen Sie die Gerätegruppe per Push an die Cloud NGFW-Ressourcen.

Weitere Informationen finden Sie unter Neueste WildFire Cloud-Funktionen.

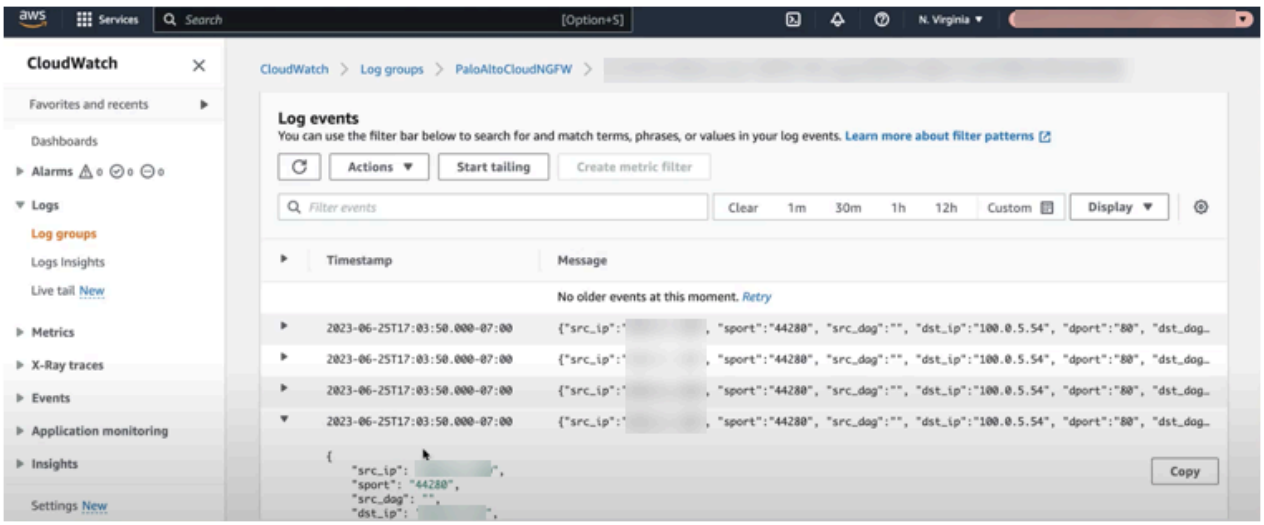
## WildFire-Übermittlungsprotokolle anzeigen

Die Anzeige von WildFire-Übermittlungsprotokollen ist möglich in:

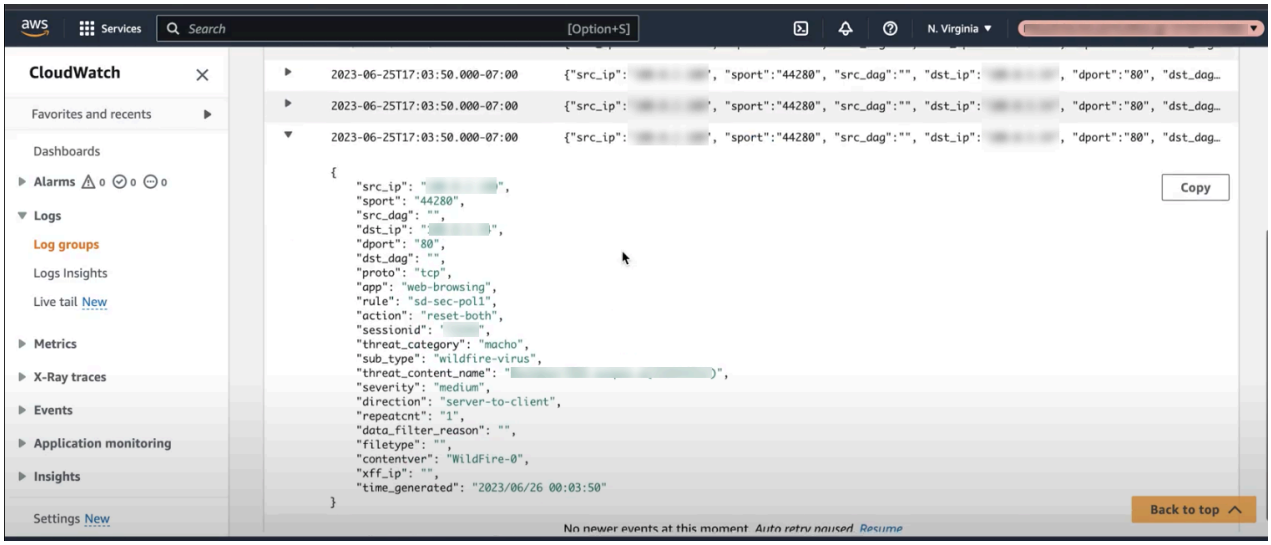
1. AWS-Protokollzielen
2. Panorama
3. Strata-Protokollierungsdienst

## Protokolle in AWS-Zielen anzeigen

Wenn Sie zuvor Amazon CloudWatch, Amazon S3 oder Amazon Kinesis als Ihr Protokollziel konfiguriert haben, können Sie diese mit WildFire auf Blöcke mit bösartigem Datenverkehr überprüfen.



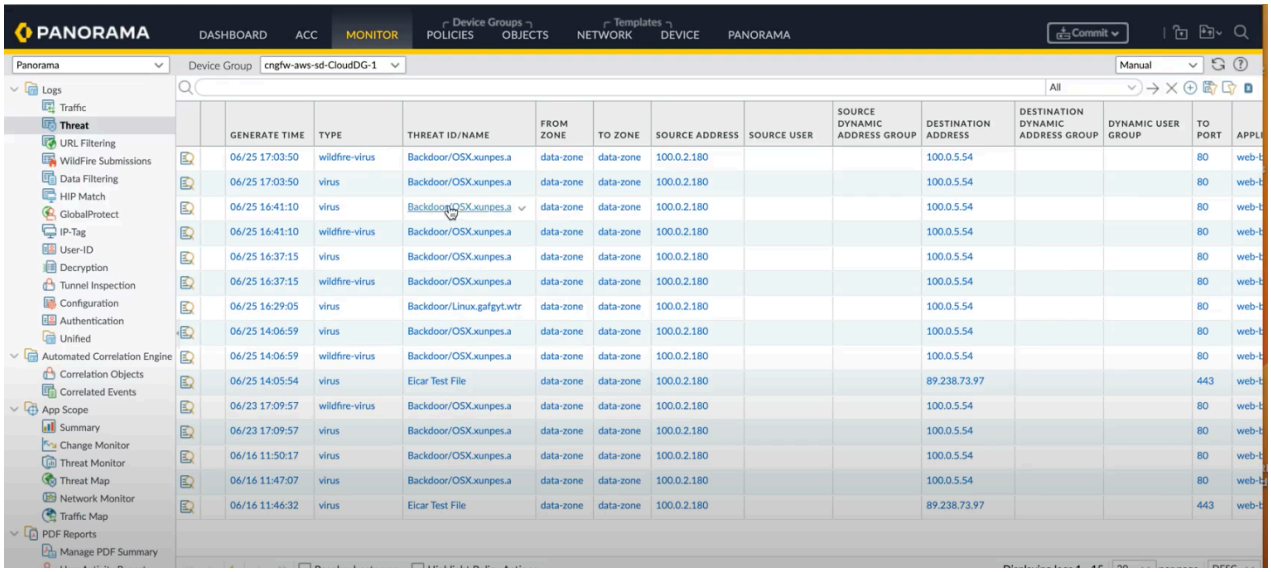

 




## Protokolle in Panorama anzeigen

In Panorama können Sie die Protokolle zur Gerätegruppe über **Monitor (Überwachen) > Threats (Bedrohungen)** anzeigen.

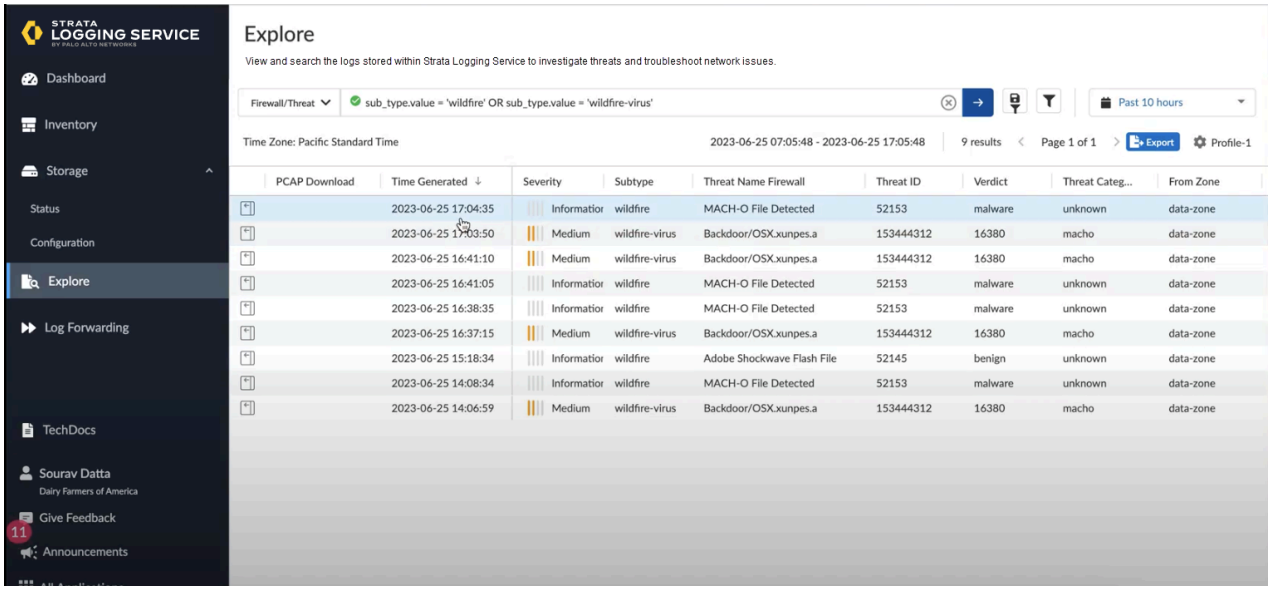


## Protokolle im Strata-Protokollierungsdienst anzeigen

Sie können WildFire-Protokolle auch in Ihrer Strata Logging Service-Instanz anzeigen.

1. Klicken Sie auf **Explore (Erkunden)** und wählen Sie aus der Dropdown-Liste „Explore“ die Option **Firewall/Threat (Firewall/Bedrohung)** aus.
2. Geben Sie `sub_typevalue = wildfire` oder `wildfire-virus` ein und filtern Sie nach WildFire-Protokollen.



# DNS Security in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

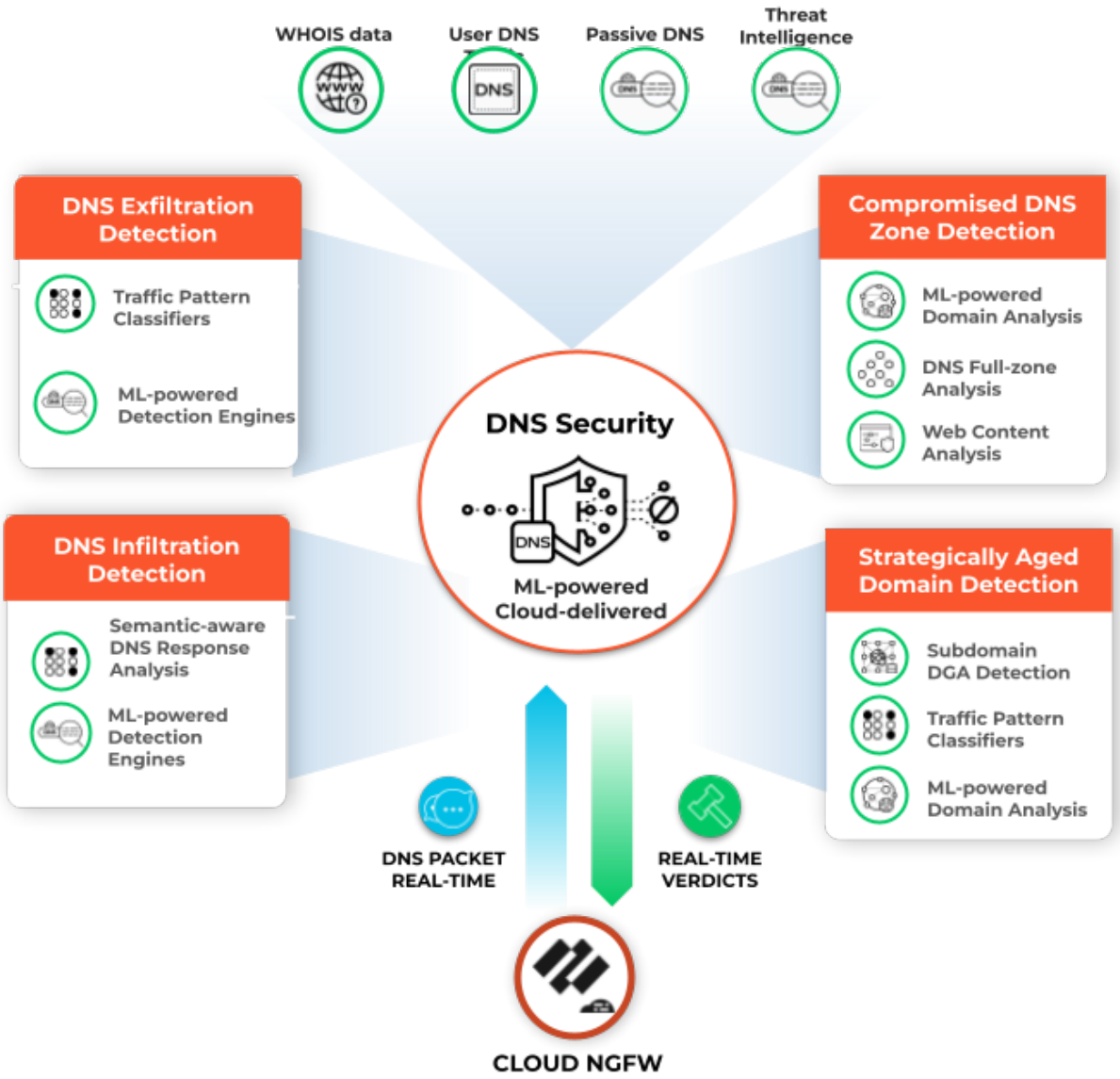
Domain Name Service (DNS) ist ein kritisches und grundlegendes Internetprotokoll, wie in den wichtigsten RFCs für das Protokoll beschrieben. Böswillige Akteure haben Command-and-Control(C2)-Kommunikationskanäle über das DNS genutzt und in einigen Fällen sogar das Protokoll verwendet, um Daten zu exfiltrieren. DNS-Exfiltration kann auftreten, wenn ein Bedrohungsakteur eine Anwendungsinstanz in Ihrer VPC kompromittiert und dann DNS-Lookup verwendet, um Daten aus der VPC an eine Domäne zu senden, die er kontrolliert. Bedrohungsakteure können auch bösartige Daten und Nutzlasten über DNS in die VPC-Workloads einschleusen. Bei Untersuchungen der Palo Alto Networks Unit 42 wurden verschiedene Arten von DNS-Missbrauch entdeckt.

Mit Cloud NGFW für AWS können Sie Ihren VPC-Datenverkehr vor erweiterten DNS-basierten Bedrohungen schützen, indem Sie die Domänen überwachen und steuern, die Ihre VPC-Ressourcen abfragen. Mit Cloud NGFW für AWS können Sie den Zugriff auf die Domänen verweigern, die Palo Alto Networks für bösartig oder verdächtig hält, und alle anderen Abfragen zulassen.

Cloud NGFW verwendet den DNS Security-Dienst von Palo Alto Networks, der bösartige Domänen proaktiv erkennt, indem er DNS-Signaturen mithilfe von erweiterten prädiktiven Analysen und maschinellem Lernen generiert und dazu Daten aus mehreren Quellen verwendet (z. B. WildFire-Verkehrsanalysen sowie Analysen von passivem DNS, aktivem Webcrawling und bösartigen Webinhalten, URL-Sandboxes, Honeynet, DGA-Reverse-Engineering, Telemetriedaten, Whois, die Forschungsorganisation Unit 42 und Cyber Threat Alliance). Anschließend wird der DNS Security-Dienst diese DNS-Signaturen kontinuierlich an Ihre Cloud NGFW-Ressourcen verteilen, um sich proaktiv vor Malware zu schützen, die DNS für C2- und Datendiebstahl nutzt.

DNS Security für Cloud NGFW erfordert Panorama. Konfigurieren Sie alle für DNS Security relevanten Richtlinienregeln in Panorama und übertragen Sie sie per Push als Teil einer Cloud-Gerätegruppe an Cloud NGFW-Ressourcen.

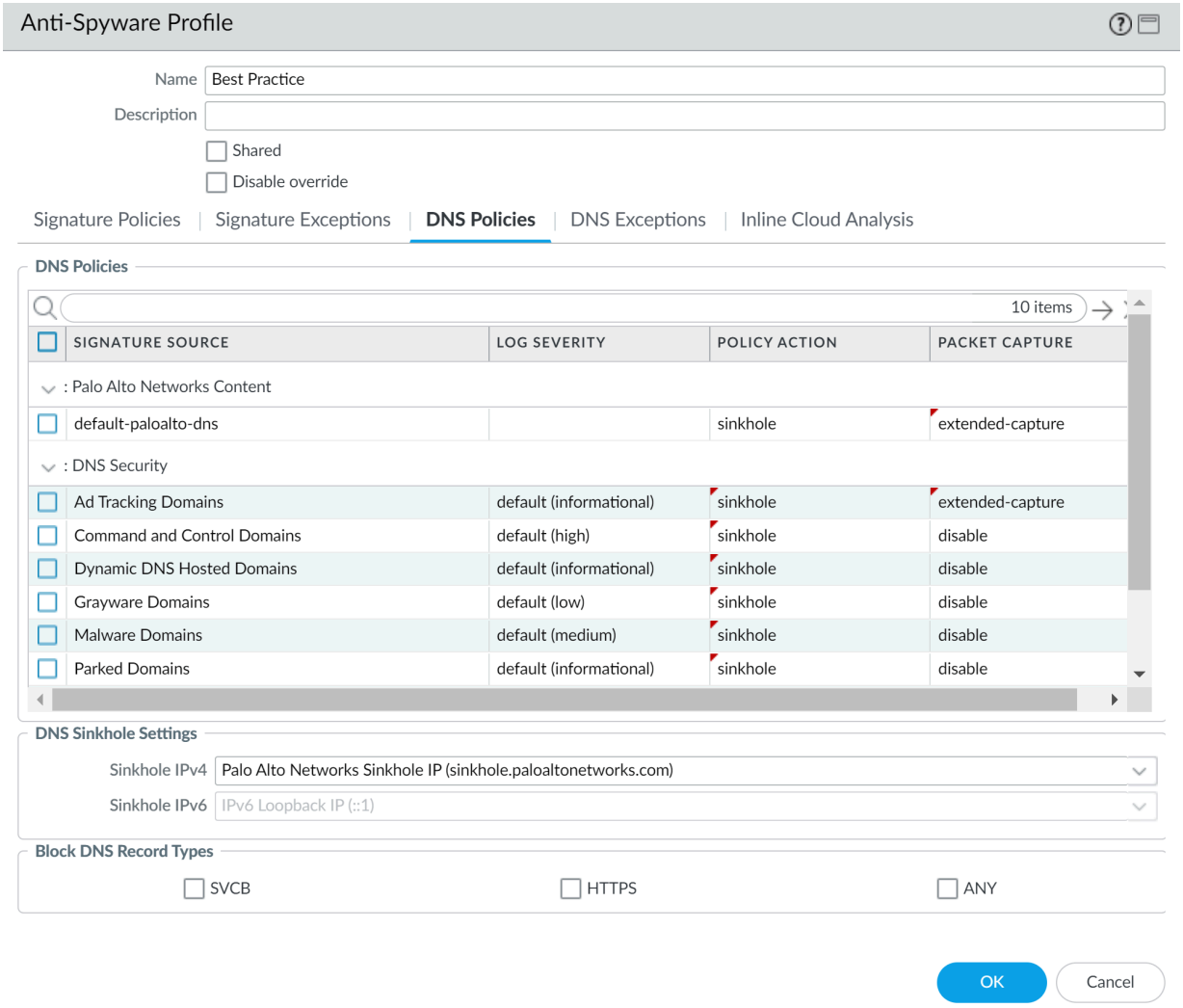
 



So aktivieren Sie DNS Security in Cloud NGFW-Ressourcen:

**STEP 1 |** Aktivieren Sie DNS Security in Panorama, indem Sie ein Anti-Spyware-Profil in Cloud-Gerätegruppen erstellen, die Ihren Cloud NGFW-Ressourcen zugeordnet sind.




**STEP 2 |** Leiten Sie Ihren DNS-Datenverkehr in Ihrer VPC an Ihre Cloud NGFW-Ressource um. Wie Sie die Datenverkehrsumleitung konfigurieren, hängt von der Einrichtung Ihres DNS-Servers ab:

- Privater DNS-Server
- DNS-Dienst Route 53
- DNS für private gehostete Zonen

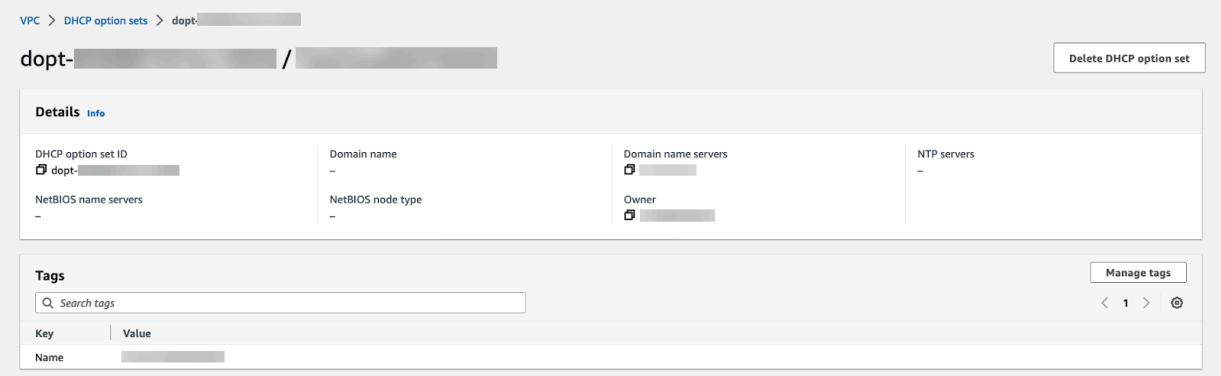
## Privater DNS-Server

Wenn Sie einen privaten oder lokalen DNS-Server verwenden, gehen Sie wie folgt vor, um den DNS-Datenverkehr an Ihre Cloud NGFW-Endpunkte weiterzuleiten.

**STEP 1 |** Melden Sie sich bei der AWS-Konsole an.

**STEP 2 |** Wählen Sie Ihre VPC und dann **DHCP option sets (DHCP-Optionssätze)** aus.

**STEP 3 |** Sie können einen neuen DHCP-Optionssatz erstellen und die IP-Adresse Ihres DNS-Servers hinzufügen. In diesem Beispiel ist 172.18.10.1 die Adresse Ihres privaten DNS-Servers. Wenn Sie bei der Konfiguration Ihres DNS-Servers eine vorhandene DHCP-Option festgelegt haben, zeigen Sie die Details an und notieren Sie sich die IP-Adresse des DNS-Servers.




**STEP 4 |** Wählen Sie **VPC** und die zu sichernde VPC aus.

**STEP 5 |** Wählen Sie aus der Dropdown-Liste **Actions (Aktionen)** die Option **Edit VPC settings (VPC-Einstellungen bearbeiten)** aus.

**STEP 6 |** Wählen Sie unter **DHCP settings (DHCP-Einstellungen)** aus der Dropdown-Liste **DHCP option set (DHCP-Optionssatz)** den für Ihren privaten DNS-Server konfigurierten DHCP-Optionssatz aus.

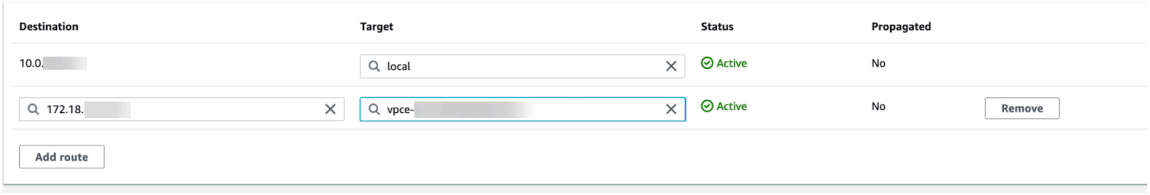
**STEP 7 |** Klicken Sie auf **Änderungen speichern**.

Die ausgewählte VPC leitet nun alle DNS-Anfragen an den konfigurierten DNS-Server weiter.

**STEP 8 |** Bearbeiten Sie Ihre Subnetz-Routentabelle.

1. Wählen Sie **VPC** > **Route tables (Routentabellen)**aus.
2. Wählen Sie die Routentabelle für das abzusichernde Subnetz aus.
3. Fügen Sie eine Route hinzu und setzen Sie „Destination“ (Zieladresse) auf die IP-Adresse Ihres DNS-Servers.




4. Klicken Sie auf **Save changes (Änderungen speichern)**.

   Jeglicher DNS-Datenverkehr aus dem geschützten Subnetz wird über den Cloud NGFW-Endpunkt und zur Überprüfung und Durchsetzung an die Cloud NGFW weitergeleitet.

### DNS-Dienst Route 53

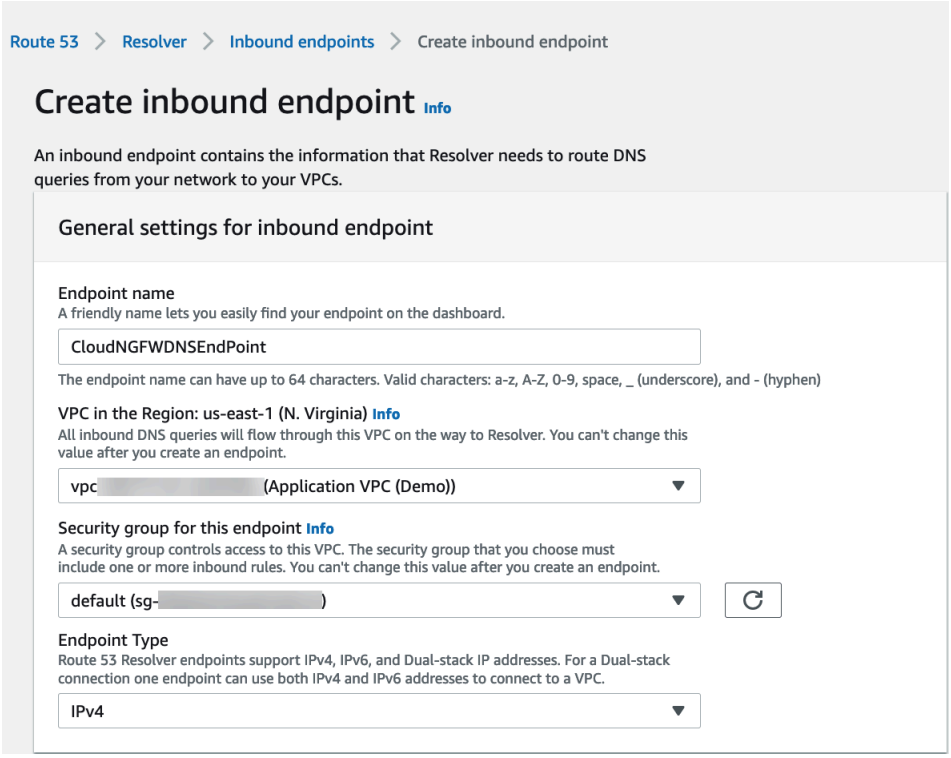
Führen Sie die folgenden Schritte aus, um den DNS-Datenverkehr in Ihren VPCs abzusichern, wenn Sie den DNS-Dienst Route 53 von Amazon verwenden. Erstellen Sie ein Subnetz in jeder Verfügbarkeitszone, die Workloads zum Bereitstellen eingehender Resolver-Endpunkte enthält.

**STEP 1 |** Melden Sie sich bei der AWS-Konsole an.

**STEP 2 |** Erstellen Sie einen eingehenden Endpunkt.

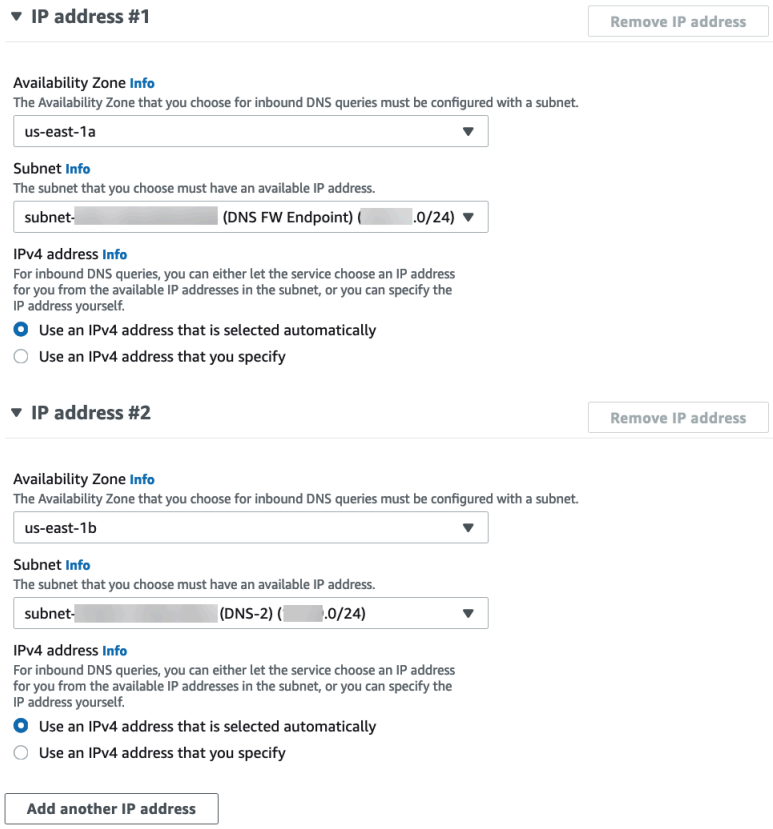
1. Wählen Sie **Services (Dienste)** > **Route 53** > **Resolver** > **Inbound Endpoints (Eingehende Endpunkte)** aus.
2. Klicken Sie auf **Create inbound endpoint (Eingehenden Endpunkt erstellen)**.
3. Geben Sie einen beschreibenden **Namen** ein.
4. Wählen Sie die VPC für den Endpunkt aus.
5. Fügen Sie eine Sicherheitsgruppe für diesen Endpunkt hinzu.
6. Setzen Sie **Endpoint Type (Endpunkttyp)** auf „IPv4“.




7. Wählen Sie die Verfügbarkeitszone aus.
8. Wählen Sie das Subnetz aus, das Sie oben erstellt haben.

*Wenn mehr als eine Verfügbarkeitszone vorhanden ist, müssen Sie jeweils die Verfügbarkeitszone und das entsprechende Subnetz angeben.*

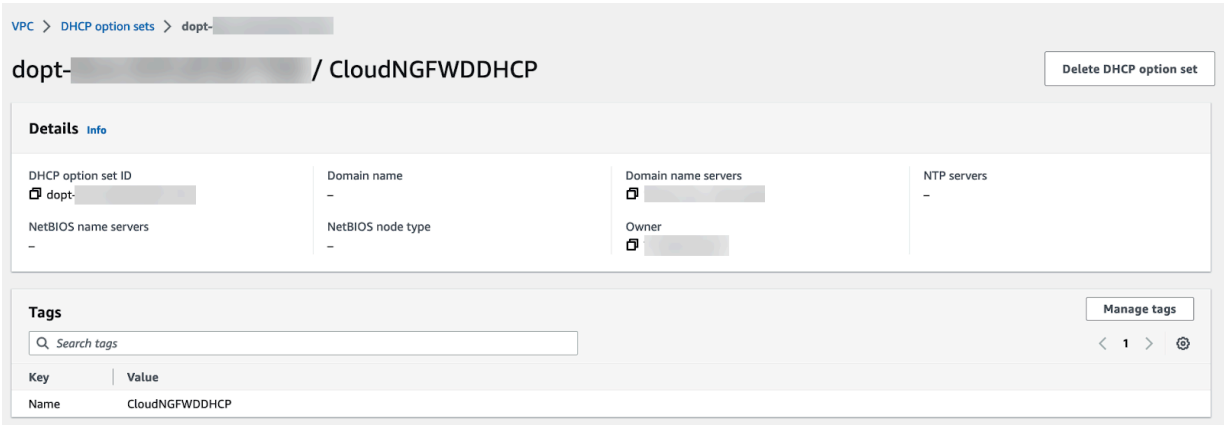
 




9. Klicken Sie auf **Create inbound endpoint (Eingehenden Endpunkt erstellen)**.
10. Beachten Sie die IP-Adresse, die jedem Subnetz zugeordnet ist, das mit Ihrem eingehenden Endpunkt verbunden ist. Verwenden Sie diese IP-Adressen bei der Konfiguration Ihrer **DHCP-Optionssätze** in den folgenden Schritten.

**STEP 3 |** Wählen Sie **VPC** > **DHCP option sets (DHCP-Optionssätze)** aus.

**STEP 4 |** Sie können einen neuen DHCP-Optionssatz erstellen und die IP-Adresse für jede Verfügbarkeitszone hinzufügen. Wenn mehrere Verfügbarkeitszonen vorhanden sind, geben Sie alle IP-Adressen als durch Kommas getrennte Liste ein.

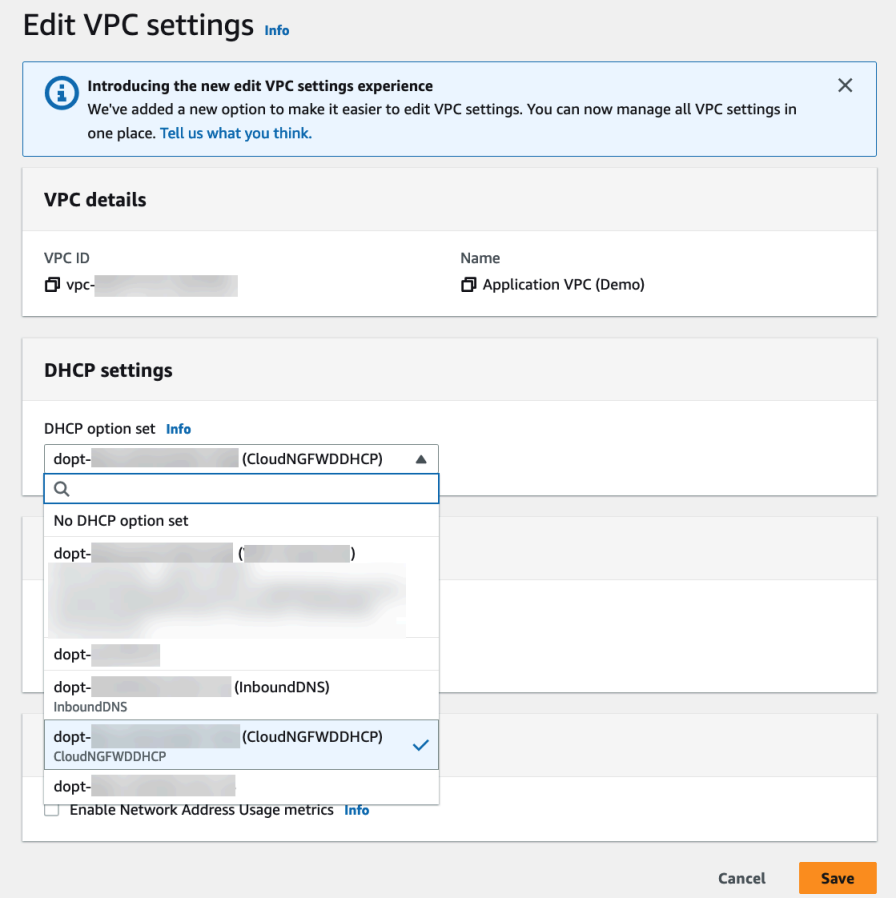


**STEP 5 |** Wählen Sie **VPC** und die zu sichernde VPC aus.

**STEP 6 |** Wählen Sie aus der Dropdown-Liste **Actions (Aktionen)** die Option **Edit VPC settings (VPC-Einstellungen bearbeiten)** aus.

**STEP 7 |** Wählen Sie unter **DHCP settings (DHCP-Einstellungen)** den oben erstellten DHCP-Optionssatz aus der Dropdown-Liste **DHCP option set (DHCP-Optionssatz)** aus.



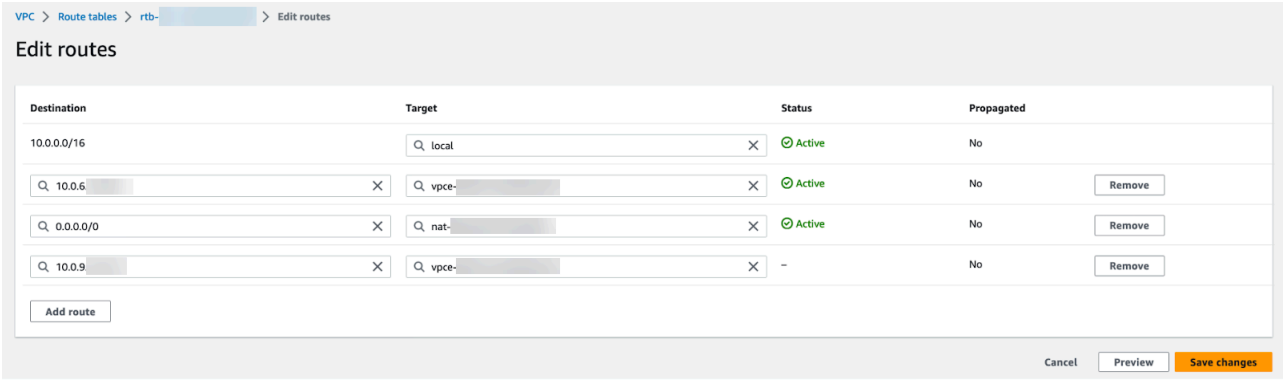

**STEP 8 |** Klicken Sie auf **Änderungen speichern**.

Die ausgewählte VPC leitet nun alle DNS-Anfragen an den konfigurierten DNS-Server weiter.

**STEP 9 |** Bearbeiten Sie Ihre Subnetz-Routentabelle.

1. Wählen Sie **VPC** > **Route Tables (Routentabellen)** aus.
2. Wählen Sie die Routentabelle für das abzusichernde Subnetz aus.
3. Fügen Sie eine Route hinzu und setzen Sie „Destination“ (Zieladresse) auf die IP-Adresse Ihres DNS-Servers und „Target“ (Ziel) auf den Cloud NGFW-Endpunkt.




4. Klicken Sie auf **Änderungen speichern**.

   Jeglicher DNS-Datenverkehr aus dem geschützten Subnetz wird über den Cloud NGFW-Endpunkt und zur Überprüfung und Durchsetzung an die Cloud NGFW weitergeleitet.

## DNS für private gehostete Zonen

Informationen zum Erstellen einer privaten gehosteten Zone in AWS finden Sie unter Private gehostete Zone erstellen.

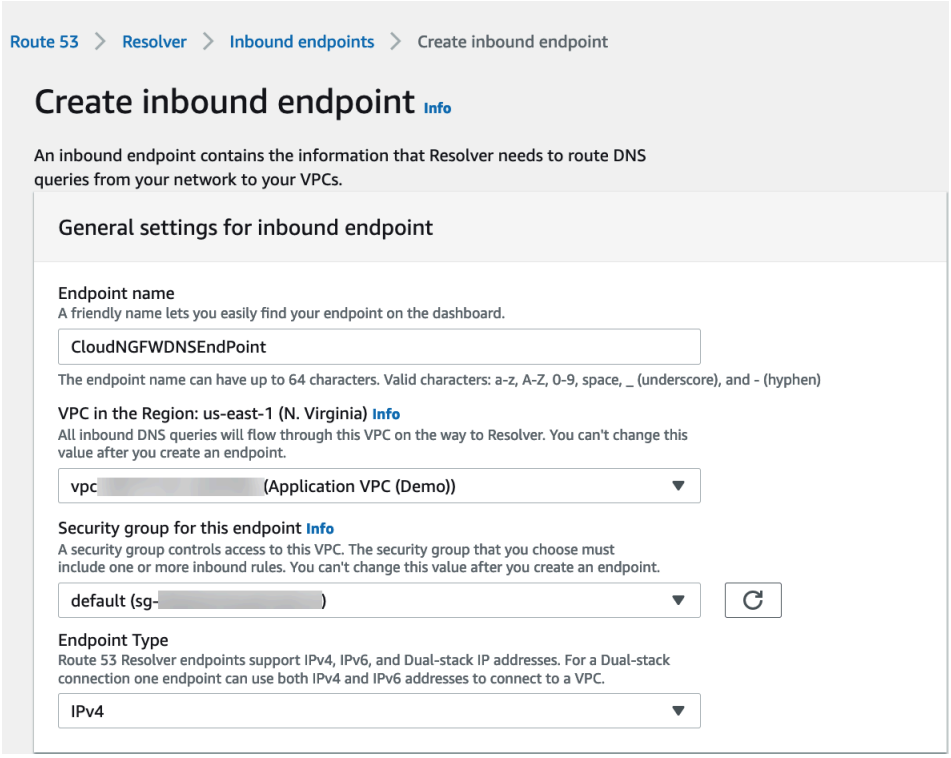
Damit Ihre Cloud NGFW-Ressource Route 53-Resolver für alle DNS-Zonen (z. B. private Zonen), die auf Route 53 gehostet werden, abfragen kann, erstellen Sie einen eingehenden Route 53-Endpunkt, wie oben beschrieben. Der eingehende Endpunkt ist eine Brücke für andere Dienste, um Route 53 nach der Auflösung von Domänennamen abzufragen. Wenn Sie einen eingehenden Endpunkt erstellen, erstellt AWS eine elastische Netzwerkschnittstelle (Elastic Network Interface, ENI) in jeder Verfügbarkeitszone (Availability Zone, AZ), die Sie für das Empfangen eingehender DNS-Abfragen angeben.

**STEP 1 |** Öffnen Sie die Amazon VPC-Konsole.

**STEP 2 |** Erstellen Sie einen eingehenden Endpunkt.

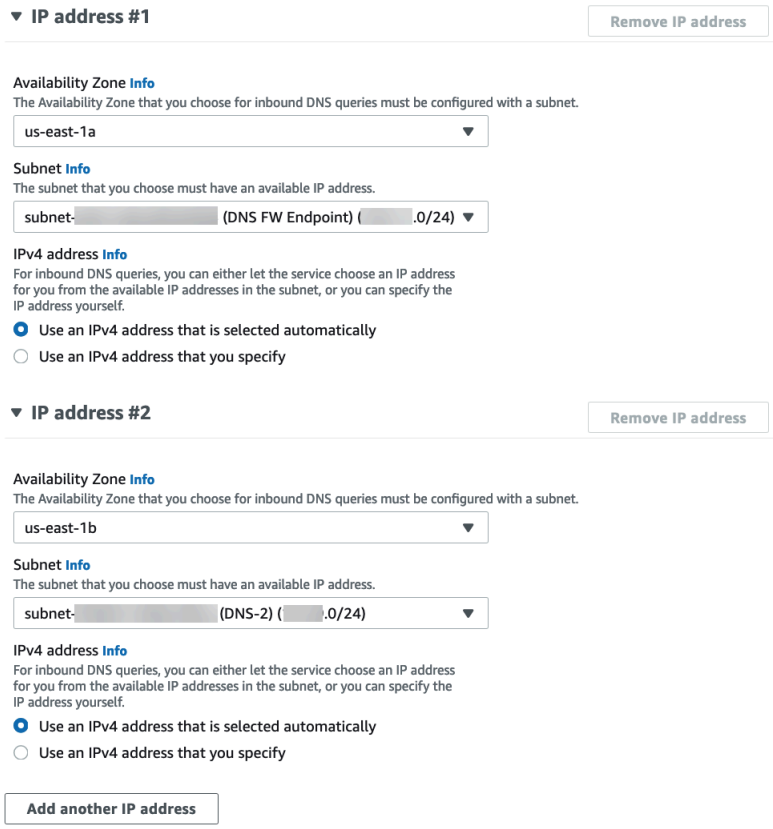
1. Wählen Sie **Services (Dienste)** > **Route 53** > **Resolver** > **Inbound Endpoints (Eingehende Endpunkte)** aus.
2. Klicken Sie auf **Create inbound endpoint (Eingehenden Endpunkt erstellen)**.
3. Geben Sie einen beschreibenden **Namen** ein.
4. Wählen Sie die VPC für den Endpunkt aus.
5. Fügen Sie eine Sicherheitsgruppe für diesen Endpunkt hinzu.
6. Setzen Sie **Endpoint Type (Endpunkttyp)** auf „IPv4“.




7. Wählen Sie die Verfügbarkeitszone aus.
8. Wählen Sie das Subnetz aus, das Sie oben erstellt haben.

*Wenn mehr als eine Verfügbarkeitszone vorhanden ist, müssen Sie jeweils die Verfügbarkeitszone und das entsprechende Subnetz angeben.*

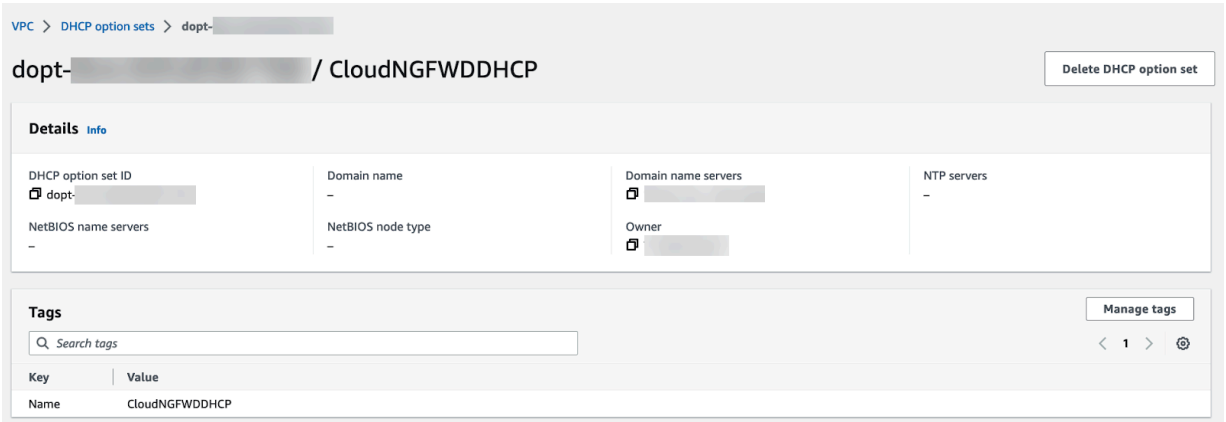
 




9. Klicken Sie auf **Create inbound endpoint (Eingehenden Endpunkt erstellen)**.
10. Beachten Sie die IP-Adresse, die jedem Subnetz zugeordnet ist, das mit Ihrem eingehenden Endpunkt verbunden ist. Verwenden Sie diese IP-Adressen bei der Konfiguration Ihrer **DHCP-Optionssätze** in den folgenden Schritten.

**STEP 3 |** Wählen Sie **VPC** > **DHCP option sets (DHCP-Optionssätze)** aus.

**STEP 4 |** Sie können einen neuen DHCP-Optionssatz erstellen und die IP-Adresse für jede Verfügbarkeitszone hinzufügen. Wenn mehrere Verfügbarkeitszonen vorhanden sind, geben Sie alle IP-Adressen als durch Kommas getrennte Liste ein.

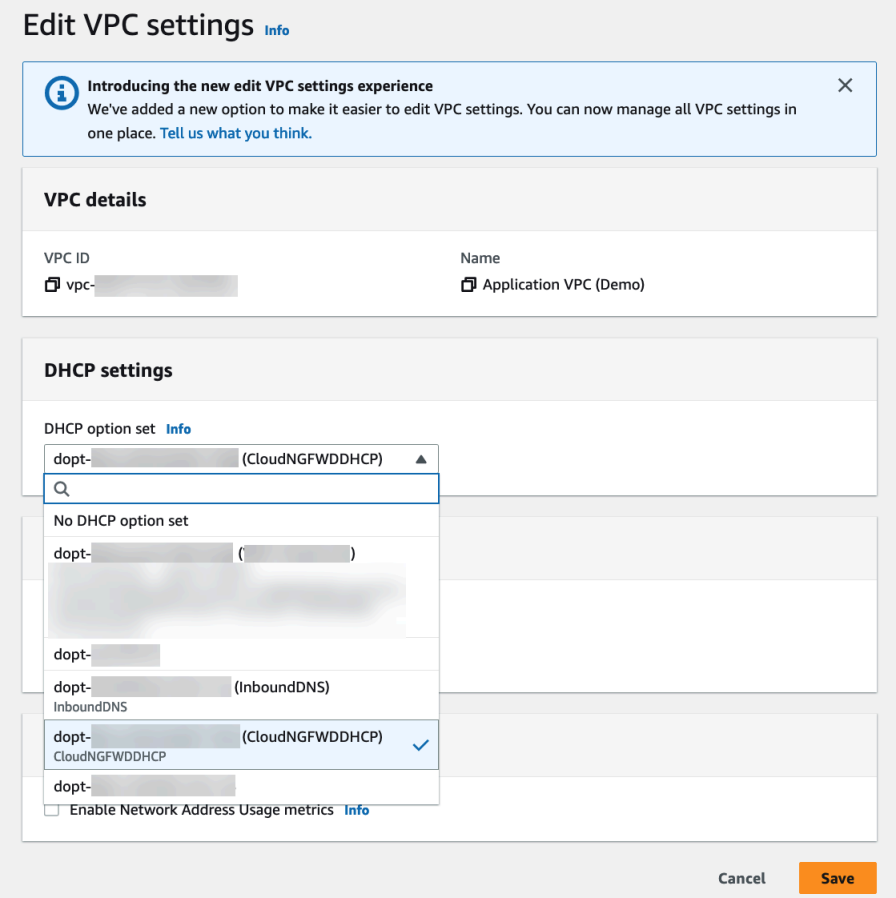


**STEP 5 |** Wählen Sie **VPC** und die zu sichernde VPC aus.

**STEP 6 |** Wählen Sie aus der Dropdown-Liste **Actions (Aktionen)** die Option **Edit VPC settings (VPC-Einstellungen bearbeiten)** aus.

**STEP 7 |** Wählen Sie unter **DHCP settings (DHCP-Einstellungen)** den oben erstellten DHCP-Optionssatz aus der Dropdown-Liste **DHCP option set (DHCP-Optionssatz)** aus.

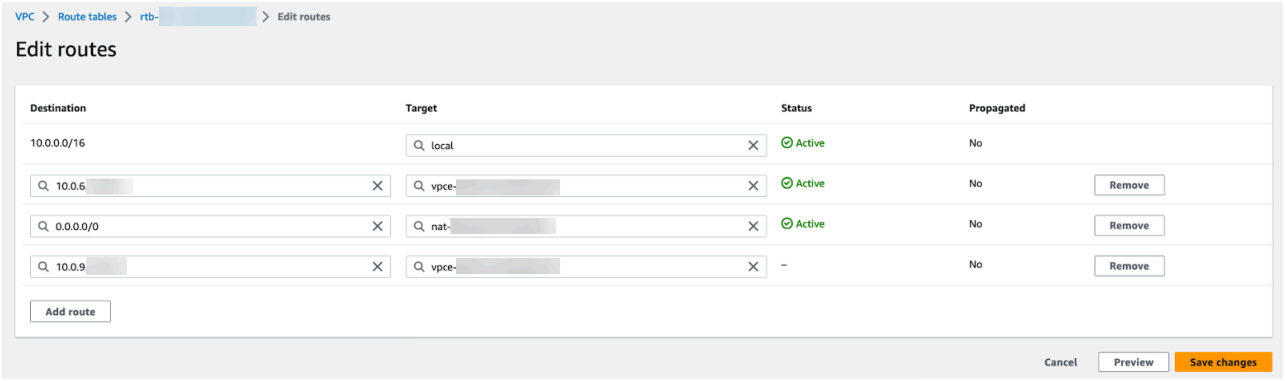



**STEP 8 |** Klicken Sie auf **Änderungen speichern**.

**STEP 9 |** Bearbeiten Sie Ihre Subnetz-Routentabelle.

1. Wählen Sie **VPC** > **Route Tables (Routentabellen)** aus.
2. Wählen Sie die Routentabelle für das abzusichernde Subnetz aus.
3. Fügen Sie eine Route hinzu und setzen Sie „Destination“ (Zieladresse) auf die IP-Adresse Ihres DNS-Servers und „Target“ (Ziel) auf den Cloud NGFW-Endpunkt.




4. Klicken Sie auf **Änderungen speichern**.

   Jeglicher DNS-Datenverkehr aus dem geschützten Subnetz wird über den Cloud NGFW-Endpunkt und zur Überprüfung und Durchsetzung an die Cloud NGFW weitergeleitet.

# Enterprise-Data-Loss-Prevention(E-DLP)-Integration mit Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Enterprise Data Loss Prevention (E-DLP) umfasst eine Reihe von Tools und Prozessen, mit denen Sie vertrauliche Informationen vor unbefugtem Zugriff, Missbrauch, Extraktion oder Weitergabe schützen können. Weitere Informationen finden Sie unter Über Enterprise DLP.

Sie können E-DLP in Cloud NGFW für AWS integrieren und die Panorama-Konsole verwenden, um Datenfilterungsprofile zu Ihren Sicherheitsrichtlinienregeln hinzuzufügen.

**Mindestanforderungen**

Im Folgenden sind die kombinierten Versionsanforderungen für Panorama und Panorama-Plug-ins für die Integration von E-DLP in Ihren Cloud NGFW-Dienst aufgeführt:

| Panorama-Version (PAN-OS) | DLP-Plug-in | AWS-Plug-in |
|---|---|---|
| 10.0.2 und höher | 1.0.9 | 5.2.0 |
| 10.2.4 und höher | 3.0.7 | 5.2.0 |
| 11.0.2 und höher | 4.0.3 | 5.2.0 |
| 11.1.0 und höher | 5.0.1 | 5.2.0 |

## Neuen E-DLP-Mandanten in Cloud NGFW für AWS bereitstellen

Wenn Sie über einen DLP-Mandanten in Ihrem Customer-Support-Portal(CSP)-Konto verfügen, der in Panorama bereitgestellt wird, verwendet der Cloud NGFW-Dienst diesen DLP-Mandanten, um DLP in Cloud NGFW zu integrieren.

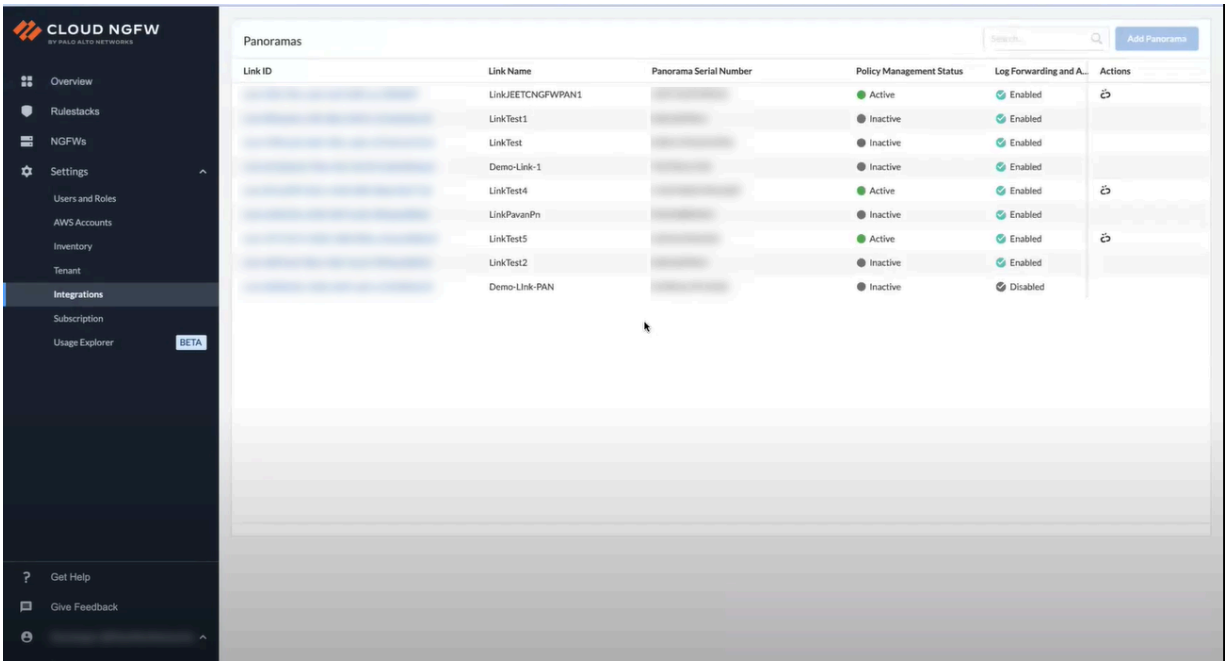
Wenn Sie keinen DLP-Mandanten in Ihrem Customer-Support-Portal-Konto haben, erstellt der Cloud NGFW-Dienst einen neuen DLP-Mandanten.

Verwenden Sie die folgenden Schritte zum Aktivieren eines neuen DLP-Mandanten in der Cloud NGFW-Konsole:

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

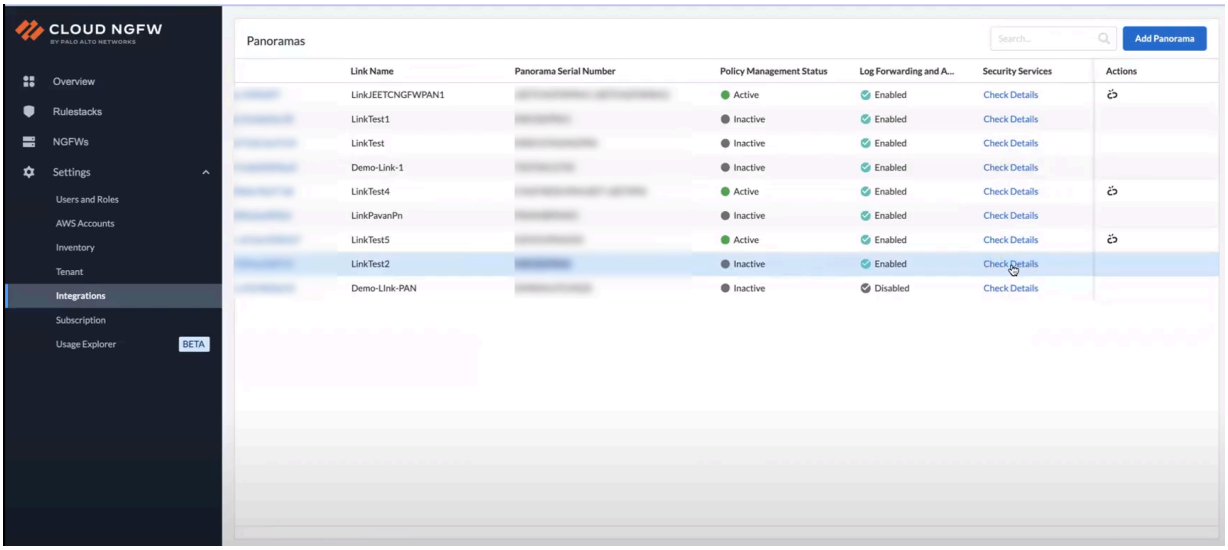
 

**STEP 2 |** Wählen Sie **Integrations (Integrationen)** aus.



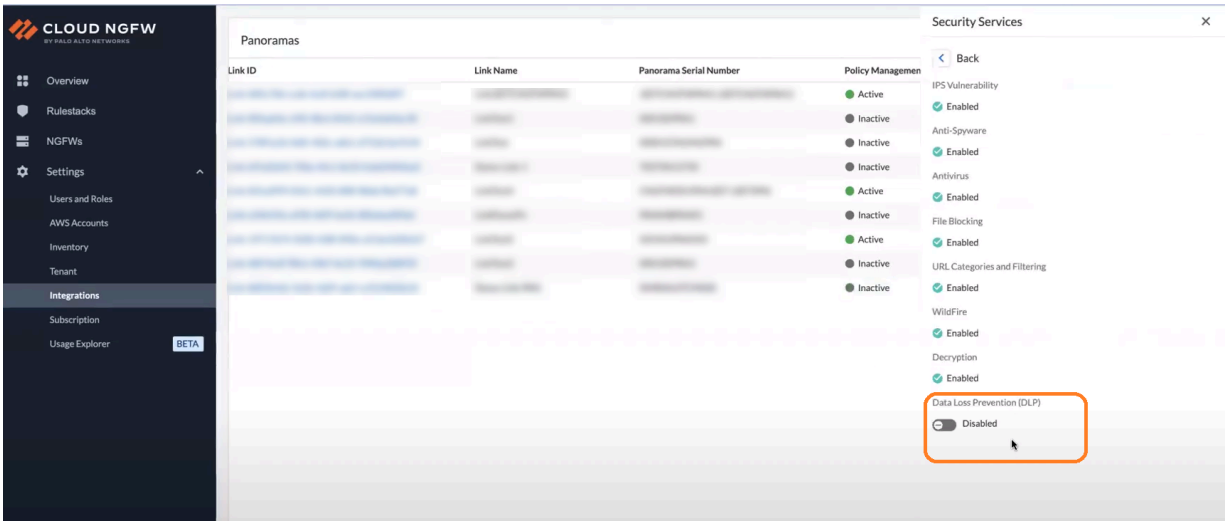
**STEP 3 |** Klicken Sie in der Spalte „Security Service“ (Sicherheitsdienst) auf **Check Details (Details prüfen)**.




*Sie können auch auf die **Verknüpfungs-ID** einer verknüpften Panorama-Instanz und anschließend auf **Check Details (Details prüfen)** klicken.*

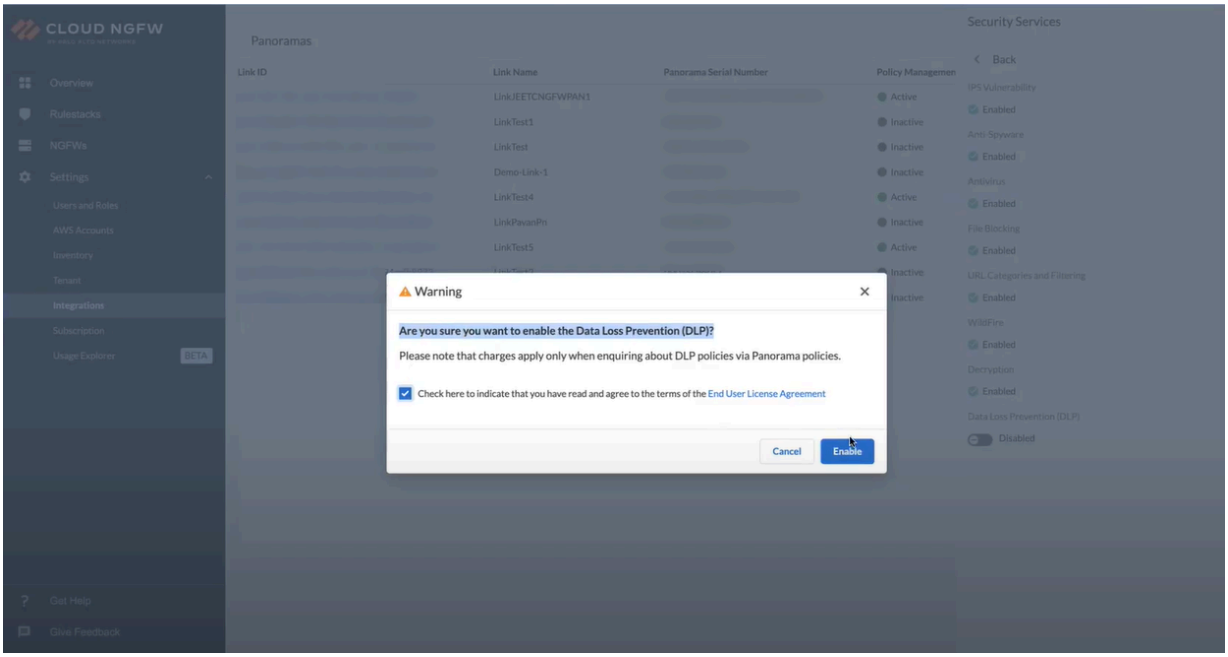
 

**STEP 4 |** Klicken Sie im Fenster **Security Services (Sicherheitsdienste)** auf den Umschalter **Data Loss Prevention (DLP)**.



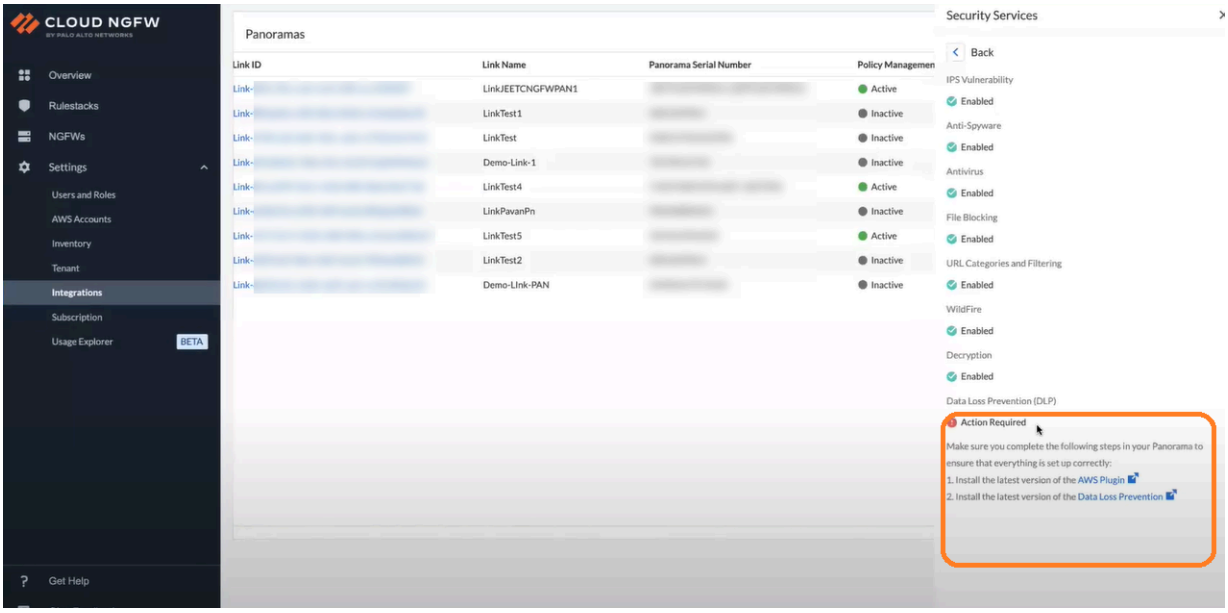

 

**STEP 5 |** Aktivieren Sie das Kontrollkästchen, um die **Endbenutzer-Lizenzvereinbarung** zu akzeptieren, und klicken Sie anschließend auf **Enable (Aktivieren)**.



**STEP 6 |** Überprüfen Sie die **erforderliche Maßnahme** in der verknüpften Panorama-Instanz.

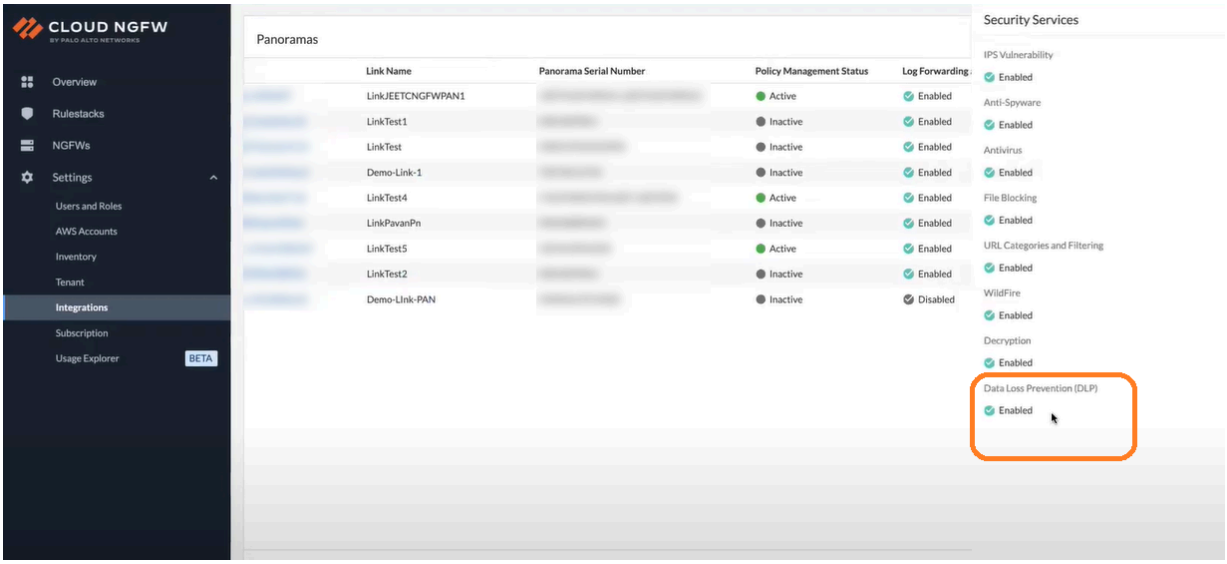



Stellen Sie sicher, dass die verknüpfte Panorama-Instanz die weiter oben auf dieser Seite angeführten minimalen Systemanforderungen erfüllt, um DLP in Ihren Cloud NGFW-Dienst integrieren zu können.

Nachdem Sie das erforderliche AWS- und DLP-Plug-in auf Ihrer Panorama-Instanz installiert haben, wird der DLP-Mandant in einer Cloud NGFW-Konsole aktiviert.

Wechseln Sie in der Cloud NGFW-Konsole auf die Seite **Integrations (Integrationen)**, wählen Sie die verknüpfte Panorama-Instanz aus und klicken Sie dann in der Spalte **Security Services (Sicherheitsdienste)** auf **Check Details (Details prüfen)**.

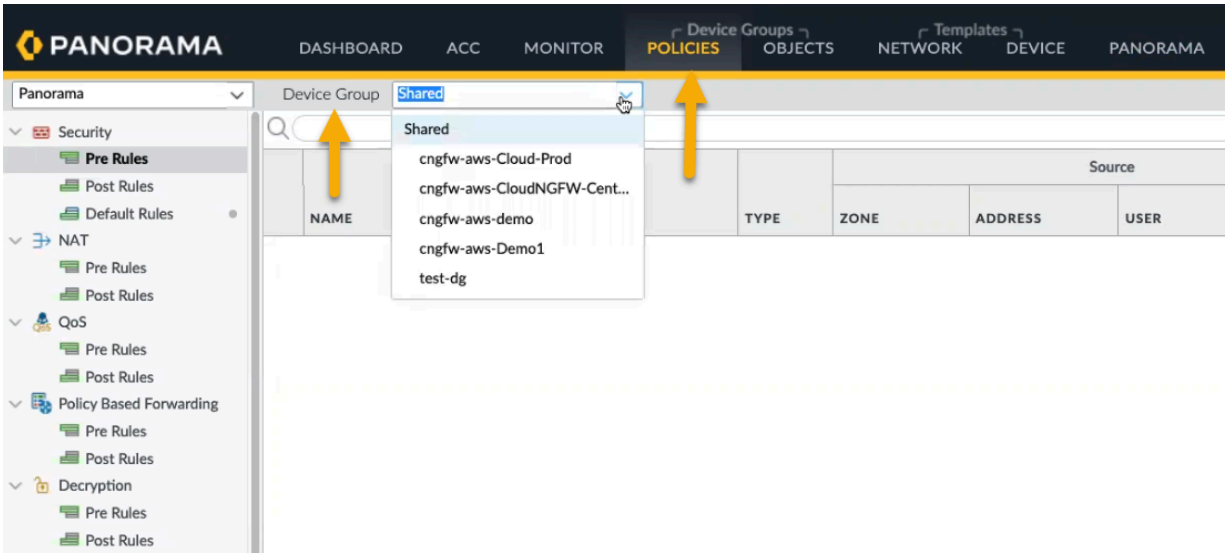



Jetzt sehen Sie, dass **Data Loss Prevention (DLP)** aktiviert wurde.

Nachdem Sie den DLP-Mandanten erfolgreich in der Cloud NGFW-Konsole aktiviert haben, können Firewalls, die der verknüpften Panorama-Instanz zugeordnet sind, mit der Verwendung der DLP-Dienste beginnen.

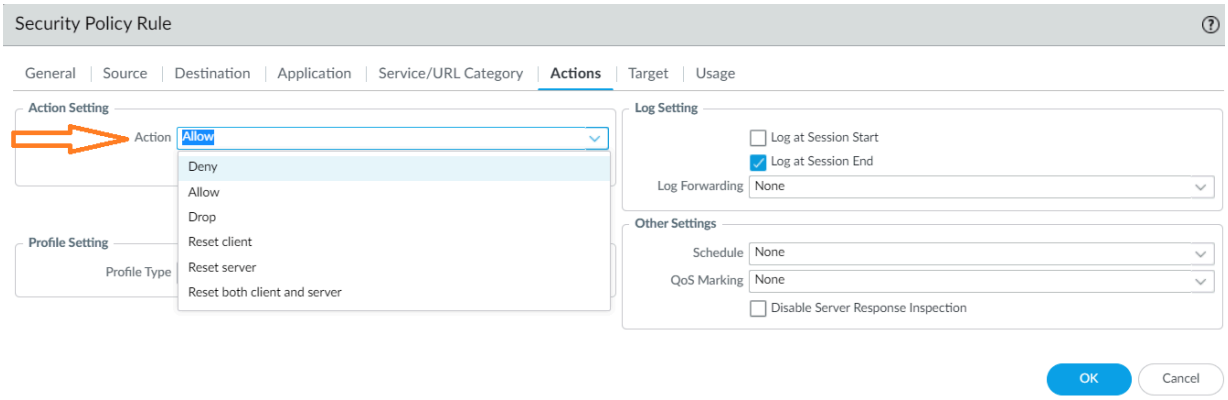
Sie können ein DLP-Filterprofil zu Ihrer **Sicherheitsrichtlinienregel** für Ihre Firewall in Panorama hinzufügen.



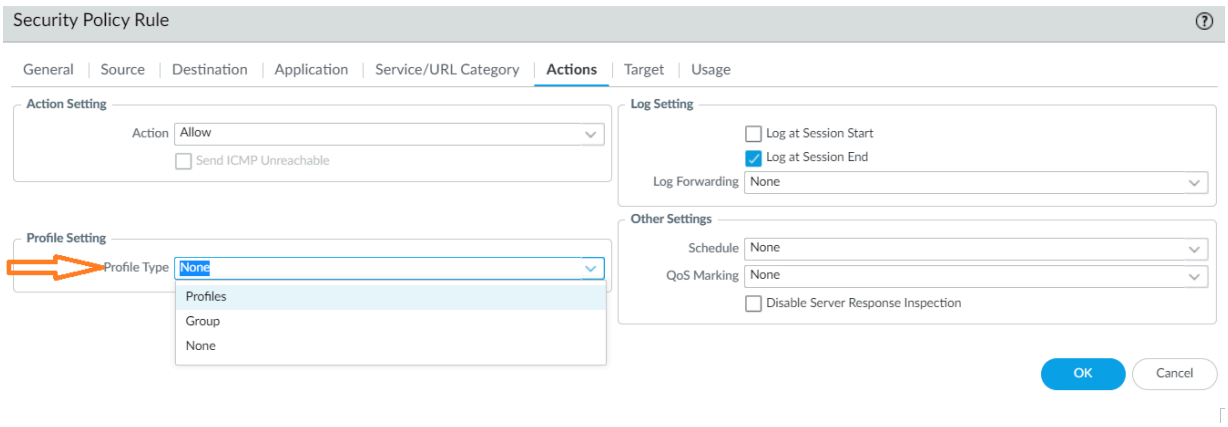

Wechseln Sie im Bildschirm **Security Policy Rule (Sicherheitsrichtlinienregel)** zur Registerkarte **Actions (Aktionen)** und wählen Sie anschließend die auszuführende Aktion aus, z. B. „allow“ (Zulassen) oder „deny“ (Verweigern).



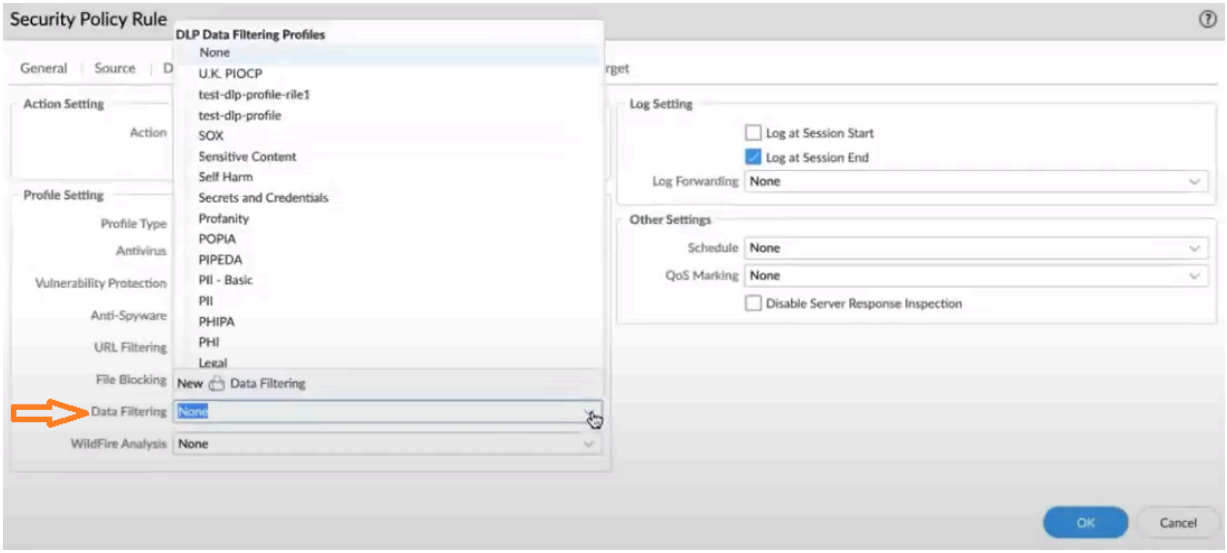

Legen Sie die **Profileinstellung** fest.



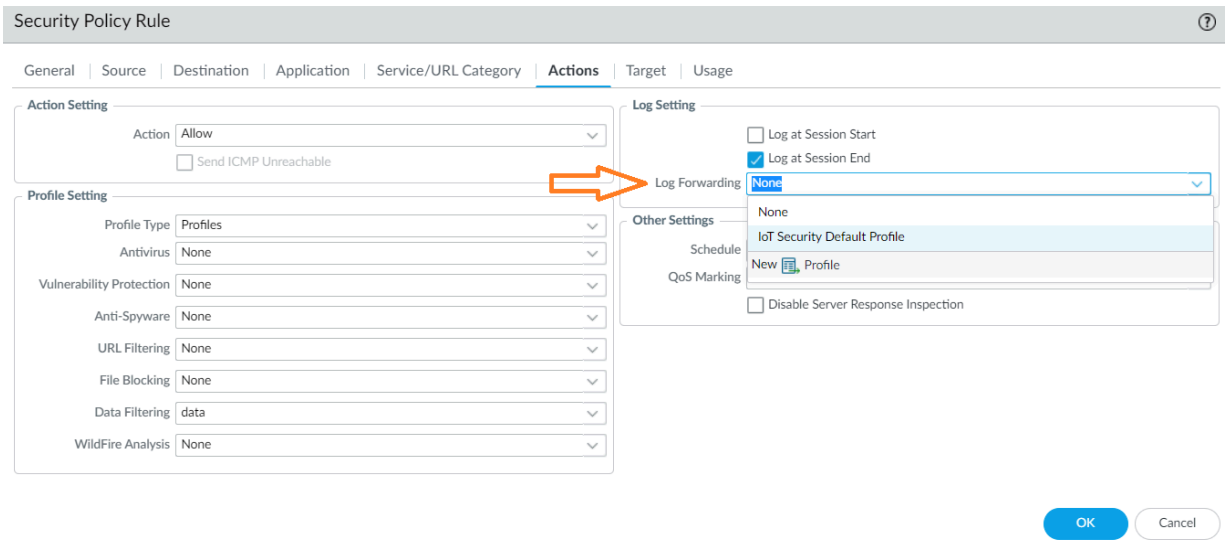

Wählen Sie ein **DLP-Datenfilterungsprofil** aus.




Konfigurieren Sie die **Protokolleinstellung** und andere Einstellungen.

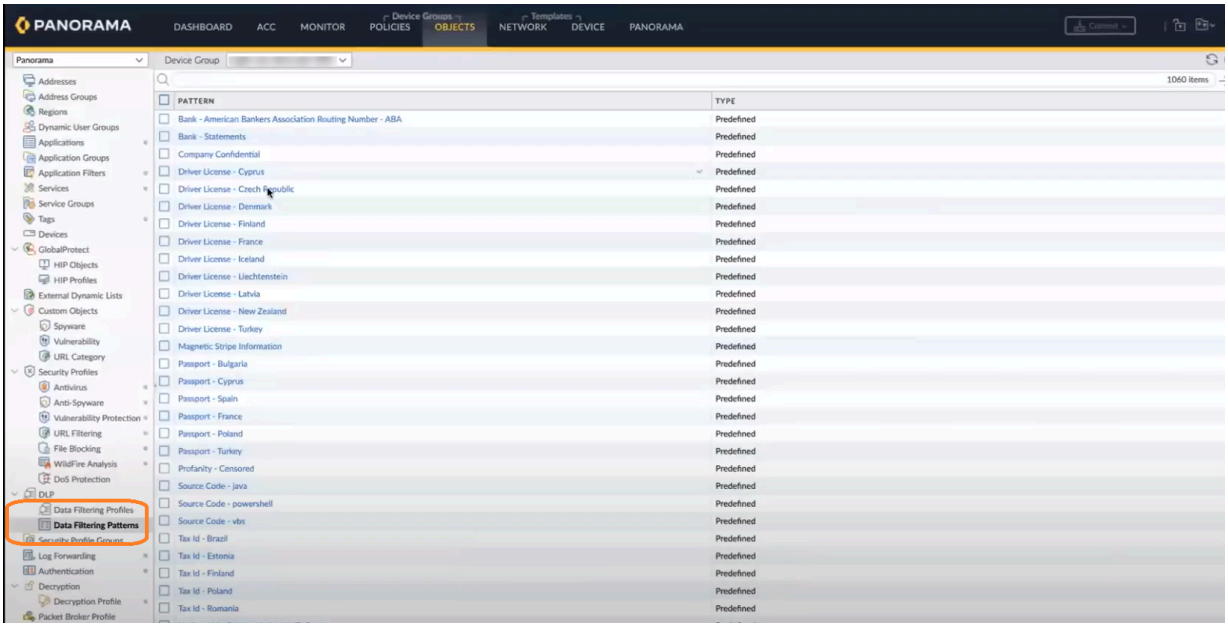
 




Weitere Informationen finden Sie unter Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden.

Nachdem Sie die Sicherheitsrichtlinienregel per Push an Ihre Firewall übertragen haben, können Sie vorhandene Datenfilterungsprofile und Datenfilterungsmuster anzeigen, die Sie für Ihren DLP-Mandanten verwenden können.

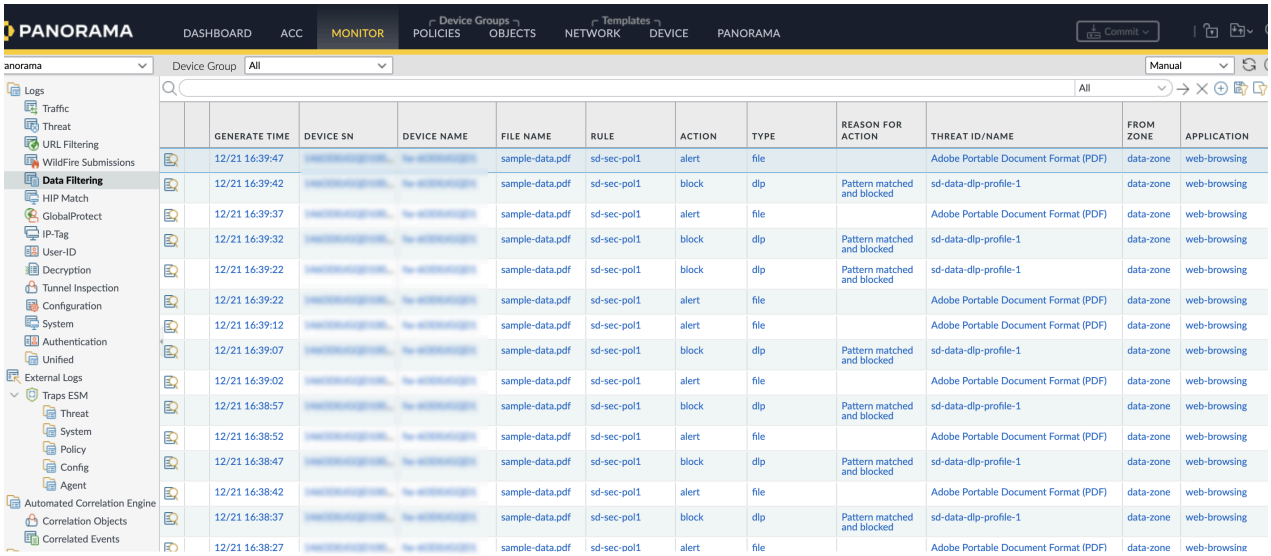


### DLP-Protokolldetails überwachen

Um Ihre DLP-Protokolle in Panorama anzuzeigen, klicken Sie auf die Registerkarte **Monitor (Überwachen)** und wechseln Sie anschließend zu **Logs (Protokolle)** > **Data Filtering (Datenfilterung)**. Weitere Informationen finden Sie unter Enterprise DLP-Protokolldetails in Panorama anzeigen.

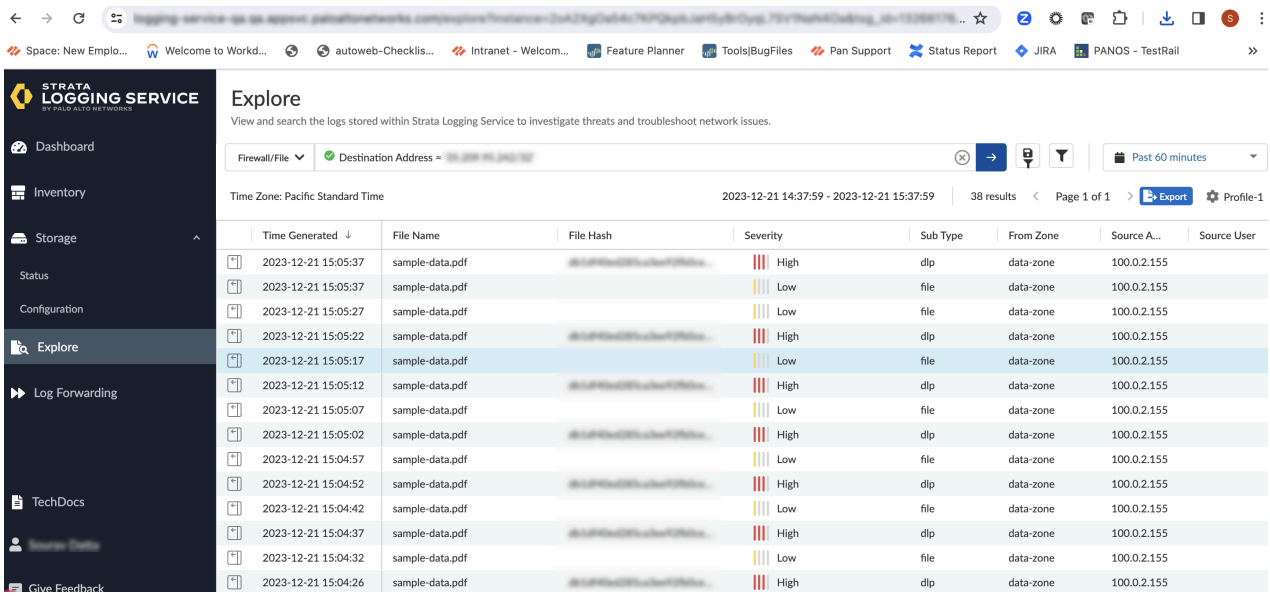



Zum Anzeigen der Protokolle Ihres Strata-Protokollierungsdienstes für DLP wechseln Sie zur Registerkarte **Explore (Erkunden)** und wählen Sie die Option **Firewall or File (Firewall oder Datei)**

aus. Weitere Informationen finden Sie unter View Log Details in der Dokumentation zum Strata-Protokollierungsdienst.

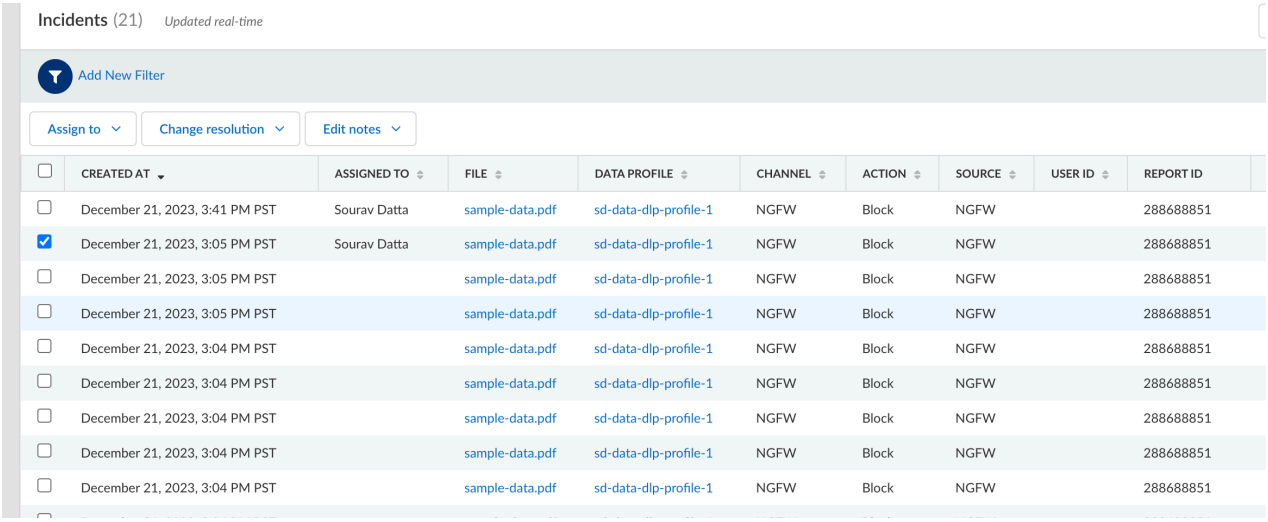
 



Informationen zum Anzeigen Ihrer DLP-Mandantenvorfallprotokolle in SCM finden Sie unter Enterprise DLP-Protokolldetails in Strata Cloud Manager anzeigen.



Incidents (21) *Updated real-time*

Add New Filter

Assign to | Change resolution | Edit notes

| CREATED AT | ASSIGNED TO | FILE | DATA PROFILE | CHANNEL | ACTION | SOURCE | USER ID | REPORT ID |
|---|---|---|---|---|---|---|---|---|
| December 21, 2023, 3:41 PM PST | Sourav Datta | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:05 PM PST | Sourav Datta | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:05 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:05 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:04 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:04 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:04 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:04 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |
| December 21, 2023, 3:04 PM PST | | sample-data.pdf | sd-data-dlp-profile-1 | NGFW | Block | NGFW | | 288688851 |

Weitere Informationen zu AWS-Zielen in DLP-Protokollen finden Sie unter Amazon CloudWatch-Protokolle.

# Native Richtlinienverwaltung in Cloud NGFW

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

In Cloud NGFW definieren Sie Sicherheitsrichtlinienregeln und gruppieren diese Regeln in einem Regelstapel.

Sicherheitsrichtlinienregeln ermöglichen es Ihnen zwar, Datenverkehr in Ihrem Netzwerk zuzulassen oder zu blockieren, Sicherheitsprofile helfen Ihnen jedoch, eine Regel für `Zulassen aber Überprüfen` zu definieren, die zugelassene Anwendungen auf Bedrohungen wie Malware, Spyware und DDoS-Angriffe überprüft. Wenn der Datenverkehr mit der in der Sicherheitsrichtlinienregel definierten `Zulassungsregel` übereinstimmt, werden die der Regel beigefügten Sicherheitsprofile für weitere Inhaltsprüfungsregeln wie Antivirenprüfungen und Datenfilterung angewendet.

Sicherheitsprofile werden nicht in den Übereinstimmungskriterien eines Datenverkehrsflusses verwendet. Das Sicherheitsprofil wird angewendet, um Datenverkehr zu scannen, nachdem die Anwendung oder Kategorie durch die Sicherheitsrichtlinienregel zugelassen wurde.

Die Firewall stellt Standardsicherheitsprofile bereit, die Sie direkt verwenden können, um mit dem Schutz Ihres Netzwerks vor Bedrohungen zu beginnen. Informationen zur Verwendung der Standardprofile in Ihrer Sicherheitsrichtlinienregel finden Sie im Abschnitt Set Up a Basic Security Policy.

Empfehlungen zu den Best Practice-Einstellungen für Sicherheitsprofile finden Sie im Abschnitt zu den Best Practices zum Erstellen von Sicherheitsprofilen.

Sie können Sicherheitsprofile hinzufügen, die häufig zusammen zum Erstellen einer Sicherheitsprofilgruppe angewendet werden. Dieser Satz von Profilen wird als Einheit behandelt und in einem Schritt zu den Sicherheitsrichtlinienregeln hinzugefügt (oder standardmäßig in die Sicherheitsrichtlinienregeln aufgenommen, wenn Sie eine Standard-Sicherheitsprofilgruppe einrichten möchten).

Sicherheitsprofile bieten grundlegenden Schutz, indem sie den Datenverkehr, den Sie im Netzwerk zulassen, auf Bedrohungen scannen. Mit Sicherheitsprofilen erhalten Sie eine vollständige Suite koordinierter Tools zur Bedrohungsabwehr, die den Peer-to-Peer-Control-and-Command(C2)-Anwendungsdatenverkehr, gefährliche Dateitypen, Versuche zur Ausnutzung von Sicherheitslücken bzw. Antivirus-Signaturen blockieren sowie neue und unbekannte Malware identifizieren.

Das Anwenden von Sicherheitsprofilen erfordert relativ wenig Aufwand, da Palo Alto Networks vordefinierte Profile bereitstellt, die Sie einfach zu Sicherheitsrichtlinien hinzufügen können. Das Anpassen von Sicherheitsprofilen ist ganz einfach, da Sie ein vordefiniertes Profil klonen und dann bearbeiten können. Sie können ein Sicherheitsprofil auch von Grund auf auf der Firewall oder auf Panorama erstellen.

Um bekannte und unbekannte Bedrohungen in Ihrem Netzwerkverkehr zu erkennen, fügen Sie allen Sicherheitsrichtlinienregeln, die den Datenverkehr im Netzwerk zulassen, Sicherheitsprofile hinzu, damit die Firewall den gesamten zulässigen Datenverkehr überprüft. Die Firewall wendet Sicherheitsprofile auf den Datenverkehr an, der mit der Sicherheitsrichtlinie übereinstimmt, scannt den Datenverkehr gemäß den Sicherheitsprofileinstellungen und ergreift dann geeignete Maßnahmen zum Schutz des Netzwerks. Sofern nichts anderes angegeben ist, gelten die Empfehlungen bewährter Sicherheitsprofile für alle vier Datenverkehrsströme des Rechenzentrums.

*Der Download der Inhaltsupdates erfolgt automatisch. Installieren Sie diese so schnell wie möglich, damit die aktuellen Signaturen und Inhalte zur Bedrohungsprävention (Antivirus, Antispyware, Sicherheitslücken, Malware usw.) auf der Firewall bereitstehen und die neuesten Bedrohungen blockieren.*

## Regelstapel und Regeln in Cloud NGFW für AWS

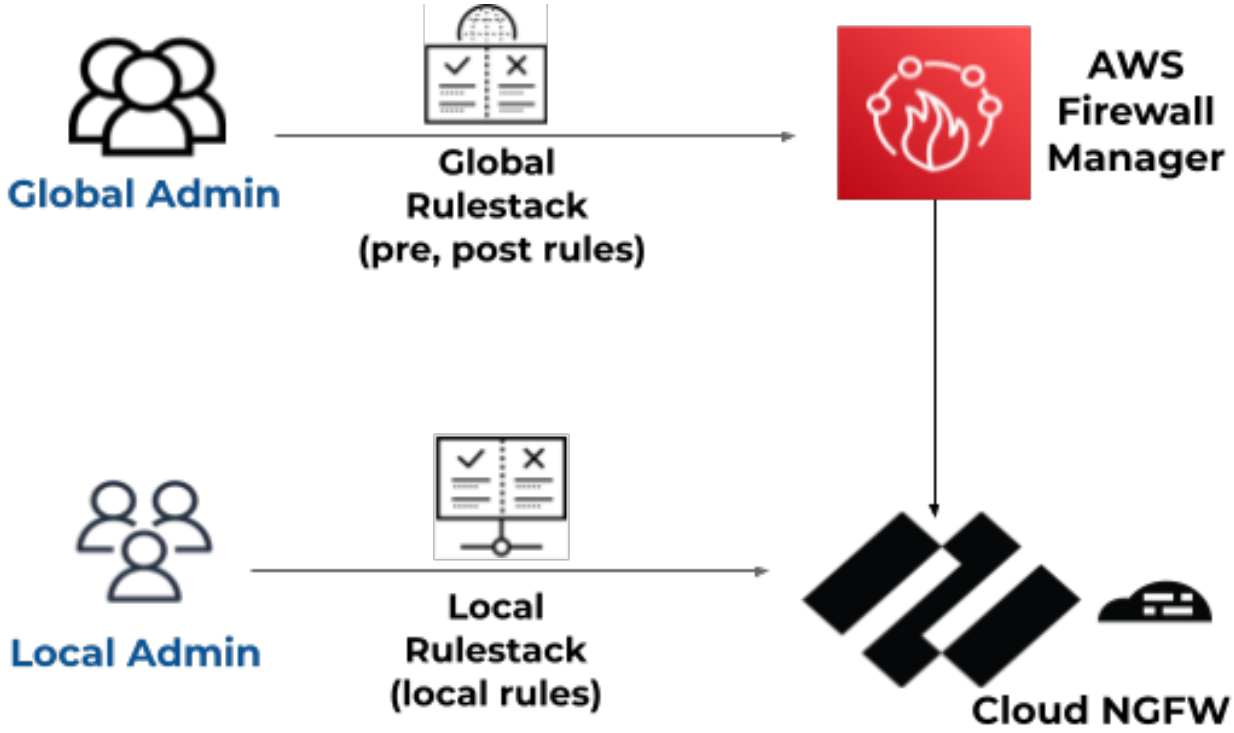
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Regelstapel definieren die Zugriffskontrolle (App-ID, URL-Filterung) und das Bedrohungsabwehrverhalten von Cloud NGFW-Ressourcen. Eine Cloud NGFW-Ressource schützt mit Ihren Regelstapeldefinitionen den Datenverkehr durch einen zweistufigen Prozess. Erstens erzwingt sie Ihre Regeln, um Ihren Datenverkehr zuzulassen oder abzulehnen. Zweitens führt sie eine Inhaltsprüfung bezüglich des zulässigen Datenverkehrs basierend auf Ihren Angaben in den Sicherheitsprofilen durch. Ein Regelstapel umfasst eine Reihe von Sicherheitsregeln, zugeordneten Objekten und Profilen, die Gerätegruppen in Panorama ähneln. Es gibt zwei Typen von Regelstapeln:

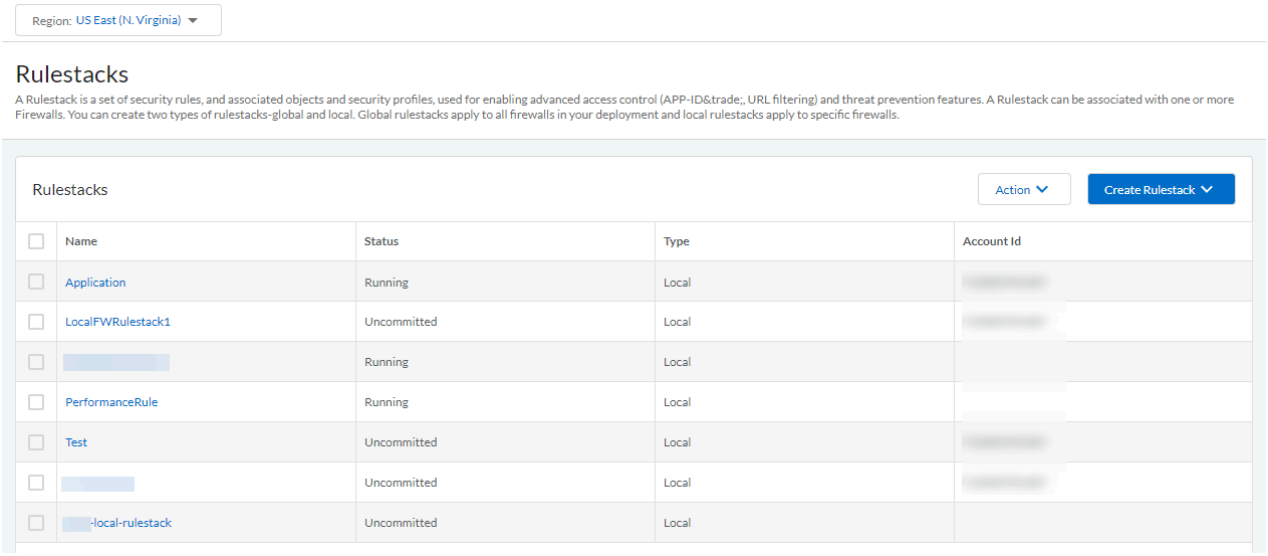
- **Lokaler Regelstapel**: Ein lokaler Regelstapel besteht aus lokalen Regeln und verwaltet diese. Ein lokaler Kontoadministrator kann einen lokalen Regelstapel mit einer NGFW in seinem AWS-Konto verknüpfen. Um lokale Regelstapel zu erstellen und zu verwalten, muss Ihnen die Rolle „Local Rulestack Admin“ (Administrator für lokalen Regelstapel) zugewiesen sein.
- **Globaler Regelstapel**: Der AWS Firewall Manager-Administrator kann eine Firewall-Manager-Service(FMS)-Richtlinie erstellen und mit ihr einen globalen Regelstapel verknüpfen. AWS Firewall Manager verwaltet den globalen Regelstapel in all diesen NGFWs in verschiedenen AWS-Konten einer AWS-Organisation. In einem globalen Regelstapel sind Vor- und Nach-Regeln für jede NGFW konfiguriert. Um globale Regelstapel zu erstellen und zu verwalten, muss Ihnen die Rolle „Global Rulestack Admin“ (Administrator für globalen Regelstapel) zugewiesen sein.
  - **Vor-Regeln**: Regeln, die am Anfang der Regelreihenfolge hinzugefügt werden. Diese Regeln werden zuerst ausgewertet.
  - **Nach-Regeln**: Regeln, die am Ende der Regelreihenfolge hinzugefügt werden. Diese Regeln werden nach den Vor-Regeln und den in einem lokalen Regelstapel definierten Regeln ausgewertet. Dieser Regelstapel wird auf eine einzelne NGFW angewendet.

Wenn Sie den AWS Firewall Manager verwenden, können Sie mit einer Kombination aus lokalen und globalen Regelstapeln ein hierarchisches Regelmodell erstellen. Die Vor-Regeln eines globalen Regelstapels können als globale Standardregeln für alle zugehörigen Firewalls fungieren. Dann können Sie mit einem lokalen Regelstapel Regeln für bestimmte Anwendungen oder Benutzer definieren. Mithilfe der Nach-Regeln können Sie Datenverkehr zulassen oder ablehnen, der nicht mit den Vor-Regeln oder den im lokalen Regelstapel definierten Regeln übereinstimmt.






*Auf jede NGFW wird ein globaler und ein lokaler Regelstapel angewendet.*

Wenn Sie Multi-Account Tenant oder Multi-VPC verwenden, sollten Sie die folgenden Änderungen am Verhalten des Regelstapels in Betracht ziehen:

- Beim Erstellen eines Regelstapels wird dieser einem bestimmten Konto zugeordnet.
- Sie können jetzt einen Regelstapel einer Firewall-Ressource in jedem eingebundenen Konto zuordnen.
- Berechtigungen werden immer noch dem Konto zugeordnet, das mit dem Regelstapel verknüpft ist. Alle Änderungen am Regelstapel werden von einem Benutzer mit LRA-Berechtigungen im Regelstapel-Konto vorgenommen.

Zertifikate von jedem eingebundenen Konto werden einem Regelstapel zugeordnet. Beispielsweise werden das Zertifikat in Konto1 und das Zertifikat in Konto2 einem Regelstapel in Konto3 zugeordnet, der mit einer Firewall-Ressource in Konto4 verknüpft sein könnte. In diesem Szenario müssen alle Konten (1–4) erfolgreich eingebunden werden.

## Regelstapel in Cloud NGFW für AWS erstellen

Im Cloud NGFW-Mandanten können Sie Regelstapel erstellen, wenn Ihnen die Rolle „LocalRuleStackAdmin“ oder „GlobalRulestackAdmin“ zugewiesen ist. Um einen globalen Regelstapel zu erstellen, müssen Sie Ihren Cloud NGFW-Mandanten mit AWS Firewall Manager erstellt haben.

Wenn Sie einen lokalen Regelstapel erstellen, müssen Sie ein AWS-Konto angeben. Wenden Sie den Regelstapel nur auf NGFWs an, die mit diesem AWS-Konto verknüpft sind. Führen Sie die folgenden Schritte aus, um einen Regelstapel zu erstellen.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** > **Create Rulestack (Regelstapel erstellen)** aus.

**STEP 2 |** Wählen Sie **Local Rulestack (Lokaler Regelstapel)** oder **Global Rulestack (Globaler Regelstapel)** (nur FMS-Bereitstellung) aus der Dropdown-Liste aus.

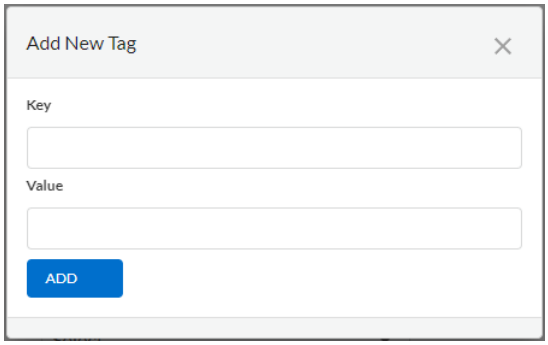
**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihren Regelstapel ein.

**STEP 4 |** (Optional) Geben Sie eine **Beschreibung** für Ihren Regelstapel ein.

**STEP 5 |** (Nur lokaler Regelstapel) Wählen Sie ein **AWS-Konto** aus der Dropdown-Liste aus.

**STEP 6 |** (Optional) Wenden Sie **Tags** an.

1. Klicken Sie auf das Symbol + und wählen Sie **Add New (Neu hinzufügen)** aus.
2. Geben Sie einen **Schlüssel** und einen **Wert** ein.
3. Klicken Sie auf **Add (Hinzufügen)**.

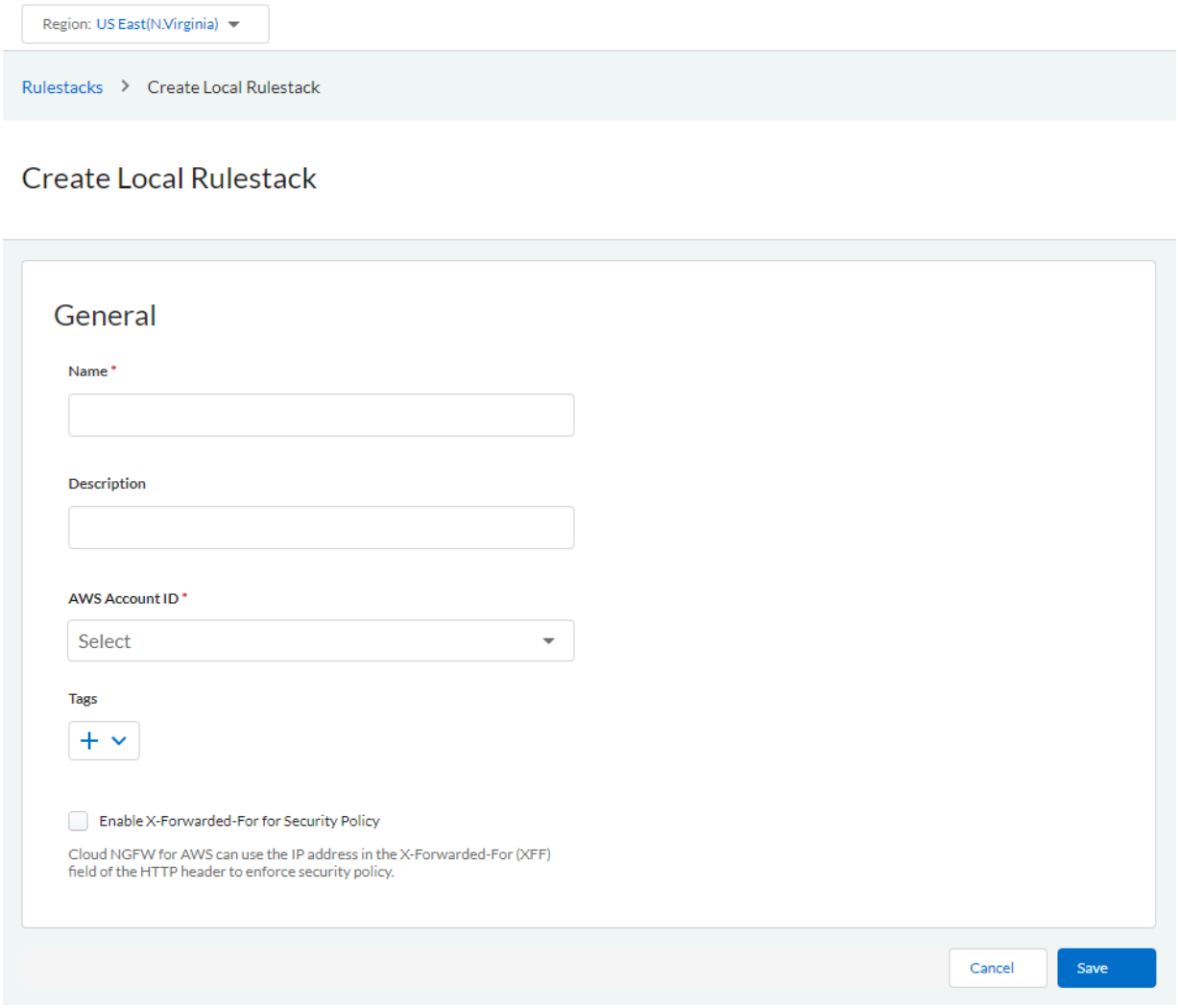



**STEP 7 |** (Optional) **Aktivieren Sie X-Forwarded-For für die Sicherheitsrichtlinie**. Weitere Informationen finden Sie unter X-Forwarded For.

**STEP 8 |** Klicken Sie auf **Save (Speichern)**.

**STEP 9 |** Nachdem Sie den Regelstapel erstellt haben, stellen Sie ihn in der Firewall bereit.




# X-Forwarded-For in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto |

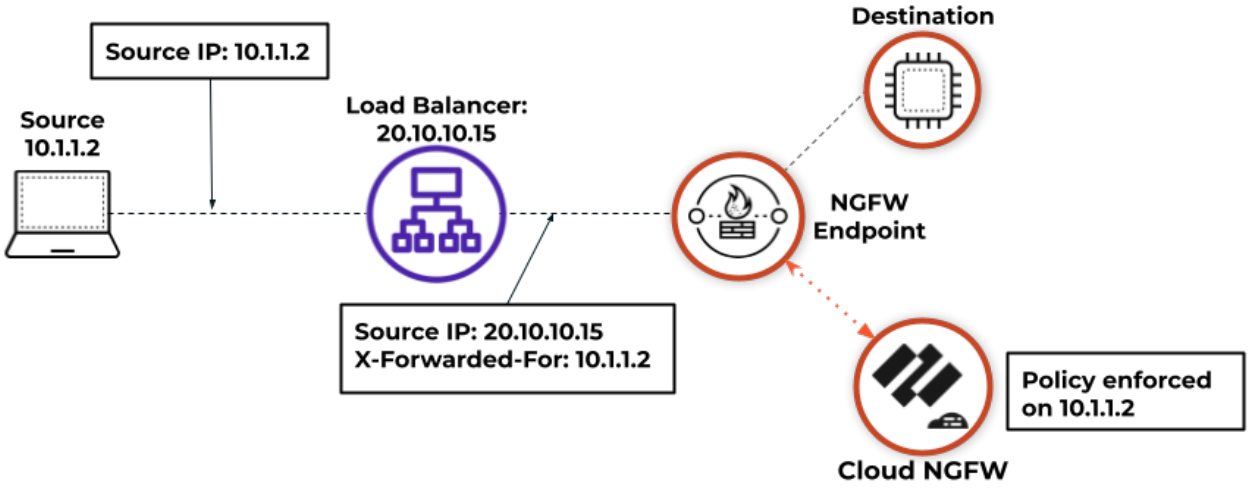
 

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Benutzerrolle (entweder Mandant oder Administrator) |

Der eingehende Datenverkehr zu Ihren Anwendungen kann AWS Load Balancer oder Proxyserver passieren, bevor er die NGFW erreicht. Da diese Geräte den Datenverkehr zwischen Quelle und Ziel abfangen, sieht die NGFW die IP-Adresse des Load Balancers oder Proxyservers anstelle der IP-Adresse der Quelle. Diese Geräte fügen HTTP-Anforderungen den X-Forwarded-For-Header (XFF) hinzu und fügen die tatsächliche IPv4- oder IPv6-Adresse des Clients hinzu, der auf Ihre Anwendung zugreift.

Der Datenverkehr zu Ihren Anwendungen hat möglicherweise mehr als einen Proxyserver passiert, bevor er die NGFW erreicht. Der XFF-Anforderungsheader kann mehrere IP-Adressen enthalten, die durch Kommas getrennt sind. Die NGFW verwendet immer die zuletzt hinzugefügte Adresse im XFF-Header, um Richtlinien durchzusetzen.

Wenn Sie Ihren Regelstapel konfigurieren, können Sie für Cloud NGFW festlegen, dass die Quell-IP-Adresse in einem XFF-HTTP-Header-Feld verwendet werden soll, um Sicherheitsleitlinien durchzusetzen.



# Präfixliste in Cloud NGFW für AWS erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Ein Sicherheitsregelobjekt ist ein einzelnes Objekt oder eine kollektive Einheit, in der diskrete Identitäten wie IP-Adressen, vollqualifizierte Domänennamen (FQDN), intelligente Feeds oder Zertifikate gruppiert werden. In der Regel gruppieren Sie beim Erstellen eines Richtlinienobjekts Objekte, die ähnliche Berechtigungen in der Richtlinie erfordern. Wenn Ihre Organisation beispielsweise einen Satz von Server-IP-Adressen für die Authentifizierung von Benutzern verwendet, können Sie diesen als Präfixlistenobjekt gruppieren und in einer oder mehreren Sicherheitsregeln auf diese Präfixliste verweisen. Durch das Gruppenobjekt können Sie den Verwaltungsaufwand beim Erstellen von Regeln erheblich reduzieren.

Mit einer Präfixliste können Sie bestimmte IP-Adressen gruppieren, für die dieselbe Richtliniendurchsetzung erforderlich ist. Eine Präfixliste kann eine oder mehrere IP-Adressen oder eine IP-Netzmaske in CIDR-Notation enthalten. Bei einem Adressobjekt vom Typ IP-Netzmaske müssen Sie bei der Eingabe der IP-Adresse oder des Netzwerks einen Schrägstrich verwenden, um das IPv4-Netzwerk anzugeben. Beispiel: 192.168.18.0/24.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den eine Präfixliste konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Objects (Objekte)** > **Prefix List (Präfixliste)** > **Create Prefix (Präfixliste erstellen)** aus.

**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihre Präfixliste ein.

**STEP 4 |** (optional) Geben Sie eine Beschreibung für Ihre Präfixliste ein.

**STEP 5 |** Geben Sie mindestens eine **Adresse** ein. Sie können IP-Adressen oder IP-Netzmasken im CIDR-Format und einen Wert pro Zeile eingeben.

**STEP 6 |** Klicken Sie auf **Save (Speichern)**.

# Zertifikat zu Cloud NGFW für AWS hinzufügen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | ❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW verwendet Zertifikate, um auf einen intelligenten Feed zuzugreifen und die ein- und ausgehende Entschlüsselung zu ermöglichen. Diese Zertifikate werden im AWS Secrets Manager gespeichert.

Bei einer typischen Bereitstellung werden drei Arten von Zertifikaten verwendet.

- **CA-Zwischenzertifikat (CA-Zertifikat)**: Eine Zertifizierungsstelle (Certificate Authority, CA) ist eine vertrauenswürdige Organisation, die SSL-Zertifikate ausstellt. Diese digitalen Zertifikate sind Dateien, die zum Verknüpfen einer Entität mit einem öffentlichen Schlüssel verwendet werden. Webbrowser verwenden diese Zertifikate, um von Webservern gesendete Inhalte zu authentifizieren. Webbrowser werden normalerweise mit Listen von Zertifizierungsstellen bereitgestellt, denen sie bei der Identifizierung von Hosts implizit vertrauen. Der Zweck der Zertifizierungsstelle besteht darin, die Authentizität der Website, Domäne oder der Organisationen zu überprüfen.
- **Serverzertifikat**: Ein Zertifikat, das einem bestimmten Domänennamen zugeordnet ist. Wenn eine Website über ein gültiges Zertifikat verfügt, bedeutet dies, dass eine Zertifizierungsstelle überprüft hat, ob die Webadresse tatsächlich zu dieser Organisation gehört. Wenn Sie eine URL eingeben, überprüft Ihr Browser das Zertifikat, um sicherzustellen, dass die Website-Adresse mit der Adresse im Zertifikat übereinstimmt. Außerdem wird sichergestellt, dass das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

  Gelegentlich stellen Sie möglicherweise eine Verbindung zu einem Server mit einem nicht vertrauenswürdigen Zertifikat her. Cloud NGFW für AWS trennt diese Verbindung so, als ob der Server sie beendet hätte.
- **CA-Stammzertifikat**: Eine Zertifizierungsstelle kann mehrere Zertifikate in Form einer Baumstruktur ausstellen. Ein Stammzertifikat ist das oberste Zertifikat in der Baumstruktur.

Wenn ein Zertifikat, das mit Cloud NGFW verwendet werden soll, zum AWS Secrets Manager hinzugefügt wird, müssen die folgenden Voraussetzungen erfüllt sein.

- Zertifikat als Schlüssel- oder Wert-Paar mit zwei Schlüsseln hinzugefügt: **private-key** und **public-key**. Für den privaten Schlüssel sollte der Wert der eigentliche Schlüssel sein und für den öffentlichen Schlüssel sollte der Wert der eigentliche Zertifikatsinhalt sein.
- Ein Tag mit dem Schlüssel **PaloAltoCloudNGFW** und dem Wert **true**.
- Importieren Sie das CA-Stammzertifikat und die CA-Zwischenzertifikate in den Truststore des Clients.
- Wenn Sie End-Entity-Zertifikate zum Entschlüsseln des Datenverkehrs verwenden, müssen nur die End-Entity-Zertifikate (sowohl private als auch öffentliche Schlüssel) im AWS Secrets Manager gespeichert werden.
- Das private Schlüsselformat PKCS8 wird unterstützt. Das private Schlüsselformat PKCS1 wird nicht unterstützt.

Unterstütztes PKCS-Format:

```
-----BEGIN PRIVATE KEY----- -----END PRIVATE KEY-----
```

Nicht unterstütztes PKCS1-Format:

```
-----BEGIN RSA PRIVATE KEY----- -----END RSA PRIVATE KEY-----
```

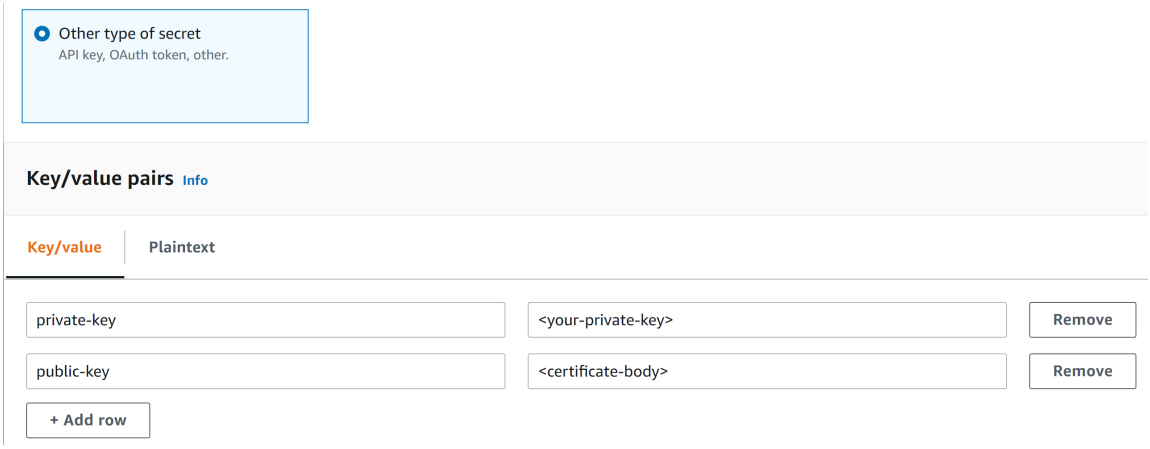
Führen Sie die folgenden Schritte aus, um ein Zertifikat hinzuzufügen, das mit Cloud NGFW für AWS verwendet werden soll.

**STEP 1 |** Fügen Sie Ihr Zertifikat zum AWS Secrets Manager hinzu.

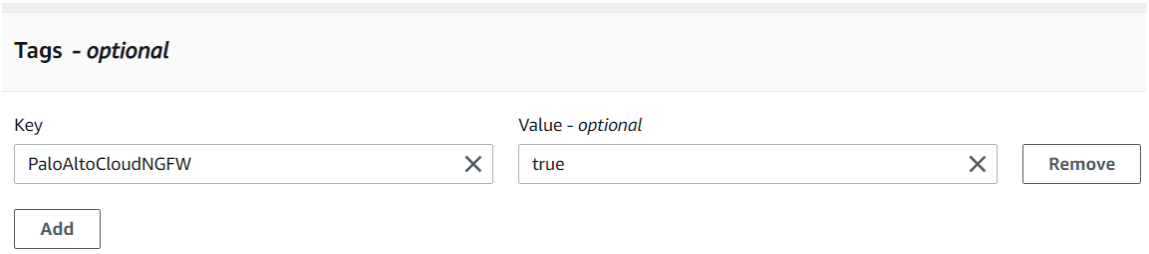
1. Melden Sie sich bei der AWS-Konsole an, navigieren Sie zum AWS Secrets Manager und klicken Sie auf **Store a new secret (Neuen geheimen Schlüssel speichern)**.
2. Wählen Sie **Other type of secret (Anderer geheimer Schlüsseltyp)** aus.
3. Erstellen Sie unter **Key and value pairs (Schlüssel- und Wert-Paare)** einen Schlüssel mit dem Namen **private-key** und einen weiteren mit dem Namen **public-key**.
4. Fügen Sie Ihren gesamten privaten Schlüssel und Ihren gesamten öffentlichen Schlüssel in das entsprechende Feld ein.




5. Klicken Sie auf **Next (Weiter)**.
6. Geben Sie einen beschreibenden **Namen für den geheimen Schlüssel** ein.
7. Fügen Sie ein Tag mit dem Schlüssel **PaloAltoCloudNGFW** und dem Wert **true** hinzu.




8. Klicken Sie auf **Next (Weiter)**, erneut auf **Next (Weiter)** und auf **Store (Speichern)**, um das Hinzufügen Ihres Zertifikats abzuschließen.

**STEP 2 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den ein Zertifikat konfiguriert werden soll.

**STEP 3 |** Wählen Sie **Objects (Objekte)** > **Certificate List (Zertifikatsliste)** > **Add Certificate (Zertifikat hinzufügen)** aus.

**STEP 4 |** Geben Sie einen beschreibenden **Namen** für Ihr Zertifikat ein.

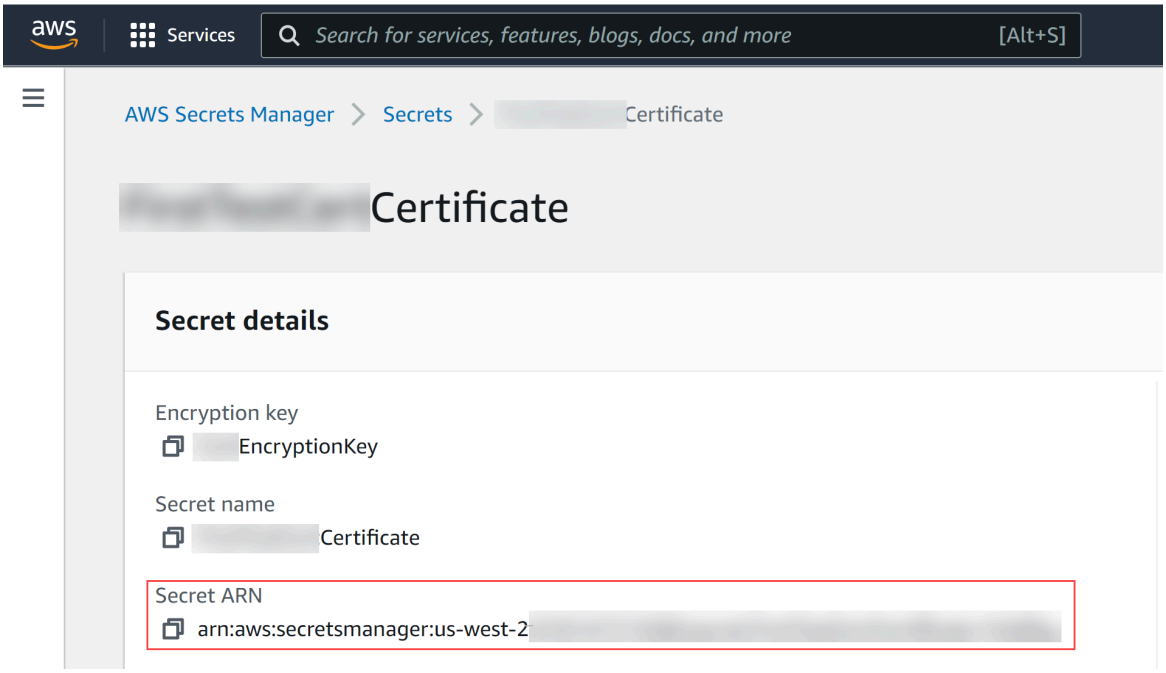
**STEP 5 |** (Optional) Geben Sie eine Beschreibung für Ihr Zertifikat ein.

**STEP 6 |** Wählen Sie ein Zertifikat aus.

- Geben Sie den **Zertifikat-ARN** ein, wenn Cloud NGFW das Zertifikat vom AWS Secrets Manager herunterladen soll.



- Aktivieren Sie **Self Signed Certificate (Selbstsigniertes Zertifikat)**, wenn Cloud NGFW ein selbstsigniertes Zertifikat erstellen soll.

**STEP 7 |** Klicken Sie auf **Save (Speichern)**.

## FQDN-Liste in Cloud NGFW für AWS erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Ein Sicherheitsregelobjekt ist ein einzelnes Objekt oder eine kollektive Einheit, in der diskrete Identitäten wie IP-Adressen, vollqualifizierte Domänennamen (FQDN), intelligente Feeds oder Zertifikate gruppiert werden. In der Regel gruppieren Sie beim Erstellen eines Richtlinienobjekts Objekte, die ähnliche Berechtigungen in der Richtlinie erfordern. Wenn Ihre Organisation beispielsweise einen Satz von Server-IP-Adressen für die Authentifizierung von Benutzern verwendet, können Sie diesen als Präfixlistenobjekt gruppieren und in einer oder mehreren Sicherheitsregeln auf diese Präfixliste verweisen. Durch das Gruppenobjekt können Sie den Verwaltungsaufwand beim Erstellen von Regeln erheblich reduzieren.

Ein FQDN-Objekt (z. B. paloaltonetworks.com) ist besonders benutzerfreundlich, da DNS die FQDN-Auflösung für die IP-Adressen bereitstellt. So müssen Sie die IP-Adressen nicht kennen und jedes Mal manuell aktualisieren, wenn der FQDN in neue IP-Adressen aufgelöst wird.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den die FQDN-Liste konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Objects (Objekte)** > **FQDN List (FQDN-Liste)** > **Create FQDN (FQDN erstellen)** aus.

**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihre FQDN-Liste ein.

**STEP 4 |** (optional) Geben Sie eine Beschreibung für Ihre FQDN-Liste ein.

**STEP 5 |** Geben Sie mindestens einen **FQDN** ein, einen pro Zeile.

**STEP 6 |** Klicken Sie auf **Save (Speichern)**.

## Intelligenten Feed in Cloud NGFW für AWS konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | ❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Ein Sicherheitsregelobjekt ist ein einzelnes Objekt oder eine kollektive Einheit, in der diskrete Identitäten wie IP-Adressen, vollqualifizierte Domänennamen (FQDN), intelligente Feeds oder Zertifikate gruppiert werden. In der Regel gruppieren Sie beim Erstellen eines Richtlinienobjekts Objekte, die ähnliche Berechtigungen in der Richtlinie erfordern. Wenn Ihre Organisation beispielsweise einen Satz von Server-IP-Adressen für die Authentifizierung von Benutzern verwendet, können Sie diesen als Präfixlistenobjekt gruppieren und in einer oder mehreren Sicherheitsregeln auf diese Präfixliste verweisen. Durch das Gruppenobjekt können Sie den Verwaltungsaufwand beim Erstellen von Regeln erheblich reduzieren.

Ein intelligenter Feed, auch externe dynamische Liste genannt, ist eine Liste, die Sie oder Drittanbieter auf einem externen Webserver hosten können. Sie können den intelligenten Feed als Quelle oder Ziel Ihrer Sicherheitsregel angeben. Die NGFW prüft die gehostete Liste in stündlichen oder täglichen Intervallen und erzwingt Ihre Sicherheitsregeln basierend auf den neuesten Einträgen in Ihrer Liste, ohne dass Sie Konfigurationsänderungen vornehmen müssen.

- **Intelligenter Feed**: Ein intelligenter Feed, auch als externe dynamische Liste (EDL) bezeichnet, ist ein fortlaufender Datenstrom im Zusammenhang mit potenziellen oder aktuellen Bedrohungen für die Sicherheit eines Unternehmens. Mit einem intelligenten Feed werden IP-Adressen und URLs aufgezeichnet und verfolgt, die mit Bedrohungen wie Phishing-Betrug, Malware, Bots, Spyware, Ransomware und mehr in Verbindung stehen.

  Cloud NGFW enthält vier integrierte intelligente Feeds.

  - **Bulletproof-IP-Adressen von Palo Alto Networks**: Enthält IP-Adressen, die von Bulletproof-Hosting-Providern bereitgestellt werden. Da diese nur wenige oder gar keine Einschränkungen für Inhalte festlegen, nutzen Angreifer diese Dienste häufig, um bösartiges, illegales und unethisches Material zu hosten und zu verbreiten.
  - **Hochrisiko-IP-Adressen von Palo Alto Networks**: Enthält bösartige IP-Adressen aus Bedrohungswarnungen von vertrauenswürdigen Drittorganisationen. Palo Alto Networks erstellt die Liste der Bedrohungswarnungen, hat jedoch keine direkten Beweise für die Bösartigkeit der IP-Adressen.
  - **Bekannte bösartige IP-Adressen von Palo Alto Networks**: Enthält IP-Adressen, die auf der Grundlage von WildFire-Analysen, Unit 42-Recherchen und Telemetriedaten als bösartig eingestuft wurden. Angreifer verwenden diese IP-Adressen fast ausschließlich, um Malware zu verbreiten, Befehls- und Kontrollaktivitäten einzuleiten und Angriffe zu starten.
  - **Tor-Exit-IP-Adressen von Palo Alto Networks**: Enthält IP-Adressen, die von mehreren Providern bereitgestellt und mit Bedrohungsdaten von Palo Alto Networks als aktive Tor-Exit-Knoten validiert wurden. Der Datenverkehr von Tor-Exit-Knoten kann einem legitimen Zweck dienen, ist jedoch unverhältnismäßig stark mit bösartigen Aktivitäten verbunden, insbesondere in Unternehmensumgebungen.

  Sie können Ihre NGFW mit den integrierten intelligenten Feeds von Palo Alto Networks und intelligenten Feeds von Drittanbietern verbinden, um aktuelle Informationen über Bedrohungen für

Ihr Netzwerk bereitzustellen. Wenn für die Verbindung Entschlüsselungszertifikate angegeben werden müssen, können Sie Cloud NGFW so konfigurieren, dass ein Cloud NGFW-Zertifikatsobjekt verwendet wird, das im Folgenden beschrieben ist.

Für IP- und URL-Listen:

- **IP-Liste**: Erzwingen Sie Richtlinien für eine Liste von Quell- oder Ziel-IP-Adressen, die ad hoc entstehen, indem Sie einen intelligenten Feed vom Typ IP-Adresse als Quell- oder Zieladressobjekt in Richtlinienregeln verwenden. Konfigurieren Sie die NGFW so, dass der Zugriff auf die in der Liste enthaltenen IP-Adressen abgelehnt oder zugelassen wird. Die NGFW behandelt einen intelligenten IP-List-Feed als Adressobjekt und alle enthaltenen IP-Adressen werden als ein Adressobjekt behandelt.

  Der intelligente Feed kann einzelne IP-Adressen, Subnetzadressen (Adresse/Maske) oder IP-Adressbereiche enthalten. Darüber hinaus kann die Sperrliste Kommentare und Sonderzeichen wie * , : , ; , # oder / enthalten. Die Syntax für jede Zeile in der Liste lautet **`[IP-Adresse, IP/Maske oder IP-Startbereich-IP-Endbereich] [Leerzeichen] [Kommentar]`**.

  Geben Sie jede IP-Adresse/jeden Bereich/jedes Subnetz in eine neue Zeile ein. URLs oder Domänen werden in dieser Liste nicht unterstützt. Ein Subnetz oder ein IP-Adressbereich, z. B. 92.168.20.0/24 oder 192.168.20.40-192.168.20.50, zählt als ein IP-Adresseintrag und nicht als mehrere IP-Adressen. Wenn Sie einen Kommentar hinzufügen, muss sich dieser in derselben Zeile wie die IP-Adresse/der Bereich/das Subnetz befinden. Das Leerzeichen am Ende der IP-Adresse ist das Trennzeichen, das einen Kommentar von der IP-Adresse trennt.

  Beispiel für eine IP-Adressliste:

  ```
  192.168.20.10/32 2001:db8:123:1::1 #IPv6-Adresse testen
   192.168.20.0/24 ; internes Subnetz testen 2001:db8:123:1::/64
   internen IPv6-Bereich testen 192.168.20.40-192.168.20.50
  ```

- **URL-Liste**: Schützen Sie Ihr Netzwerk mithilfe von URLs vor neuen Bedrohungsquellen oder Malware. Die NGFW verarbeitet einen intelligenten Feed mit URLs wie eine benutzerdefinierte URL-Kategorie. Weitere Informationen zur Formatierung der URL-Liste finden Sie unter Erweiterte URL-Filterung in Cloud NGFW für AWS.

Die NGFW benötigt ein Zertifikatsobjekt, um auf den intelligenten Feed zugreifen zu können. Weitere Informationen finden Sie unter Zertifikat zu Cloud NGFW für AWS hinzufügen.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den die Dateiblockade konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Objects (Objekte)** > **Intelligent Feed (Intelligenter Feed)** > **Create Intelligent Feed (Intelligenten Feed erstellen)** aus.

**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihren intelligenten Feed ein.

**STEP 4 |** (optional) Geben Sie eine Beschreibung für Ihren intelligenten Feed ein.

**STEP 5 |** Wählen Sie den **Typ** des intelligenten Feeds aus.

**STEP 6 |** Geben Sie die **Quell-URL** ein.

**STEP 7 |** Wählen Sie das **Zertifizierungsprofil** aus.

**STEP 8 |** Legen Sie die **Aktualisierungshäufigkeit** fest: **Hourly (stündlich)** oder **Daily (täglich)**.

**STEP 9 |** Klicken Sie auf **Save (Speichern)**.

# Sicherheitsregeln in Cloud NGFW für AWS erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Sicherheitsregeln schützen Netzwerk-Assets vor Bedrohungen und Störungen und helfen, Netzwerkressourcen optimal zuzuweisen, um die Produktivität und Effizienz in Geschäftsprozessen zu steigern. In Cloud NGFW für AWS bestimmen individuelle Sicherheitsregeln, ob eine Sitzung basierend auf Datenverkehrsattributen wie Quell- und Ziel-IP-Adresse, Quell- und Ziel-FQDN oder der Anwendung abgelehnt oder zugelassen wird.

Der gesamte Datenverkehr, der die Firewall passiert, wird mit einer Sitzung abgeglichen und jede Sitzung wird mit einer Regel abgeglichen. Bei einer Sitzungsübereinstimmung wendet die NGFW die Übereinstimmungsregel auf bidirektionalen Datenverkehr in dieser Sitzung an (Client-zu-Server und Server-zu-Client). Für Datenverkehr, der mit keiner definierten Regel übereinstimmt, gelten die Standardregeln.

Sicherheitsrichtlinienregeln werden von links nach rechts und von oben nach unten ausgewertet. Ein Paket wird mit der ersten Regel abgeglichen, die die definierten Kriterien erfüllt. Sobald eine Übereinstimmung festgestellt wird, werden nachfolgende Regeln nicht ausgewertet. Daher müssen die spezifischeren Regeln den allgemeineren vorausgehen, um die Kriterien für die beste Übereinstimmung durchzusetzen.

Sobald Sie einen Regelstapel erstellt haben, können Sie Regeln erstellen und zu Ihrem Regelstapel hinzufügen.

Sie können anzeigen, wie oft der Datenverkehr eine bestimmte Regel erfüllt hat, indem Sie zu **Rulestacks (Regelstapel)** > **<rulestack-name>** > **Security Rules (Sicherheitsregeln)** > **<rule-name>** > **Usage (Nutzung)** navigieren. Auf der Registerkarte **Usage (Nutzung)** wird angezeigt, wie oft die vermutete Regel durch Datenverkehr ausgelöst wurde, der die NGFW passiert. Der Trefferzähler wird alle 15 Sekunden aktualisiert.

Zusätzlich können Sie den Regeltrefferzähler anzeigen, indem Sie **NGFWs** > **<firewall-name>** > **Rules (Regeln)** > **<rule-name>** auswählen. Wenn der Trefferzähler über das NGFWs-Menü angezeigt wird, zeigt er an, wie oft die ausgewählte Regel für diese bestimmte NGFW ausgelöst wurde.

**STEP 1 |** Wählen Sie **Manage (Verwalten)** > **Rulestacks (Regelstapel)** und den gewünschten Regelstapel für Ihre neue Regel aus.

**STEP 2 |** Klicken Sie auf **Create New (Neu erstellen)**. Wenn Sie eine Regel zu einem globalen Regelstapel hinzufügen, müssen Sie **Pre Rule (Vor-Regel)** oder **Post Rule (Nach-Regel)** auswählen.

**STEP 3 |** Geben Sie einen beschreibenden **Namen** für Ihre Regel ein.

**STEP 4 |** (optional) Geben Sie eine **Beschreibung** für Ihre Regel ein.

**STEP 5 |** Legen Sie die **Regelpriorität** fest.

Die Regelpriorität bestimmt die Reihenfolge, in der die Regeln ausgewertet werden. Regeln mit niedrigerer Priorität werden zuerst ausgewertet. Darüber hinaus kann jede Regel innerhalb eines Regelstapels ausgeführt werden.

**STEP 6 |** Standardmäßig ist die Sicherheitsregel auf **Enabled (Aktiviert)** gesetzt. Entfernen Sie das Häkchen bei **Enabled (Aktiviert)**, um die Regel zu deaktivieren. Sie können eine Regel jederzeit aktivieren oder deaktivieren.

**STEP 7 |** Legen Sie die **Quelle** fest.

1. Wählen Sie **Any (Beliebig)** oder **Match (Übereinstimmung)** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von der Quelle anhand der Regel ausgewertet.
2. Wenn Sie **Match (Übereinstimmung)** auswählen, klicken Sie auf das Symbol für Hinzufügen (+ ⌄) und geben Sie mindestens ein Quellobjekt an: IP-Adresse (CIDR), Präfixliste, Länder oder intelligenter Feed (IP-Typ).

**STEP 8 |** Legen Sie das **Ziel** fest.

1. Wählen Sie **Any (Beliebig)** oder **Match (Übereinstimmung)** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig vom Ziel anhand der Regel ausgewertet.
2. Wenn Sie **Match (Übereinstimmung)** auswählen, klicken Sie auf das Symbol für Hinzufügen (+ ⌄) und geben Sie mindestens ein Zielobjekt an: IP-Adresse (CIDR), Präfixliste, FQDN-Liste, Länder oder intelligenter Feed (IP-Typ).

**STEP 9 |** Legen Sie die granulare Steuerung **Application (App-ID) (Anwendung (App-ID))** fest.

1. Wählen Sie **Any (Beliebig)** oder **Select (Auswählen)** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von der Anwendung ausgewertet. Durch die Angabe einer Anwendung wird der Datenverkehr anhand der Regel ausgewertet, wenn der Datenverkehr mit der angegebenen Anwendung übereinstimmt.
2. Wenn Sie „Select“ (Auswählen) auswählen, klicken Sie auf das Symbol für Hinzufügen (+ −) und geben Sie mindestens eine Anwendung an.

**STEP 10 |** Legen Sie die granulare Steuerung **URL Category (URL-Kategorie)** fest.

1. Wählen Sie **Any (Beliebig)** oder **Match (Übereinstimmung)** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von der URL ausgewertet. Durch die Angabe einer Anwendung wird der Datenverkehr anhand der Regel ausgewertet, wenn der Datenverkehr mit der angegebenen URL-Kategorie oder dem angegebenen intelligenten Feed (URL-Typ) übereinstimmt.
2. Wenn Sie sich für **Match (Übereinstimmung)** entscheiden, wählen Sie **URLCategoryNames** oder **Feeds** aus und klicken Sie auf das Symbol für Hinzufügen (+ ⌄ −). Wählen Sie aus der Dropdown-Liste eine URL-Kategorie oder einen intelligenten Feed aus.

**STEP 11 |** Legen Sie die granulare Steuerung **Port & Protocol (Port und Protokoll)** fest.

1. Wählen Sie **application-default (Anwendungsstandard)**, **Any (Beliebig)** oder **Select (Auswählen)** aus.

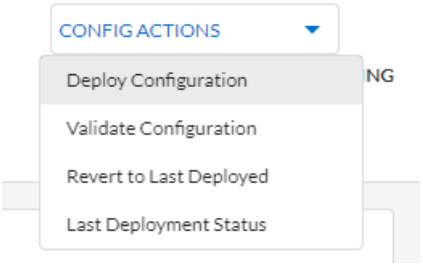
   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von Port und Protokoll ausgewertet. Durch die Angabe eines Ports und Protokolls wird der Datenverkehr anhand der Regel ausgewertet, wenn der Datenverkehr mit dem angegebenen Port und Protokoll übereinstimmt.
2. Wenn Sie sich für „Select“ (Auswählen) entscheiden, wählen Sie das Protokoll aus der Dropdown-Liste aus und geben Sie die Portnummer ein. Sie können eine einzelne Portnummer oder mithilfe von Kommas mehrere Ports angeben. Beispiel: 80, 8080.

**STEP 12 |** Legen Sie **Actions (Aktionen)** fest.

1. Legen Sie die Aktion fest, die die Firewall ausführen soll, wenn der Datenverkehr mit der Regel übereinstimmt: **Allow (Zulassen)**, **Deny (Ablehnen)**, **Reset Server (Server zurücksetzen)** oder **Reset Both (Beide zurücksetzen)**.
2. Aktivieren Sie **Outbound TLS Decryption (Ausgehende TLS-Entschlüsselung)**.
3. Aktivieren Sie **Logging (Protokollierung)**.

**STEP 13 |** Klicken Sie auf **Create (Erstellen)**.

**STEP 14 |** Nachdem Sie Regeln für Ihren Regelstapel erstellt haben, prüfen Sie Ihre Konfiguration oder stellen Sie sie bereit.




# Sicherheitsprofile in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW verwendet Ihre Regelstapeldefinitionen, um Ihren VPC-Datenverkehr in einem zweistufigen Prozess zu schützen. Erstens setzt es Ihre Regeln durch, um Ihren Datenverkehr zuzulassen oder zu verweigern. Zweitens führt es eine Inhaltsüberprüfung des zulässigen Datenverkehrs (URLs, Bedrohungen, Dateien) anhand dessen durch, was Sie in den Sicherheitsprofilen angeben. Darüber hinaus können

Sie definieren, wie Cloud NGFW den zulässigen Datenverkehr scannen und Bedrohungen wie Viren, Malware, Spyware und DDoS-Angriffe blockieren soll.

## IPS und Schutz vor Spyware-Bedrohungen

- **IPS Vulnerability (IPS-Sicherheitslücke)** – (standardmäßig aktiviert und basierend auf Best Practices vorkonfiguriert) Ein Sicherheitslückenprofil für Intrusion Prevention System (IPS) stoppt Versuche, Systemfehler auszunutzen oder unbefugten Zugriff auf Systeme zu erlangen. Während Anti-Spyware-Profile infizierte Hosts identifizieren, wenn Datenverkehr das Netzwerk verlässt, schützen IPS-Sicherheitslückenprofile vor Bedrohungen, die in das Netzwerk eindringen. Vulnerability Protection-Profile schützen beispielsweise vor Pufferüberläufen, illegaler Codeausführung und anderen Versuchen, Systemsicherheitslücken auszunutzen. Das Standardprofil für Vulnerability Protection schützt Clients und Server vor allen bekannten Bedrohungen mit kritischem, hohem und mittlerem Schweregrad.

  In der folgenden Tabelle wird die Best Practice-Standardkonfiguration für IPS-Sicherheitslücken beschrieben.

| Schweregrad der Signatur | Aktion |
|---|---|
| Kritisch | Beide zurücksetzen |
| Hoch | Beide zurücksetzen |
| Mittel | Beide zurücksetzen |
| Informativ | Standard |
| Niedrig | Standard |

- **Anti-Spyware** – (standardmäßig aktiviert und basierend auf Best Practices vorkonfiguriert) Ein Anti-Spyware-Profil hindert Spyware daran, auf kompromittierten Hosts externe Command-and-Control-Server (C2) per Telefon oder Beacon zu erreichen, sodass Sie bösartigen Datenverkehr erkennen können, der das Netzwerk über infizierte Clients verlässt.

  In der folgenden Tabelle wird die Best Practice-Standardkonfiguration für Anti-Spyware beschrieben.

| Schweregrad der Signatur | Aktion |
|---|---|
| Kritisch | Beide zurücksetzen |
| Hoch | Beide zurücksetzen |
| Mittel | Beide zurücksetzen |
| Informativ | Standard |

| Schweregrad der Signatur | Aktion |
|---|---|
| Niedrig | Standard |


In der folgenden Tabelle sind alle möglichen Signaturen für die Kategorien „Vulnerability“ (Sicherheitslücken) und „Spyware“ aufgeführt. Diese Signaturen werden in Ihren NGFWs kontinuierlich aktualisiert.

| Bedrohungskategorie | Beschreibung |
|---|---|
| **Signaturen für Sicherheitslücken** | |
| Brute-Force | Eine Brute-Force-Signatur erkennt mehrere Vorkommen eines Problems in einem bestimmten Zeitraum. Die isolierte Aktivität kann zwar harmlos sein, die Brute-Force-Signatur weist aber darauf hin, dass die Häufigkeit und Geschwindigkeit, mit der die Aktivität aufgetreten ist, verdächtig ist. Beispielsweise deutet ein einzelner FTP-Anmeldefehler nicht auf bösartige Aktivitäten hin. Viele fehlgeschlagene FTP-Anmeldungen innerhalb eines kurzen Zeitraums können jedoch darauf hindeuten, dass ein Angreifer versucht, Passwortkombinationen für den Zugriff auf einen FTP-Server zu finden. |
| code execution | Erkennt eine Sicherheitslücke bei der Codeausführung, die ein Angreifer nutzen kann, um Code auf einem System mit den Berechtigungen des angemeldeten Benutzers auszuführen. |
| code-obfuscation | Erkennt Code, der umgewandelt wurde, um bestimmte Daten zu verbergen, während seine Funktion erhalten bleibt. Verschleierter Code ist schwer oder unmöglich zu lesen und lässt nicht erkennen, welche Befehle er ausführt oder mit welchen Programmen er interagieren soll. Am häufigsten wird Code von bösartigen Akteuren verschleiert, um Malware zu verbergen. Seltener können auch seriöse Entwickler Code verschleiern, um die Privatsphäre und das geistige Eigentum zu schützen oder die Benutzererfahrung zu |

| Bedrohungskategorie | Beschreibung |
|---|---|
| | verbessern. Beispielsweise reduzieren bestimmte Arten der Verschleierung (wie Minimierung) die Dateigröße, wodurch die Ladezeiten der Website und die Bandbreitennutzung verringert werden. |
| DoS | Erkennt einen Denial-of-Service-Angriff (Nichtverfügbarkeit des Dienstes, DoS), bei dem ein Angreifer versucht, ein Zielsystem unnutzbar zu machen, wodurch das System und abhängige Anwendungen und Dienste vorübergehend unterbrochen werden. Um einen DoS-Angriff durchzuführen, kann ein Angreifer ein Zielsystem mit Datenverkehr überfluten oder Informationen senden, die zum Ausfall führen. DoS-Angriffe verhindern, dass berechtigte Benutzer (wie Mitarbeiter, Mitglieder und Kontoinhaber) den Dienst oder die Ressource nutzen können, auf den bzw. die sie zugreifen möchten. |
| exploit-kit | Erkennt eine Exploit-Kit-Landingpage. Exploit-Kit-Landingpages enthalten oft mehrere Exploits, die eine oder mehrere gängige Sicherheitslücken (Common Vulnerabilities and Exposures, CVEs) bei Browsern und Plug-ins ausnutzen. Da sich die CVEs schnell ändern, werden Exploit-Kit-Signaturen basierend auf der Exploit-Kit-Landingpage und nicht basierend auf den CVEs ausgelöst.<br><br>Wenn ein Benutzer eine Website mit einem Exploit-Kit besucht, sucht das Exploit-Kit nach den CVEs und versucht, im Hintergrund eine bösartige Nutzlast auf den Computer des Opfers zu übertragen. |
| info-leak | Erkennt eine Software-Sicherheitslücke, die ein Angreifer ausnutzen könnte, um vertrauliche oder geschützte Informationen zu stehlen. Oft kann es zu einem Informationsleck kommen, weil keine umfassenden Überprüfungen zum Schutz der Daten vorhanden sind. Angreifer können Informationslecks außerdem ausnutzen, indem sie speziell ausgearbeitete Anfragen senden. |
| insecure-credentials | Erkennt die Verwendung von schwachen, kompromittierten Passwörtern und von Hersteller-Standardpasswörtern für Software, Netzwerkgeräte und IoT-Geräte. |
| Overflow | Erkennt eine Überlauf-Sicherheitslücke, bei der ein Mangel an ordnungsgemäßen Überprüfungen von Anfragen ausgenutzt werden könnte. Ein erfolgreicher Angriff könnte zur Remotecodeausführung mit den Berechtigungen der Anwendung, des Servers oder des Betriebssystems führen. |
| phishing | Erkennt, wenn ein Benutzer versucht, eine Verbindung zu einer Phishing-Kit-Landingpage herzustellen (wahrscheinlich nachdem er eine E-Mail mit einem Link zu der schädlichen Website erhalten hat). Eine Phishing-Website verleitet Benutzer dazu, Anmelde-Informationen einzugeben, die ein Angreifer dann abgreifen kann, um Zugriff auf das Netzwerk zu erhalten. |

| Bedrohungskategorie | Beschreibung |
|---|---|
| protocol-anomaly | Erkennt Protokollanomalien: ein Protokollverhalten, das von der standardmäßigen und konformen Verwendung abweicht. Ein fehlerhaftes Paket, eine schlecht geschriebene Anwendung oder eine Anwendung, die auf einem nicht standardmäßigen Port ausgeführt wird, würden beispielsweise als Protokollanomalien betrachtet und könnten als Sicherheitsumgehungstools verwendet werden. |
| sql-injection | Erkennt eine gängige Hacking-Technik, bei der ein Angreifer SQL-Abfragen in die Anforderungen einer Anwendung einfügt, um aus einer Datenbank zu lesen oder diese zu ändern. Diese Art von Technik wird häufig auf Websites verwendet, die Benutzereingaben nicht umfassend bereinigen. |
| **Signaturen für Spyware** | |
| Spyware | Erkennt ausgehende C2-Kommunikation. Diese Signaturen werden entweder automatisch generiert oder manuell von den Forschern von Palo Alto Networks erstellt.<br><br>*Sowohl Spyware- als auch Autogen-Signaturen erkennen ausgehende C2-Kommunikation. Autogen-Signaturen sind jedoch nutzlastbasiert und können C2-Kommunikationen mit unbekannten oder sich schnell ändernden C2-Hosts eindeutig erkennen.* |
| adware | Erkennt Programme, die potenziell unerwünschte Werbung anzeigen. Manche Adware modifiziert Browser, um die am häufigsten gesuchten Keywords auf Webseiten hervorzuheben und zu verlinken. Diese Links leiten Benutzer zu Werbewebsites weiter. Adware kann Updates auch von einem Command-and-Control-Server (C2) abrufen und diese Updates in einem Browser oder auf einem Clientsystem installieren. |
| autogen | Diese nutzlastbasierten Signaturen erkennen Command-and-Control(C2)-Datenverkehr und werden automatisch generiert. Wichtig ist, dass autogen-Signaturen C2-Datenverkehr auch dann erkennen können, wenn der C2-Host unbekannt ist oder sich schnell ändert. |
| Backdoor | Erkennt ein Programm, das es einem Angreifer ermöglicht, unbefugten Remotezugriff auf ein System zu erlangen. |
| Botnet | Zeigt Botnet-Aktivitäten an. Ein Botnet ist ein Netzwerk von mit Malware infizierten Computern („Bots“), die ein Angreifer kontrolliert. Der Angreifer kann jedem Computer in einem Botnet zentral befehlen, gleichzeitig eine koordinierte Aktion auszuführen (wie zum Beispiel einen DoS-Angriff zu starten). |

| Bedrohungskategorie | Beschreibung |
|---|---|
| browser-hijack | Erkennt ein Plug-in oder eine Software, die die Browsereinstellungen ändert. Ein Browser-Hijacker kann die automatische Suche übernehmen oder die Webaktivität der Benutzer verfolgen und diese Informationen an einen C2-Server senden. |
| cryptominer | (Manchmal auch als Cryptojacking oder Miner bezeichnet) Erkennt den Download-Versuch oder den Netzwerkverkehr, der von bösartigen Programmen generiert wird, die Computerressourcen verwenden, um Kryptowährungen ohne Wissen des Benutzers zu schürfen. Cryptominer-Binärdateien werden häufig von einem Shell-Skript-Downloader bereitgestellt, der versucht, die Systemarchitektur zu bestimmen und andere Miner-Prozesse auf dem System zu beenden. Einige Miner werden in anderen Prozessen ausgeführt, z. B. in einem Webbrowser, der eine schädliche Webseite rendert. |
| data-theft | Erkennt ein System, das Informationen an einen bekannten C2-Server sendet. |
| DNS | Erkennt DNS-Anfragen zum Herstellen einer Verbindung zu bösartigen Domänen. |
| downloader | (Auch bekannt als Dropper, Stager oder Loader) Erkennt Programme, die eine Internetverbindung verwenden, um eine Verbindung zu einem Remote-Server herzustellen und dann Malware auf das kompromittierte System herunterzuladen und dort auszuführen. Der häufigste Anwendungsfall ist die Bereitstellung eines Downloaders als Höhepunkt der *ersten Phase* eines Cyberangriffs. Die abgerufene Nutzlastausführung des Downloaders wird als *zweite Phase* betrachtet. Shell-Skripte (Bash, PowerShell usw.), Trojaner und bösartige Köderdokumente (auch bekannt als MalDocs) wie PDFs und Word-Dateien sind gängige Downloader-Typen. |
| fraud | (Einschließlich Formjacking, Phishing und Scam) Erkennt den Zugriff auf kompromittierte Websites, denen böswilliger JavaScript-Code injiziert wurde, um sensible Benutzerinformationen zu sammeln. (Beispiel: Name, Adresse, E-Mail, Kreditkartennummer, CVV, Ablaufdatum) aus Zahlungsformularen, die auf den Kassenseiten von E-Commerce-Websites erfasst werden. |
| hacktool | Erkennt den von Softwaretools generierten Datenverkehr, die von bösartigen Akteuren verwendet werden, um Dinge auszukundschaften, anfällige Systeme anzugreifen oder Zugriff auf sie zu erhalten, Daten herauszufiltern oder einen Command-and-Control-Kanal zu erstellen, über den ein Computersystem unbemerkt und ohne Autorisierung gesteuert werden kann. Diese Programme werden mit Malware und Cyberangriffen in Verbindung gebracht. Hacking-Tools können auch auf harmlose Weise eingesetzt werden, z. B. für Red- and Blue-Team-Übungen, Penetrationstests und Forschung und Entwicklung. Die Verwendung oder der Besitz dieser Tools ist in manchen Ländern illegal, unabhängig von der Nutzungsabsicht. |

| Bedrohungskategorie | Beschreibung |
|---|---|
| networm | Erkennt ein Programm, das sich selbst repliziert und von System zu System verbreitet. Netzwürmer nutzen freigegebene Ressourcen oder Sicherheitslücken, um auf Zielsysteme zuzugreifen. |
| phishing-kit | Erkennt, wenn ein Benutzer versucht, eine Verbindung zu einer Phishing-Kit-Landingpage herzustellen (wahrscheinlich nachdem er eine E-Mail mit einem Link zu der schädlichen Website erhalten hat). Eine Phishing-Website verleitet Benutzer dazu, Anmelde-Informationen einzugeben, die ein Angreifer dann abgreifen kann, um Zugriff auf das Netzwerk zu erhalten. |
| postexploitation | Erkennt Aktivitäten, die auf einen vorangegangenen Exploit-Angriff hinweisen. In dieser Phase versuchen die Angreifer, den Wert eines kompromittierten Systems zu bestimmen. Dies kann die Bewertung der Sensibilität der auf dem System gespeicherten Daten und die Nützlichkeit des Systems für die weitere Kompromittierung des Netzwerks umfassen. |
| Webshell | Erkennt Web-Shells und Web-Shell-Verkehr, einschließlich Implantaten und Befehls- und Steuerungsinteraktionen. Ein Bedrohungsakteur implantiert eine Web-Shell auf dem kompromittierten Host, wobei das Ziel meistens Webserver oder Frameworks sind. Die anschließende Kommunikation mit der Web-Shell-Datei ermöglicht es einem böswilligen Akteur häufig, im System Fuß zu fassen, Dienst- und Netzwerk-Enumerationen durchzuführen, Daten herauszufiltern und Remotecode im Kontext des Webserverbenutzers auszuführen. Die gebräuchlichsten Web-Shell-Typen sind PHP-, .NET- und Perl-Markup-Skripte. Angreifer können auch Web-Shell-infizierte Webserver verwenden (die Webserver können sowohl mit dem Internet als auch mit internen Systemen verbunden sein), um andere interne Systeme ins Visier zu nehmen. |
| keylogger | Erkennt Programme, mit denen Angreifer Benutzeraktivitäten heimlich verfolgen können, indem sie Tastenanschläge protokollieren und Screenshots aufnehmen.<br><br>Keylogger verwenden verschiedene C2-Methoden, um regelmäßig Protokolle und Berichte an eine vordefinierte E-Mail-Adresse oder einen C2-Server zu senden. Durch die Keylogger-Überwachung kann ein Angreifer Anmelde-Informationen abrufen, die den Netzwerkzugriff ermöglichen. |

## Schutz vor Malware und dateibasierten Bedrohungen

- **Antivirus** – (standardmäßig aktiviert und basierend auf Best Practices vorkonfiguriert) Antivirenprofile schützen vor Malware, Würmern und Trojanern sowie vor Spyware-Downloads. Mithilfe einer streambasierten Malware-Präventions-Engine, die den Datenverkehr überprüft, sobald das erste Paket empfangen wird, kann die Antivirus-Lösung von Palo Alto Networks Clients schützen, ohne die Leistung der Firewall erheblich zu beeinträchtigen. Dieses Profil scannt ausführbare

Dateien, PDF-Dateien, HTML und JavaScript auf Malware, auch in komprimierten Dateien und Datencodierungsschemata.

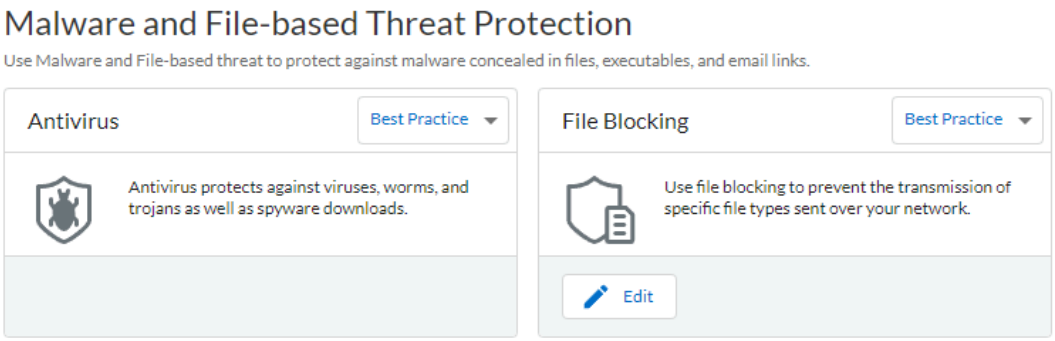
In der folgenden Tabelle wird die Best Practice-Standardkonfiguration für Antivirus-Lösungen beschrieben.

| Protokoll | Aktion |
|---|---|
| FTP | Beide zurücksetzen |
| HTTP | Beide zurücksetzen |
| HTTP2 | Beide zurücksetzen |
| IMAP | Beide zurücksetzen |
| POP3 | Benachrichtigen |
| SMB | Beide zurücksetzen |
| SMTP | Beide zurücksetzen |

- **File Blocking (Dateiblockade)** – Ein Dateiblockade-Profil ermöglicht es Ihnen, bestimmte Dateitypen anzugeben, die Sie blockieren oder überwachen möchten. Die Firewall verwendet Datei-Blockade-Profile, um bestimmte Dateitypen über bestimmte Anwendungen und in der angegebenen Sitzungsrichtung (eingehend/ausgehend/beides) zu blockieren. Sie können das Profil so einstellen, dass es beim Hoch- und/oder Herunterladen alarmiert oder blockiert, und Sie können angeben, für welche Anwendungen das Datei-Blockade-Profil gelten soll.
  - **Alert (Benachrichtigen)** – Wenn der angegebene Dateityp erkannt wird, wird ein Protokoll im Datenfilterungsprotokoll generiert.

- **Block (Blockieren)** – Wenn der angegebene Dateityp erkannt wird, wird die Datei blockiert. Im Datenfilterungsprotokoll wird auch ein Protokoll generiert. Informationen zum Ändern Ihres Dateiblockadeprofils finden Sie unter Dateiblockade einrichten.




In der folgenden Tabelle wird die Best Practice-Standardkonfiguration für Dateiblockaden beschrieben.

| Dateitypen | Anwendung | Richtung | Aktion |
|---|---|---|---|
| Alle riskanten Dateitypen:<br>• 7z<br>• bat<br>• cab<br>• chm<br>• class<br>• CPL<br>• DLL<br>• exe<br>• flash<br>• hip<br>• hta<br>• msi<br>• Multi-Level-Encoding<br>• ocx<br>• PE<br>• pif<br>• rar<br>• scr<br>• tar<br>• torrent | Beliebige | Beides (Hochladen und Herunterladen) | Blockieren |

| Dateitypen | Anwendung | Richtung | Aktion |
|---|---|---|---|
| • vbe<br>• wsf<br>• encrypted-rar<br>• encrypted-zip | | | |
| Alle übrigen Dateitypen | Beliebige | Beides (Hochladen und Herunterladen) | Benachrichtigen |

In der folgenden Tabelle sind alle möglichen Signaturen für die Kategorie „Antivirus“ aufgeführt. Diese Signaturen werden in Ihren NGFWs kontinuierlich aktualisiert.

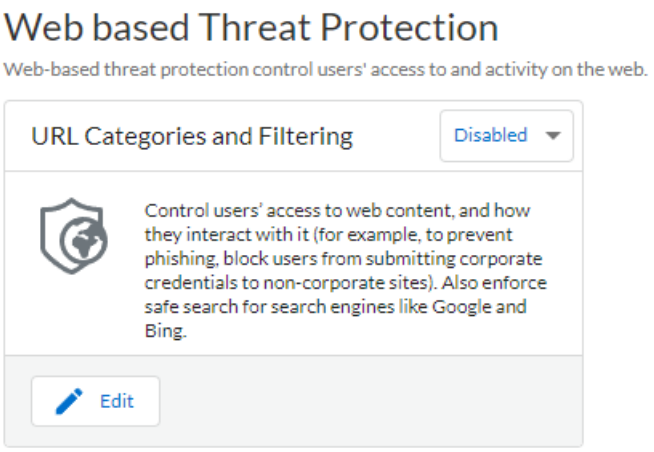
| Bedrohungskategorie | Beschreibung |
|---|---|
| **Antivirus-Signaturen** | |
| APK | Bösartige Android-Anwendungsdateien (APK). |
| Mac OS X | Bösartige Mac OS X-Dateien, einschließlich:<br>• Apple Disk Image (DMG)-Dateien.<br>• Mach-Objektdateien (Mach-O) sind ausführbare Dateien, Bibliotheken und Objektcode.<br>• Apple-Software-Installationspakete (PKGs) |
| flash | In Webseiten eingebettete Adobe Flash-Applets und Flash-Inhalte. |
| jar | Java-Applets (JAR-/Klassendateitypen). |
| ms-office | Microsoft Office-Dateien, einschließlich Dokumenten (DOC, DOCX, RTF), Arbeitsmappen (XLS, XLSX) und PowerPoint-Präsentationen (PPT, PPTX). Dazu gehören auch Office Open XML (OOXML) 2007+-Dokumente. |
| pdf | PDF-Dateien (Portable Document Format). |
| PE | Portable-Executable(PE)-Dateien können automatisch auf einem Microsoft Windows-System ausgeführt werden und sollten nur zugelassen werden, wenn sie autorisiert sind. Zu diesen Dateitypen gehören:<br>• Objektcode.<br>• Schriftarten (FONs).<br>• Systemdateien (SYS).<br>• Treiberdateien (DRV).<br>• Elemente der Windows-Systemsteuerung (CPLs).<br>• DLLs (Dynamic-Link-Bibliotheken). |

| Bedrohungskategorie | Beschreibung |
|---|---|
| | • OCXs (Bibliotheken für benutzerdefinierte OLE-Steuerelemente oder ActiveX-Steuerelemente).<br>• Windows-Bildschirmschonerdateien (SCRs).<br>• Extensible-Firmware-Interface(EFI)-Dateien, die zwischen einem Betriebssystem und der Firmware ausgeführt werden, um Geräteaktualisierungen und Startvorgänge zu erleichtern.<br>• Programminformationsdateien (PIFs). |
| linux | Executable and Linking Format-Dateien (ELF). |
| archive | Roshal Archive (RAR)- und 7-Zip (7z)-Archivdateien. |

## Schutz vor webbasierten Bedrohungen

- **URL Categories and Filtering (URL-Kategorien und Filterung)** – Mit URL-Filterungsprofilen können Sie überwachen und steuern, wie Benutzer über HTTP und HTTPS auf das Web zugreifen. Die Firewall verfügt über ein Standardprofil, das so konfiguriert ist, dass Websites wie bekannte Malware-Websites, Phishing-Websites und Websites mit nicht jugendfreien Inhalten blockiert werden. Das URL-Filterungsprofil ist standardmäßig nicht aktiviert. Wenn Sie das URL-Filterungsprofil in Ihrem Regelstapel aktivieren, erzwingt Cloud NGFW das Best Practices-URL-Filterungsprofil für Ihren Datenverkehr. Sie haben die Möglichkeit, die Standardzugriffsoption für jede der Kategorien entsprechend Ihren Anforderungen zu ändern




In der folgenden Tabelle wird die Best Practice-Standardkonfiguration für die URL-Filterung beschrieben.

| URL-Kategorien | Websitezugriff | Übermittlung von Anmeldeinformationen |
|---|---|---|
| Bösartige und missbräuchliche Kategorien:<br>• adult | Blockieren | Blockieren |

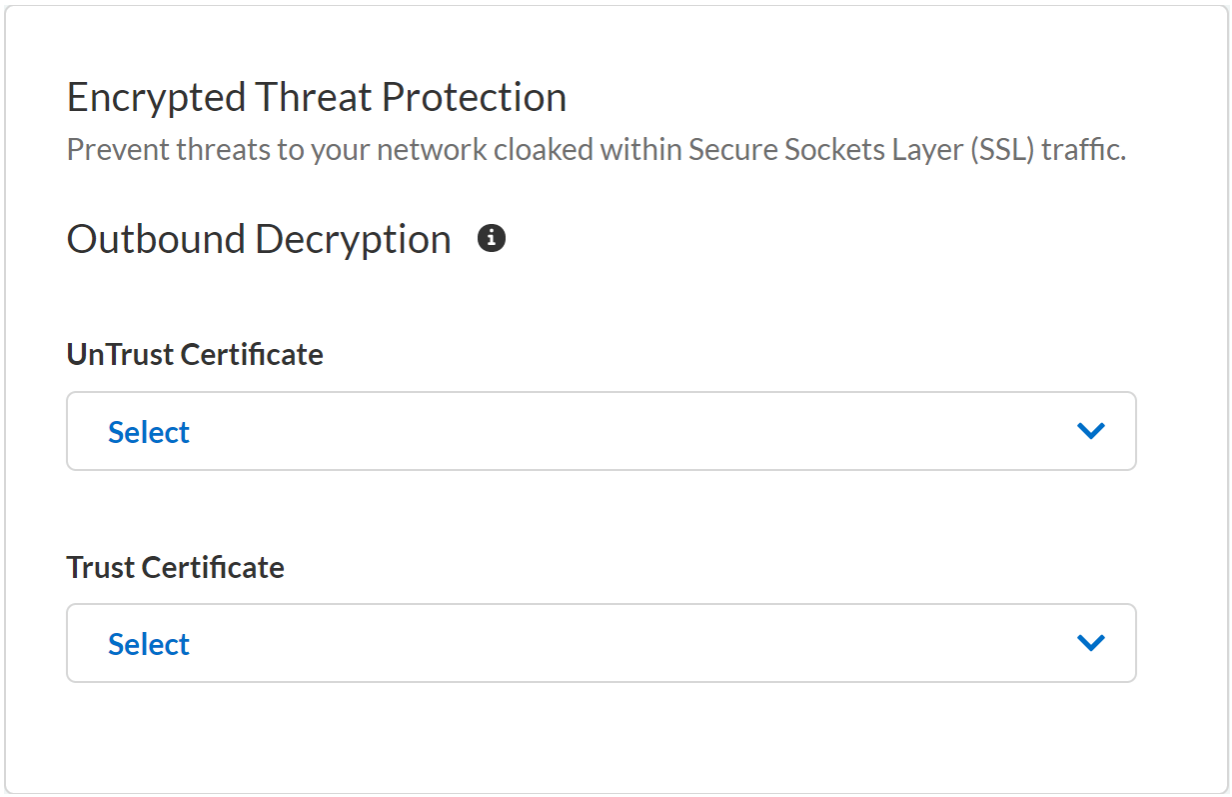
| URL-Kategorien | Websitezugriff | Übermittlung von Anmeldeinformationen |
|---|---|---|
| • Command and Control<br>• copyright-infringement<br>• Dynamisches DNS<br>• extremism<br>• Malware<br>• parked<br>• phishing<br>• proxy-avoidance-and-anonymizers<br>• unknown | | |
| Alle anderen URL-Kategorien | Benachrichtigen | Benachrichtigen |

## Schutz vor Verschlüsselungsbedrohungen

- **Outbound Decryption (Ausgehende Entschlüsselung)** – Mit einem Profil für ausgehende Entschlüsselung können Sie den zu entschlüsselnden Datenverkehr nach Ziel, Quelle, Dienst oder URL-Kategorie angeben und den angegebenen Datenverkehr gemäß den Sicherheitseinstellungen im zugehörigen Entschlüsselungsprofil blockieren, einschränken oder weiterleiten. Ein Profil für ausgehende Entschlüsselung steuert SSL-Protokolle, Zertifikatsverifizierung und Fehlerprüfungen, um zu verhindern, dass Datenverkehr, der schwache Algorithmen oder nicht unterstützte Modi verwendet, auf das Netzwerk zugreift. Cloud NGFW-Ressourcen verwenden Zertifikate, um Datenverkehr in Klartext zu entschlüsseln. Anschließend werden App-ID- und Sicherheitsprofile für den Klartext-Datenverkehr durchgesetzt, einschließlich Profilen für Entschlüsselung, Antivirus, Sicherheitslücken, Anti-Spyware, URL-Filter und Dateiblockaden. Nach dem Entschlüsseln und Überprüfen des

Datenverkehrs verschlüsselt die Firewall den Klartext-Datenverkehr beim Verlassen der Firewall erneut, um Datenschutz und Sicherheit zu gewährleisten.



## Vordefinierte URL-Kategorien für Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

In der folgenden Tabelle werden die vordefinierten URL-Kategorien beschrieben, die in Cloud NGFW für AWS verfügbar sind. Sie können diese Kategorien in Sicherheitsregeln verwenden, um den Zugriff auf Websites, die in diese Kategorien fallen, zu blockieren oder zuzulassen.

| URL-Kategorie | Beschreibung |
|---|---|
| **Risikokategorien** | |
| Hohes Risiko | Websites, die zuvor als bösartig eingestuft wurden, aber seit mindestens 30 Tagen harmlose Aktivitäten aufweisen. Websites, die auf Bulletproof-ISPs gehostet werden oder eine IP von einem ASN verwenden, das bekanntermaßen bösartigen Inhalt hat. Websites mit einer Domäne, die mit der Domäne einer bekannten bösartigen Website identisch ist. Alle Websites in der Kategorie „Unknown“ (Unbekannt) weisen ein hohes Risiko auf. |
| Mittleres Risiko | Websites, die als bösartig bestätigt wurden, aber seit mindestens 60 Tagen harmlose Aktivitäten aufweisen. Alle Websites in der Kategorie „Online Storage and Backup“ (Online-Speicher und Datensicherung) weisen standardmäßig ein mittleres Risiko auf. |
| Geringes Risiko | Jede Website, die kein hohes oder mittleres Risiko aufweist. Dazu gehören Websites, die zuvor als bösartig bestätigt wurden, aber seit mindestens 90 Tagen harmlose Aktivitäten aufweisen. |
| **Bedrohungskategorien** | |
| Command and Control | Command-and-Control-URLs und -Domänen, die von Malware und/oder kompromittierten Systemen verwendet werden, um heimlich mit dem Remote-Server eines Angreifers zu kommunizieren und bösartige Befehle zu empfangen oder Daten abzugreifen. |

| URL-Kategorie | Beschreibung |
|---|---|
| Malware | Websites, von denen bekannt ist, dass sie Malware hosten oder für Command-and-Control-Datenverkehr (C2) verwendet werden. Kann auch Exploit-Kits ausgeben. |
| **Mit Bedrohungen zusammenhängende Kategorien** | |
| Dynamisches DNS | Hosts und Domänennamen für Systeme mit dynamisch zugewiesenen IP-Adressen, die häufig verwendet werden, um Malware-Nutzlasten oder C2-Datenverkehr zu übermitteln. Außerdem durchlaufen dynamische DNS-Domänen nicht den gleichen Überprüfungsprozess wie Domänen, die durch ein seriöses Domänenregistrierungsunternehmen registriert wurden, und sind daher weniger vertrauenswürdig. |
| Grayware | Webinhalte, die keine direkte Sicherheitsbedrohung darstellen, aber durch andere aufdringliche Verhaltensweisen auffallen und den Endbenutzer dazu verleiten, Fernzugriff zu gewähren oder andere nicht autorisierte Aktionen durchzuführen. Grayware umfasst illegale und kriminelle Aktivitäten, Rogueware, Adware und andere unerwünschte oder unerbetene Anwendungen, wie eingebettete Crypto-Miner, Clickjacking oder Hijacker, die die Elemente des Browsers manipulieren. Typosquatting-Domänen, die keine Bösartigkeit aufweisen und nicht zur Zieldomäne gehören, werden als Grayware kategorisiert. |
| Hacken | Websites, die auf Kommunikationsgeräte und Software illegal oder in fragwürdiger Weise zugreifen oder diese illegal oder in fragwürdiger Weise nutzen. Entwicklung und Verbreitung von Programmen, Anleitungen und/oder Tipps, die zur Kompromittierung von Netzwerken und Systemen führen können. Umfasst auch Websites, die die Umgehung von Lizenzierungs- und digitalen Rechtesystemen erleichtern. |
| Phishing | Webinhalte, die heimlich versuchen, den Benutzer zu täuschen, um mithilfe von Social-Engineering-Techniken Informationen zu sammeln, einschließlich Anmeldeinformationen, Kreditkarteninformationen (absichtlich oder unabsichtlich), Kontonummern, PINs und aller Informationen, die als personenbezogene Daten gelten. Betrug mit technischem Support und Scareware gehören ebenfalls zur Phishing-Kategorie. |
| **Verdächtig** | |
| Unzureichender Inhalt | Websites und Dienste, die Testseiten oder keinen Inhalt präsentieren, API-Zugriff gewähren, der nicht für die Anzeige |

| URL-Kategorie | Beschreibung |
| --- | --- |
| | durch Endbenutzer vorgesehen ist, oder eine Authentifizierung erfordern, ohne andere Inhalte anzuzeigen, die auf eine andere Kategorisierung schließen lassen. Diese Kategorie sollte keine Websites enthalten, die Fernzugriff ermöglichen, wie etwa webbasierte VPN-Lösungen, webbasierte E-Mail-Dienste oder Seiten zum Phishing identifizierter Anmeldeinformationen. |
| Neu registrierte Domäne | Neu registrierte Domänen werden häufig absichtlich oder durch Domänengenerierungsalgorithmen generiert und für bösartige Aktivitäten verwendet. |
| Geparkt | Von Einzelpersonen registrierte Domänen, die oft später für Anmeldedaten-Phishing verwendet werden. Diese Domänen können legitimen Domänen ähneln, z. B. pal0alto0netw0rks.com, mit der Absicht, Anmeldeinformationen oder personenbezogene Daten abzugreifen. Oder es können Domänen sein, an denen eine Person Rechte erwirbt, in der Hoffnung, dass sie eines Tages wertvoll sein könnten, wie z. B. panw.net. |
| Proxy-Vermeidung und Anonymisierer | URLs und Dienste, die häufig verwendet werden, um Inhaltsfilterungen zu umgehen. |
| Unbekannt | Websites, die noch nicht von Palo Alto Networks identifiziert wurden. Wenn Verfügbarkeit für Ihr Unternehmen von entscheidender Bedeutung ist und Sie den Datenverkehr zulassen müssen, lassen Sie sich vor unbekannten Websites warnen, wenden Sie Best-Practice-Sicherheitsprofile auf den Datenverkehr an und gehen Sie den Warnungen nach. |
| **Rechtliches/Richtlinienbezogenes** | |
| Abtreibung | Websites, die sich mit Informationen oder Gruppen für oder gegen Abtreibung befassen, Einzelheiten zu Abtreibungsverfahren enthalten, Hilfe- oder Unterstützungsforen für oder gegen Abtreibung umfassen, oder Websites, die Informationen zu den Folgen und Auswirkungen einer Abtreibung (oder einer nicht vorgenommenen Abtreibung) bereitstellen. |
| Drogenmissbrauch | Websites, die für den Missbrauch legaler und illegaler Drogen, die Verwendung und den Verkauf von Drogenutensilien, die Herstellung und/oder den Verkauf von Drogen werben. |
| Erwachsene | Sexuell explizites Material, Medien (einschließlich Sprache), Kunst und/oder Produkte, Online-Gruppen oder Foren, die sexuell explizit sind. Websites, die nicht jugendfreie Dienste |

| URL-Kategorie | Beschreibung |
|---|---|
| | wie Video- und Telefonanrufe, Escort-Services, Stripclubs usw. bewerben. Alles, was nicht jugendfreie Inhalte enthält (auch wenn es sich um Spiele oder Comics handelt), wird als nicht jugendfrei kategorisiert. |
| Alkohol und Tabak | Websites, auf denen es um den Verkauf, die Herstellung oder den Konsum von Alkohol und/oder Tabakprodukten und damit verbundenen Utensilien geht. Umfasst auch Websites im Zusammenhang mit elektronischen Zigaretten. |
| Auktionen | Websites, die den Verkauf von Waren zwischen Privatpersonen fördern. |
| Geschäft und Wirtschaft | Marketing, Management, Wirtschaft und Websites in Bezug auf Unternehmertum oder die Führung eines Unternehmens. Umfasst auch Werbe- und Marketingfirmen. Sollte keine Unternehmens-Websites umfassen, da sie anhand der Technologien kategorisiert werden sollten. Auch Speditions-Websites wie fedex.com und ups.com. |
| Computer- und Internetinformationen | Allgemeine Informationen zu Computern und Internet. Sollte Websites zu Informatik, Technik, Hardware, Software, Sicherheit, Programmierung usw. enthalten. Programmierung kann sich mit „Referenz und Recherche“ überschneiden, aber die Hauptkategorie sollte „Computer- und Internetinformationen“ bleiben. |
| Content Delivery Networks | Websites, deren Hauptaugenmerk auf der Bereitstellung von Inhalten für Drittanbieter liegt, z. B. Anzeigen, Medien, Dateien usw. Umfasst auch Bildserver. |
| Copyright-Verletzung | Domänen mit illegalen Inhalten, wie z. B. Inhalten, die das illegale Herunterladen von Software oder anderem geistigen Eigentum ermöglichen, was ein potenzielles Haftungsrisiko darstellt. Diese Kategorie wurde eingeführt, um die Einhaltung der in der Bildungsbranche erforderlichen Kinderschutzgesetze sowie der Gesetze in Ländern zu ermöglichen, die Internetanbieter dazu verpflichten, Benutzer an der Weitergabe von urheberrechtlich geschütztem Material über ihren Dienst zu hindern. |
| Kryptowährung | Websites, die Kryptowährungen bewerben, Krypto-Mining-Websites (aber keine eingebetteten Krypto-Miner), Kryptowährungsbörsen und -anbieter sowie Websites, die Kryptowährungs-Wallets und -Ledger verwalten. Diese Kategorie umfasst keine herkömmlichen Finanzdienstleistungs-Websites, die auf Kryptowährungen verweisen; Websites, die erklären und beschreiben, wie Kryptowährungen und |

| URL-Kategorie | Beschreibung |
|---|---|
| | Blockchains funktionieren; oder Websites, die eingebettete Kryptowährungs-Miner (Grayware) enthalten. |
| Dating | Websites, die Online-Dating-Dienste, Beratung und andere persönliche Anzeigen anbieten. |
| Bildungseinrichtungen | Offizielle Websites für Schulen, Universitäten, Online-Kurse und andere akademische Einrichtungen. Das können vor allem größere, etablierte Bildungseinrichtungen wie Grundschulen, Gymnasien, Universitäten etc. sein. Auch Nachhilfeakademien gehören dazu. |
| Unterhaltung und Kunst | Websites für Filme, Fernsehen, Radio, Videos, Programmführer und -tools, Comics, darstellende Künste, Museen, Kunstgalerien oder Bibliotheken. Umfasst Websites für Unterhaltung und News über Prominente sowie Branchennachrichten. |
| Extremismus | Websites, die Terrorismus, Rassismus, Faschismus oder andere extremistische Ansichten fördern, die Menschen oder Gruppen unterschiedlicher ethnischer Herkunft, Religion oder anderer Überzeugungen diskriminieren. Diese Kategorie wurde eingeführt, um die Einhaltung der in der Bildungsbranche erforderlichen Kinderschutzgesetze zu ermöglichen. In einigen Regionen können Gesetze und Vorschriften den Zugriff auf extremistische Websites verbieten und das Erlauben des Zugriffs kann ein Haftungsrisiko darstellen. |
| Finanzielle Dienstleistungen | Websites, die sich auf persönliche Finanzinformationen oder -beratung beziehen, z. B. Online-Banking, Kredite, Hypotheken, Schuldenmanagement, Kreditkartenunternehmen und Versicherungsunternehmen. Umfasst keine Websites in Bezug auf Aktienmärkte, Maklergeschäfte oder Handelsdienstleistungen. Umfasst Websites für Devisenumtausch. |
| Glücksspiel | Lotterie- oder Glücksspiel-Websites, die den Tausch von echtem und/oder virtuellem Geld ermöglichen. Verwandte Websites, die Informationen, Tutorials oder Ratschläge zum Glücksspiel bieten, einschließlich Wettquoten und Wettpools. Unternehmenswebsites für Hotels und Casinos, bei denen keine Glücksspiele möglich sind, werden unter „Reisen“ kategorisiert. |
| Spiele | Websites, die Online-Spiele oder Downloads von Video- und/oder Computerspielen, Spielrezensionen, Tipps oder Tricks sowie Anleitungsseiten für nicht elektronische Spiele, den Verkauf und Handel von Brettspielen oder verwandte Veröffentlichungen/Medien anbieten. Hierzu zählen |

| URL-Kategorie | Beschreibung |
|---|---|
| | Websites, die Online-Gewinnspiele und/oder Werbegeschenke unterstützen oder hosten. |
| Regierung | Offizielle Websites für lokale, staatliche und nationale Regierungen sowie der zugehörigen Behörden, Dienste oder Gesetze. |
| Gesundheit und Medizin | Websites mit Informationen zu allgemeinen Gesundheitsthemen, Problemen sowie traditionellen und nicht traditionellen Tipps, Heilmitteln und Behandlungen. Umfasst auch Websites für verschiedene medizinische Fachgebiete, Praxen und Einrichtungen (z. B. Fitnessstudios und Fitnessclubs) sowie Fachleute. Websites zu Krankenversicherungen und Schönheitsoperationen sind ebenfalls enthalten. |
| Haus und Garten | Informationen, Produkte und Dienstleistungen in Bezug auf Hausreparatur und -wartung, Architektur, Design, Bau, Dekoration und Gartenarbeit. |
| Jagen und Fischen | Jagd- und Angeltipps, Anleitungen, Verkauf von dazugehöriger Ausrüstung und Utensilien. |
| Internetkommunikation und Telefonie | Websites, die Dienste für Video-Chats, Instant Messaging oder Telefoniefunktionen unterstützen oder bereitstellen. |
| Internetportale | Websites, die als Ausgangspunkt für Benutzer dienen, normalerweise durch die gesammelte Darstellung einer breiten Palette von Inhalten und Themen. |
| Job-Suche | Websites, die Stellenangebote und Arbeitgeberbewertungen, Ratschläge und Tipps für Vorstellungsgespräche oder damit verbundene Dienstleistungen für Arbeitgeber und potenzielle Kandidaten bereitstellen. |
| Rechtliches | Informationen, Analysen oder Beratung in Bezug auf das Gesetz, juristische Dienstleistungen, Anwaltskanzleien oder andere rechtliche Fragen |
| Militär | Informationen oder Kommentare zu militärischen Bereichen, Rekrutierung, aktuellen oder vergangenen Operationen oder damit zusammenhängenden Militaria. |
| Kraftfahrzeuge | Informationen in Bezug auf Bewertungen, Verkauf und Handel, Modifikationen, Teile und andere verwandte Themen zu Autos, Motorrädern, Booten, Lastwagen und Wohnmobilen. |

| URL-Kategorie | Beschreibung |
|---|---|
| Musik | Musikverkauf, -vertrieb oder -informationen. Umfasst Websites für Musikkünstler, Gruppen, Labels, Veranstaltungen, Songtexte und andere Informationen zum Musikgeschäft. Umfasst kein Musik-Streaming. |
| Nachrichten | Online-Veröffentlichungen, Newsticker-Dienste und andere Websites, die aktuelle Ereignisse, Wetter oder sonstige aktuelle Themen zusammenstellen. Umfasst Zeitungen, Radiosender, Zeitschriften und Podcasts. |
| Nicht aufgelöst | Zeigt an, dass die Website nicht in der lokalen URL-Filterdatenbank gefunden wurde und die Firewall keine Verbindung zur Cloud-Datenbank herstellen konnte, um die Kategorie zu überprüfen. Wenn eine Suche nach URL-Kategorien durchgeführt wird, überprüft die Firewall zuerst den Cache der Datenebene auf die URL. Wenn keine Übereinstimmung gefunden wird, überprüft sie den Cache der Management-Ebene. Wenn dort keine Übereinstimmung gefunden wird, fragt sie die URL-Datenbank in der Cloud ab. Beachten Sie bei der Entscheidung, welche Maßnahmen für den als nicht aufgelöst kategorisierten Datenverkehr ergriffen werden sollen, dass eine Blockade für Benutzer sehr lästig sein kann. |
| Nacktheit | Websites, die nackte oder halbnackte Darstellungen des menschlichen Körpers zeigen, unabhängig von Kontext oder Absicht, wie z. B. Kunstwerke. Umfasst Nudisten- oder FKK-Websites mit Bildern von Teilnehmern. |
| Online-Speicher und Datensicherung | Websites, die die Online-Speicherung von Dateien kostenlos und als Dienstleistung anbieten. |
| Peer-to-Peer | Websites, die Zugriff auf oder Clients für die Peer-zu-Peer-Freigabe von Torrents, Downloadprogrammen, Mediendateien oder anderen Softwareanwendungen bieten. Dies gilt in erster Linie für Websites, die BitTorrent-Download-Funktionen bieten. Umfasst keine Shareware- oder Freeware-Websites. |
| Persönliche Seiten und Blogs | Persönliche Websites und Blogs von Einzelpersonen oder Gruppen. Sollte zunächst anhand des Inhalts kategorisiert werden. Wenn jemand zum Beispiel einen Blog nur über Autos hat, dann sollte die Seite unter „Motor Vehicles“ (Kraftfahrzeuge) kategorisiert werden. Handelt es sich bei der Seite allerdings um einen reinen Blog, dann sollte sie unter „Personal Sites and Blogs“ (Persönliche Seiten und Blogs) eingestuft werden. |

| URL-Kategorie | Beschreibung |
|---|---|
| Philosophie und politische Interessenvertretung | Websites mit Informationen, Standpunkten oder Kampagnen zu philosophischen oder politischen Ansichten. |
| Private IP-Adressen | Diese Kategorie umfasst IP-Adressen, die in RFC 1918 „Address Allocation for Private Intranets“ definiert sind. Sie umfasst auch Domänen, die nicht beim öffentlichen DNS-System registriert sind (*.local und *.onion). |
| Fraglich | Websites mit geschmacklosem Humor und anstößigen Inhalten in Bezug auf bestimmte demografische Merkmale von Einzelpersonen oder Personengruppen. |
| Immobilien | Informationen über die Vermietung und den Verkauf von Immobilien und damit verbundene Tipps oder Informationen. Umfasst Websites für Immobilienmakler und -firmen, Vermietungsdienste, Anzeigen (und Anzeigensuchmaschinen) und Immobilienmodernisierungen. |
| Erholung und Hobbys | Informationen, Foren, Vereine, Gruppen und Publikationen zu Freizeit und Hobby. |
| Referenz und Recherche | Private, berufliche oder akademische Referenzportale, Materialien oder Dienstleistungen. Umfasst Online-Wörterbücher, Karten, Almanache, Bevölkerungsstatistik, Bibliotheken, Genealogie und wissenschaftliche Informationen. |
| Religion | Informationen zu verschiedenen Religionen, verwandten Aktivitäten oder Veranstaltungen. Umfasst Websites für religiöse Organisationen, offizielle Vertreter und Kultstätten. Umfasst Websites für Wahrsagerei. |
| Suchmaschinen | Websites, die eine Suchmaske für Schlüsselwörter, Phrasen oder andere Parameter bereitstellen, die Informationen, Websites, Bilder oder Dateien als Ergebnisse zurückgeben. |
| Sexuelle Aufklärung | Informationen zu Fortpflanzung, sexueller Entwicklung, Safer-Sex-Praktiken, sexuell übertragbaren Krankheiten, Empfängnisverhütung, Tipps für besseren Sex sowie alle zugehörigen Produkte oder zugehörigen Utensilien. Umfasst Websites verwandter Gruppen, Foren oder Organisationen. |
| Shareware und Freeware | Websites, die kostenlosen Zugriff oder Zugriff auf freiwilliger Spendenbasis auf Software, Bildschirmschoner, Symbole, Hintergrundbilder, Dienstprogramme, Klingeltöne, Designs oder Widgets bieten. Umfasst auch Open-Source-Projekte. |

| URL-Kategorie | Beschreibung |
|---|---|
| Shopping | Websites, die den Kauf von Waren und Dienstleistungen ermöglichen. Umfasst Online-Händler, Websites für Kaufhäuser, Einzelhandelsgeschäfte, Kataloge sowie Websites, die Preise zusammenstellen und verfolgen. Die hier aufgeführten Websites sollten Online-Händler sein, die eine Vielzahl von Artikeln verkaufen (oder deren Hauptzweck der Online-Verkauf ist). Eine Webseite eines Kosmetikunternehmens, das zufällig auch Online-Käufe ermöglicht, sollte unter „Cosmetics“ (Kosmetik) und nicht unter „Shopping“ kategorisiert werden. |
| Soziale Netzwerke | Benutzergemeinschaften und Websites, auf denen Benutzer miteinander interagieren, Nachrichten und Bilder posten oder anderweitig mit Personengruppen kommunizieren. Umfasst keine Blogs oder persönlichen Websites. |
| Gesellschaft | Themen, die die Allgemeinheit und eine Vielzahl von Menschen betreffen, wie Mode, Schönheit, philanthropische Gruppen, Gesellschaften oder Kinder. Enthält auch Websites für Kinder sowie für Restaurants. |
| Sport | Informationen über Sportveranstaltungen, Athleten, Trainer, Funktionäre, Mannschaften oder Organisationen, Sportergebnisse, Zeitpläne und damit verbundene Nachrichten sowie alle zugehörigen Utensilien. Umfasst Websites zu Fantasy-Sport und anderen virtuellen Sportligen. |
| Aktienberatung und Tools | Informationen über den Aktienmarkt, den Handel mit Aktien oder Optionen, die Verwaltung des Palo Alto Network Portfolios, Anlagestrategien, Kurse oder verwandte Nachrichten. |
| Streaming-Medien | Websites, die Audio- oder Videoinhalte kostenlos und/oder zum Kauf streamen. Umfasst Online-Radiosender und andere Streaming-Musikdienste. |
| Badeanzüge und intime Bekleidung | Websites, die Informationen oder Bilder zu Badeanzügen, Unterwäsche oder anderen freizügigen Kleidungsstücken enthalten. |
| Schulungen und Tools | Websites, die Online-Schulungen sowie zugehörige Materialien anbieten. Dies können Fahr- und Verkehrsschulen, Schulungen für den Arbeitsplatz usw. sein. |
| Übersetzung | Websites, die Übersetzungsdienste anbieten, sowohl von Benutzereingaben als auch ganzer Websites. Diese Websites können Benutzern auch ermöglichen, eine Filterung zu |

| URL-Kategorie | Beschreibung |
|---|---|
| | umgehen, da der Inhalt der Zielseite im Kontext der URL des Übersetzers präsentiert wird. |
| Reisen | Reisetipps und -angebote, Preisinformationen, Informationen zu Reisezielen, Tourismus und damit verbundene Dienstleistungen. Umfasst Websites für Hotels, lokale Sehenswürdigkeiten, Casinos, Fluggesellschaften, Kreuzfahrtlinien, Reisebüros, Fahrzeugvermietungen und Websites, die Buchungstools wie Preisalarme bereitstellen. Umfasst Websites für Sehenswürdigkeiten und Touristenattraktionen wie den Eiffelturm, den Grand Canyon etc. |
| Waffen | Verkauf, Rezensionen, Beschreibungen oder Anleitungen zu Waffen und deren Verwendung. |
| Web-Werbung | Anzeigen, Medien, Inhalte und Banner. |
| Webhosting | Kostenlose oder kostenpflichtige Hosting-Dienste für Webseiten, einschließlich Informationen zu Webentwicklung, Veröffentlichung, Werbung und anderer Methoden zur Steigerung des Datenverkehrs. |
| Webbasierte E-Mail | Jede Website, die Zugriff auf einen E-Mail-Posteingang und die Möglichkeit bietet, E-Mails zu senden und zu empfangen. |

## Dateiblockade in Cloud NGFW für AWS konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Bei der Dateiblockade können Sie bestimmte Dateitypen angeben, die Sie blockieren oder überwachen möchten. Für den Großteil des Datenverkehrs (einschließlich des Datenverkehrs in Ihrem internen Netzwerk) gilt, dass Sie Dateien blockieren sollten, von denen bekannt ist, dass sie Bedrohungen enthalten, oder bei denen es keinen wirklichen Anwendungsfall für Uploads und Downloads gibt. Dazu gehören Batchdateien, DLLs, Java-Klassendateien, Hilfedateien, Windows-Verknüpfungen (.lnk) und BitTorrent-Dateien.

Cloud NGFW kann die folgenden Aktionen für Dateien ausführen, die sich durch Ihr Netzwerk bewegen.

- **Alert (Benachrichtigen)** – Wenn der angegebene Dateityp erkannt wird, wird ein Protokoll im Datenfilterungsprotokoll generiert.
- **Block (Blockieren)** – Wenn der angegebene Dateityp erkannt wird, wird die Datei blockiert und dem Benutzer eine entsprechende (anpassbare) Seite angezeigt. Im Datenfilterungsprotokoll wird auch ein Protokoll generiert.
- **Continue (Weiter)** – Wenn der angegebene Dateityp erkannt wird, wird dem Benutzer eine Antwortseite angezeigt. Der Benutzer kann sich durch die Seite klicken, um die Datei herunterzuladen. Im Datenfilterungsprotokoll wird auch ein Protokoll generiert. Da diese Art der Weiterleitungsaktion eine Benutzerinteraktion erfordert, ist sie nur für Webdatenverkehr anwendbar.

Darüber hinaus können Sie Dateitypen basierend auf der Bewegungsrichtung zulassen oder blockieren: Herunterladen, Hochladen oder Hochladen und Herunterladen.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den die Dateiblockade konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Security Profiles (Sicherheitsprofile)** > **Malware and File-based Threat Protection (Schutz vor Malware und dateibasierten Bedrohungen)** > **File Blocking (Dateiblockade)** > **Edit (Bearbeiten)** aus.

**STEP 3 |** Wählen Sie den Dateityp aus der angezeigten Liste aus.

**STEP 4 |** Legen Sie in den Dropdown-Listen mit **Action (Aktion)** die Aktion und mit **Direction of traffic (Richtung des Datenverkehrs)** die Richtung des Datenverkehrs für die ausgewählten Dateitypen fest.

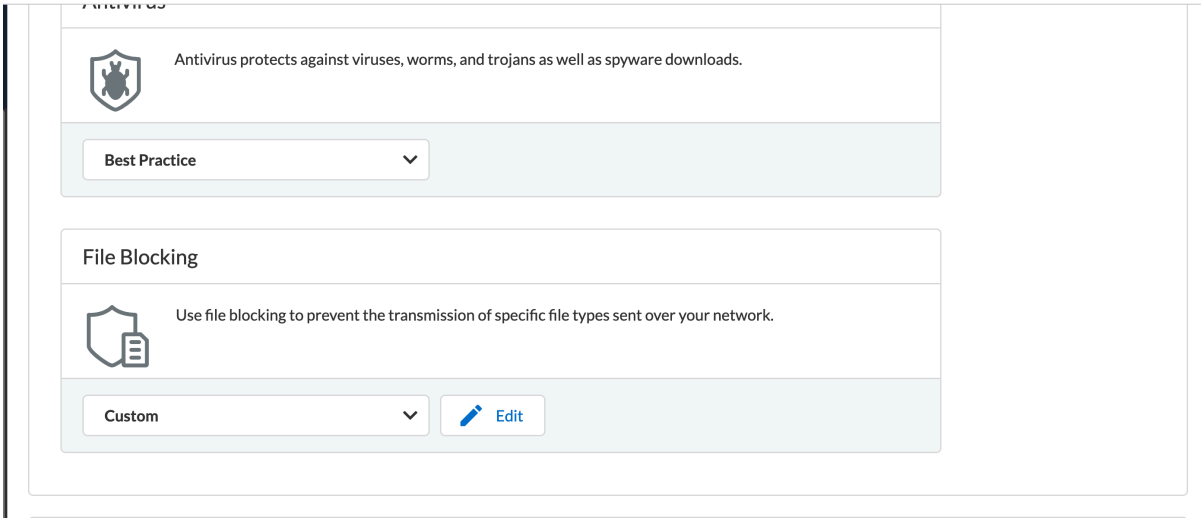
**STEP 5 |** Klicken Sie auf **Save (Speichern)**.

### Ändern des Dateiblockade-Profils

Standardmäßig ist das Dateiblockade-Profil auf **Best Practice** gesetzt. So ändern Sie das Dateiblockade-Profil:

**STEP 1 |** Navigieren Sie im Bildschirm **Malware and File-based Threat Protection (Schutz vor Malware und dateibasierten Bedrohungen)** zu **File Blocking (Dateiblockade)**.

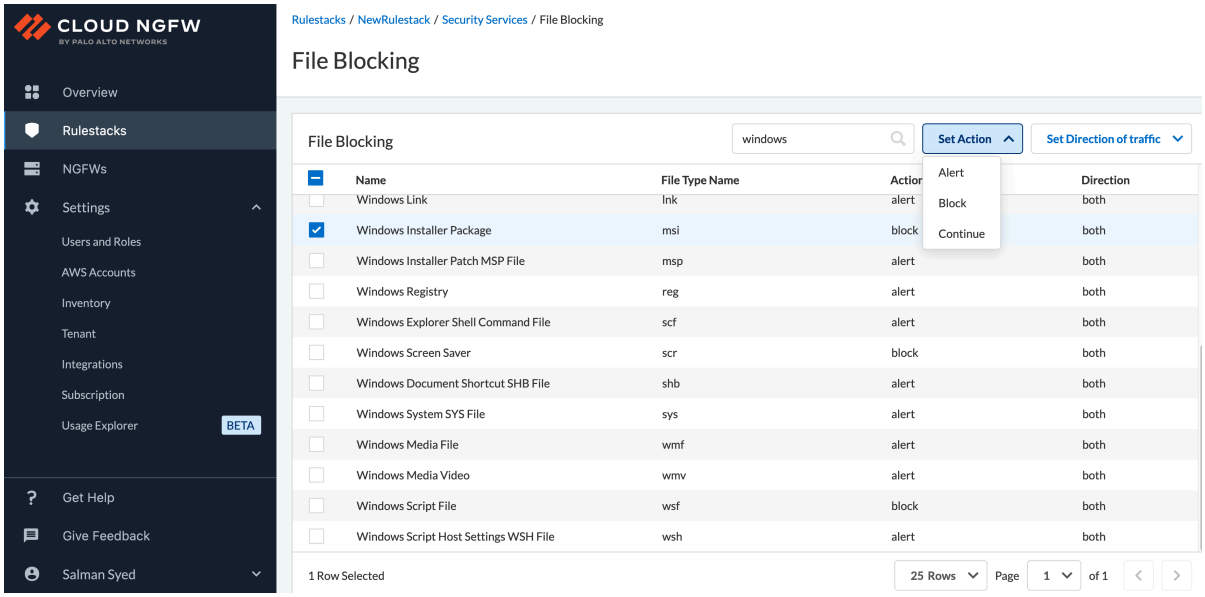
**STEP 2 |** Wählen Sie aus der Dropdown-Liste die Option **Custom (Benutzerdefiniert)** aus.



**STEP 3 |** Öffnen Sie die Cloud NGFW-Konsole. Navigieren Sie zu **Rulestacks > Rulestack name > Security Services > File Blocking (Regelstapel > Name des Regelstapels > Sicherheitsdienste > Dateiblockade)**.

**STEP 4 |** Legen Sie in der Dropdown-Liste **Set Action (Aktion festlegen)** die Aktion auf **Alert (Benachrichtigen)** oder **Continue (Weiter)** fest.




## Ausgehende Entschlüsselung in Cloud NGFW für AWS einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Bei der ausgehenden Entschlüsselung verhält sich Cloud NGFW wie ein SSL-Weiterleitungsproxy und verwendet die zugehörigen Zertifikate, um als vertrauenswürdiger Dritter (Meddler-in-the-Middle (MitM)) für die Client-Server-Sitzung zu fungieren. Cloud NGFW hält die Header und Nutzlast der Datenverkehrspakete aber intakt und bietet Ihren Zielen eine vollständige Sichtbarkeit der Identität der Quelle.

Bei der ausgehenden Entschlüsselung werden zwei Zertifikatsobjekte verwendet: Trust und Untrust. Die NGFW präsentiert das Trust-Zertifikat den Clients während der SSL-Entschlüsselung, wenn die Clients eine Verbindung zu einem Server herstellen, der über ein von einer Certificate Authority (Zertifizierungsstelle, CA) signiertes Zertifikat verfügt. Alternativ. Die NGFW präsentiert das Untrust-Zertifikat den Clients, die eine Verbindung zu einem Server herstellen, der über ein Zertifikat verfügt, das von einer CA signiert wurde, der die NGFW nicht vertraut.

Sie können die NGFW-Ressource so konfigurieren, dass der SSL-Datenverkehr, der Ihre VPC oder Ihr Subnetz verlässt, entschlüsselt wird. Anschließend können Sie App-ID- und Sicherheitseinstellungen für den Klartext-Datenverkehr durchsetzen, einschließlich Profilen für Antivirus, Sicherheitslücken, Anti-Spyware, URL-Filter und Dateiblockaden. Nach dem Entschlüsseln und Überprüfen des Datenverkehrs verschlüsselt die Firewall den Klartext-Datenverkehr beim Verlassen der Firewall erneut, um Datenschutz und Sicherheit zu gewährleisten.

Dieses Verfahren definiert nur die Zertifikate, die die Firewall für die ausgehende TLS-Entschlüsselung verwendet. Aktivieren Sie die ausgehende TLS-Entschlüsselung während der Regelerstellung.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, der auf das Zertifikat angewendet werden soll.

**STEP 2 |** Wählen Sie **Security Services (Sicherheitsdienste)** > **Outbound Decryption (Ausgehende Entschlüsselung)** aus.

Der CA-Wert unter „Basic Constraints“ (Grundlegende Einschränkungen) im CA-Zertifikat muss auf **true** gesetzt werden.

**STEP 3 |** Wählen Sie ein Zertifikat aus.

- Wählen Sie ein **Untrust Certificate (Untrust-Zertifikat)** aus.
- Wählen Sie ein **Trust-Zertifikat** aus.

Erstellen Sie ein Zertifikat, *falls Sie dies noch nicht getan haben.*

Das Zertifikat und der private Schlüssel werden im AWS Secrets Manager (ASM) gespeichert und die Workload verwendet diese Informationen, um den Datenverkehr zu entschlüsseln.

Das Zertifikat muss ein CA-Zertifikat sein. Der CA-Wert in den „Basic Constraints“ (Grundlegende Einschränkungen) muss auf TRUE gesetzt werden. Nachfolgend sehen Sie ein Beispiel für ein privates CA-Zertifikat.

```
Zertifikat: Daten: Version: 3 (0x2) Seriennummer: 4121 (0x1019)
 Signature Algorithm: sha256WithRSAEncryption Issuer: C=US,
 ST=Washington, L=Seattle, O=Example Company Root CA, OU=Corp,
 CN=www.example.com/emailAddress=corp@www.example.com Validity
 Not Before: Feb 26 20:27:56 2018 GMT Not After : Feb 24 20:27:56
 2028 GMT Subject: C=US, ST=WA, L=Seattle, O=Examples Company
 Subordinate CA, OU=Corporate Office, CN=www.example.com Subject
 Public Key Info: Public Key Algorithm: rsaEncryption Public-
Key: (2048 bit) Modulus: 00:c0: ... a3:4a:51 Exponent: 65537
 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier:
 F8:84:EE:37:21:F2:5E:0B:6C:40:C2:9D:C6:FE:7E:49:53:67:34:D9 X509v3
 Authority Key Identifier:
 keyid:0D:CE:76:F2:E3:3B:93:2D:36:05:41:41:16:36:C8:82:BC:CB:F8:A0
 X509v3 Basic Constraints: critical CA:TRUE X509v3 Key Usage:
 critical Digital Signature, CRL Sign Signature Algorithm:
 sha256WithRSAEncryption 6:bb:94: ... 80:d8
```

Wenn es sich bei dem Zertifikat um eine Kette handelt, verwenden Sie das Blattzertifikat und den Schlüssel. Importieren Sie das CA-Stammzertifikat und das CA-Zwischenzertifikat in den

Client-Truststore. Das folgende Beispiel veranschaulicht, wie ein CA-Stammzertifikat und ein CA-Zwischenzertifikat in den Truststore im Ubuntu-Betriebssystem importiert werden können.

```
$ sudo apt-get install -y ca-certificates $ sudo cp root-ca.crt /
usr/local/share/ca-certificates $ sudo cp intermediate-ca.crt /usr/
local/share/ca-certificates $ sudo update-ca-certificates
```

Wenn Sie zum Entschlüsseln des Datenverkehrs ein End-Entity-Zertifikat verwenden, muss nur das End-Entity-Zertifikat mit öffentlichem und privatem Schlüssel im ASM gespeichert werden.

*PKCS8 ist das unterstützte Zertifikatformat.*

*Die ausgehende Entschlüsselung mit dem Zertifikatsobjekt „Trust“ (Vertrauen) unterstützt keine selbstsignierten Zertifikate.*

**STEP 4 |** Klicken Sie auf **Save (Speichern)**.

## Eingehende Entschlüsselung in Cloud NGFW für AWS einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW verwendet eingehende SSL-Entschlüsselung, um eingehenden SSL/TLS-Datenverkehr von einem Client zu einem Zielnetzwerkserver (jeder Server, für den Sie das Zertifikat haben und es in die Firewall importieren können) zu untersuchen und zu entschlüsseln und verdächtige Sitzungen zu blockieren. Die Firewall fungiert als Proxy zwischen dem externen Client und dem internen Server und generiert für jede sichere Sitzung einen neuen Sitzungsschlüssel. Die Firewall erstellt eine sichere Sitzung zwischen dem Client und der Firewall und eine weitere sichere Sitzung zwischen der Firewall und dem Server, um den Datenverkehr zu entschlüsseln und zu untersuchen. Cloud NGFW hält die Header und die Nutzlast der Datenverkehrspakete aber intakt und bietet den Anwendungen in den VPCs eine vollständige Sichtbarkeit der Identität der Quelle.

Ihr Zertifikat und Ihr Sitzungsschlüssel werden im AWS Secrets Manager gespeichert, um eine eingehende SSL-Inspektion durchzuführen. Die Firewall überprüft, ob das vom Zielserver während des SSL/TLS-Handshakes gesendete Zertifikat mit einem Zertifikat in Ihrer Entschlüsselungsrichtlinienregel übereinstimmt. Bei Übereinstimmung leitet die Firewall das Zertifikat des Servers an den Client weiter, der den Serverzugriff anfordert, und stellt eine sichere Verbindung her.

**STEP 1 |** Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, der auf das Zertifikat angewendet werden soll.

**STEP 2 |** Wählen Sie **Rules (Regeln)** und erstellen Sie dann mit **Create (Erstellen)** eine neue **Sicherheitsregel (Security Rule)** für die Entschlüsselung.

**STEP 3 |** Geben Sie unter **General (Allgemein)** die folgenden Details an.

- **Name** – Name der Regel.
- **Description (Beschreibung)** – Eine Beschreibung für die Regel.
- **Rule Priority (Regelpriorität)** – Eine eindeutige Priorität für die Regel.
- **Enabled (Aktiviert)** – Aktivieren Sie das Feld, um den Regelstapel mit der Regel zu verknüpfen. Dieses Feld ist standardmäßig aktiviert.

**STEP 4 |** Definieren Sie Übereinstimmungskriterien für die Felder mit den IP-Adressen für **Source (Quelle)** und **Destination (Ziel)**.

**STEP 5 |** Konfigurieren Sie unter **Granular Controls (Granulare Steuerelemente)** granulare Steuerelemente.

- Geben Sie die **Anwendungen (App-ID)** an, die die Regel zulassen oder blockieren soll.

  *Sie können TLS-Entschlüsselungsregeln über **Anwendungen (App-ID)** – **Any (Beliebig)** oder **SSL** – nur **Match (Übereinstimmung)** erstellen.*

- Geben Sie unter **URL Category (URL-Kategorie)** eine URL-Kategorie als Übereinstimmungskriterium für die Regel an.
- Geben Sie unter **Protocol and Ports (Protokolle und Ports)** die Protokolle und Ports an, die von der Regel zugelassen oder blockiert werden sollen.

**STEP 6 |** Geben Sie unter **Action (Aktion)** die Aktion an, die die Firewall ausführen soll, wenn der Datenverkehr mit einer der von Ihnen erstellten Regeln übereinstimmt.

- **Allow (Zulassen)** – Datenverkehr zulassen.
- **Deny (Ablehnen)** – Blockiert Datenverkehr und erzwingt die standardmäßige *Ablehnen-Aktion*, die für die abzulehnende Anwendung definiert ist.
- **Reset Server (Server zurücksetzen)** – Sendet die TCP-Zurücksetzung an das serverseitige Gerät.
- **Reset Both (Beide zurücksetzen)** – Sendet eine TCP-Zurücksetzung an client- und serverseitige Geräte.

**STEP 7 |** Wählen Sie unter **TLS Decryption (TLS-Entschlüsselung)** die Option **Inbound (Eingehend)** und dann unter **Inbound Inspection Certificate (Eingehendes Inspektionszertifikat)** ein eingehendes Inspektionszertifikat aus.

Erstellen Sie ein Zertifikat, *falls Sie dies noch nicht getan haben. Der Amazon-Ressourcenname (ARN) des Geheimnisses muss beim Erstellen des Zertifikatobjekts im Zertifikat-ARN verwendet werden.*

Zertifikat und privater Schlüssel werden im AWS Secrets Manager (ASM) gespeichert und Application Load Balancer (ALB) verwendet diese Informationen, um den Datenverkehr zu entschlüsseln. Bei dem

Zertifikat muss es sich nicht um ein CA-Zertifikat handeln. Wenn es sich bei dem Zertifikat um eine Kette handelt, verwenden Sie das Blattzertifikat und den Schlüssel.

*PKCS8 ist das unterstützte Zertifikatsformat.*

*Die eingehende Entschlüsselung unterstützt keine selbstsignierten Zertifikate.*

*Das Entschlüsselungsprofil für die TLS-Entschlüsselung ist auf „Best Practice Security Policy“ (Best-Practices-Sicherheitsleitlinie) eingestellt. Weitere Informationen finden Sie unter* Datenverkehr für vollständige Sichtbarkeit und Bedrohungsprüfung entschlüsseln.

**STEP 8 |** Klicken Sie auf **Enabled (Aktiviert)**, um die Protokollierung zu aktivieren.

**STEP 9 |** Klicken Sie auf **Save (Speichern)**.

**STEP 10 |** Klicken Sie auf **Config Actions (Konfigurationsaktionen)** > **Deploy Configuration (Konfiguration bereitstellen)** > **Commit (Übergeben)**, um die Regel in der laufenden Konfiguration der Firewall zu speichern.

# Regelnutzung in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Verwenden Sie Panorama, um Regeln für Ihre Cloud NGFW-Ressource zu verwalten, sodass Sie die Regelnutzung für Vorgänge und Fehlerbehebungsaufgaben verfolgen und überwachen können. In der Panorama-Konsole können Sie die Regelnutzung in der Cloud-Gerätegruppe anzeigen, um festzustellen, ob alle, einige oder keine der Cloud NGFW-Ressourcen Übereinstimmungen hinsichtlich des Datenverkehrs aufweisen.

In Panorama können Sie die Details zur Regelnutzung für verwaltete Firewalls anzeigen, für die die Anzahl der Richtlinienregeltreffer aktiviert ist (Standard) und für die Sie Richtlinienregeln mithilfe von Gerätegruppen definiert und übertragen haben. Panorama kann keine Details zur Regelnutzung für Richtlinienregeln abrufen, die lokal in der Firewall konfiguriert sind, daher müssen Sie sich bei der Firewall anmelden, um Informationen zur Regelnutzung für lokal konfigurierte Regeln anzuzeigen. Weitere Informationen finden Sie unter Nutzung von Richtlinienregeln überwachen.

## Regelnutzung – Regeltreffer und Richtlinienoptimierer

**Systemanforderungen**

Im Folgenden sind die Mindestsystemanforderungen für die Überwachung der Nutzung Ihrer Sicherheitsrichtlinienregeln aufgeführt:

- Panorama (PAN-OS) Version 10.2.8 und höher
- AWS-Plug-in Version 5.2.0 und höher
- Cloud Services-Plug-in Version 5.0.0 und höher
- Cloud Connector-Plug-in Version 2.0.1 und höher

### Regeltrefferanzahl für eine Cloud-Gerätegruppe anzeigen

Nachdem Sie in der Panorama-Konsole eine Cloud-Gerätegruppe einer Cloud NGFW-Ressource zugeordnet und Richtlinien für die Cloud-Gerätegruppe konfiguriert haben, führen Sie die folgenden Schritte aus, um die Anzahl der Regeltreffer für eine Cloud-Gerätegruppe in Panorama anzuzeigen:

*Die NGFW-Firewall-Ressourcen melden Ihre Regeltrefferdaten alle 2 Minuten an den Cloud NGFW-Dienst, woraufhin der Cloud NGFW-Dienst bei der Abfrage von Daten von Firewall-Ressourcen eine Latenz von maximal 2 Minuten aufweist. Daraus ergibt sich eine maximale Latenz von 4 Minuten bei der Anzeige der Daten zur Regeltrefferanzahl in der Panorama-Konsole.*

**STEP 1 |** Wählen Sie **Policies (Richtlinien)** aus.

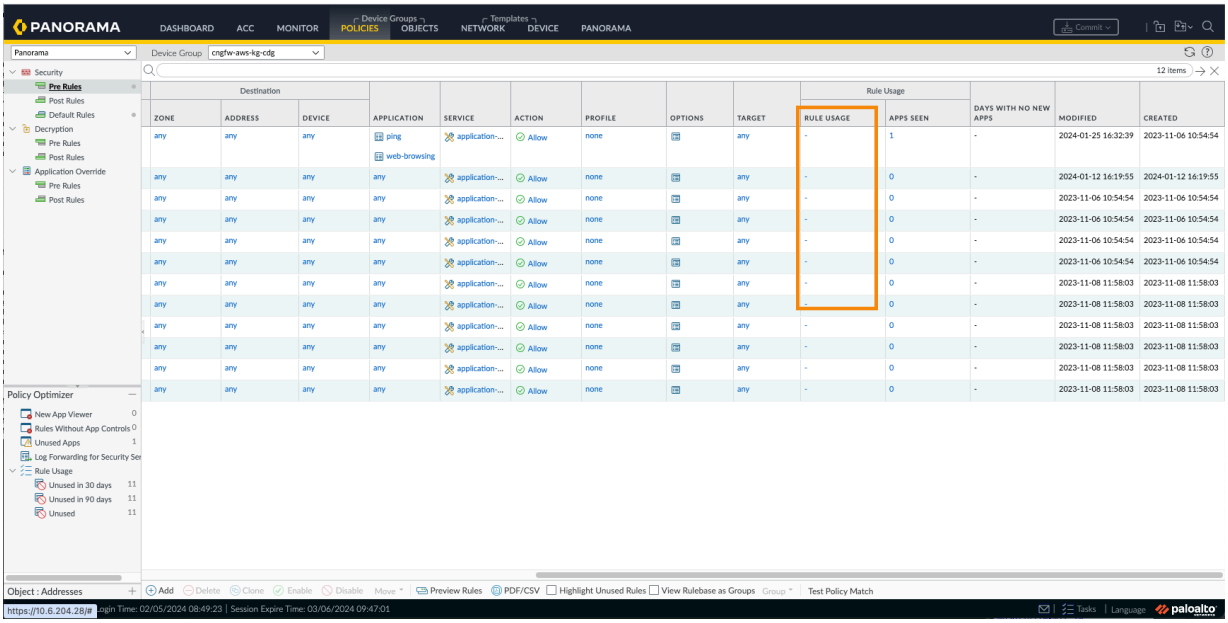
**STEP 2 |** Wählen Sie im Abschnitt **Device Group (Gerätegruppe)** mithilfe der Dropdown-Liste die Cloud-Gerätegruppe aus.

**STEP 3 |** Wählen Sie eine Regel aus und klicken Sie auf **Rule Usage (Regelnutzung)**.

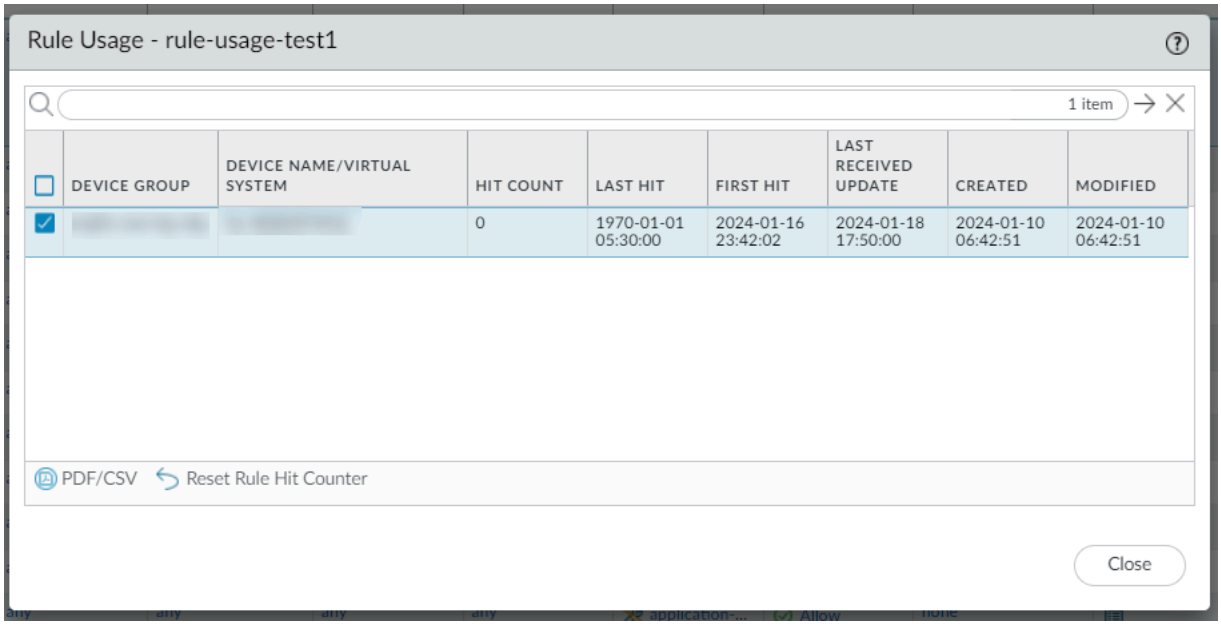
Sie können den Regelnutzungsstatus Ihrer Vor-, Nach- und Standardregeln der Richtlinientypen „Security“ (Sicherheit), „Decryption“ (Entschlüsselung) und „Application-override“ (Außerkraftsetzung von Anwendungen) überwachen.



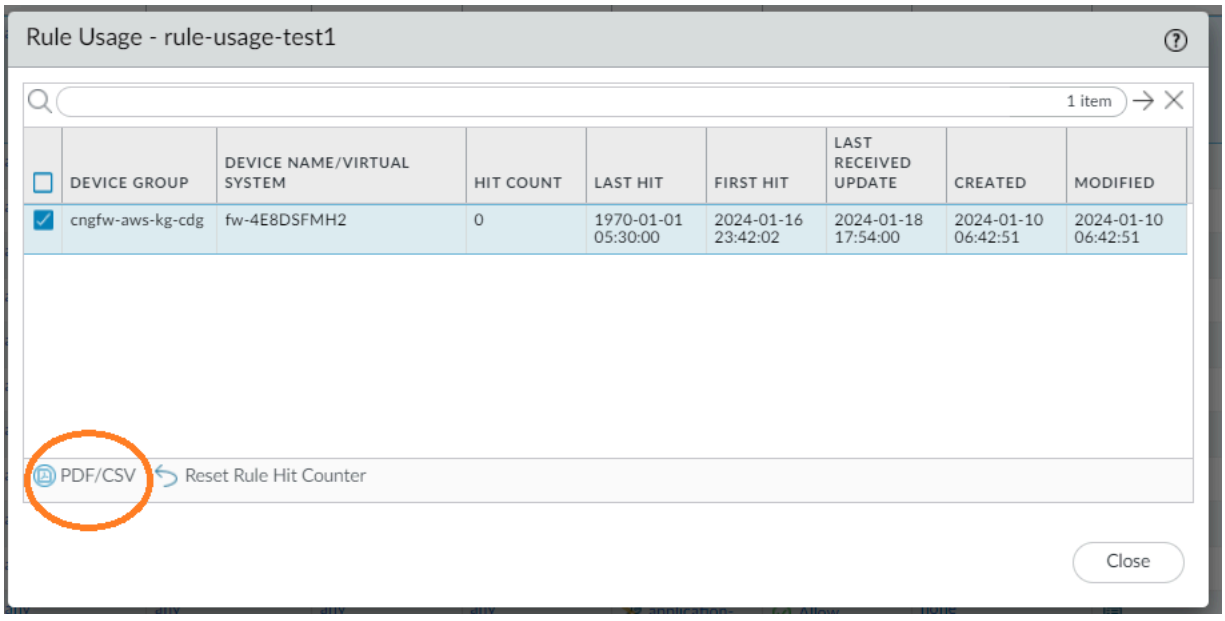
In der Spalte **Hit Count (Trefferanzahl)** wird nun die Anzahl der Treffer angezeigt.




*In der Panorama-Konsole wird die Regeltrefferanzahl standardmäßig in 4-Minuten-Intervallen aktualisiert.*

Klicken Sie auf **Reset Rule Hit Counter (Regeltrefferzähler zurücksetzen)**, um die Trefferanzahl der ausgewählten Regel zu aktualisieren.

Klicken Sie auf **PDF/CSV**, um die Details zur Nutzung einer ausgewählten Regel als CSV- oder PDF-Datei zu exportieren.



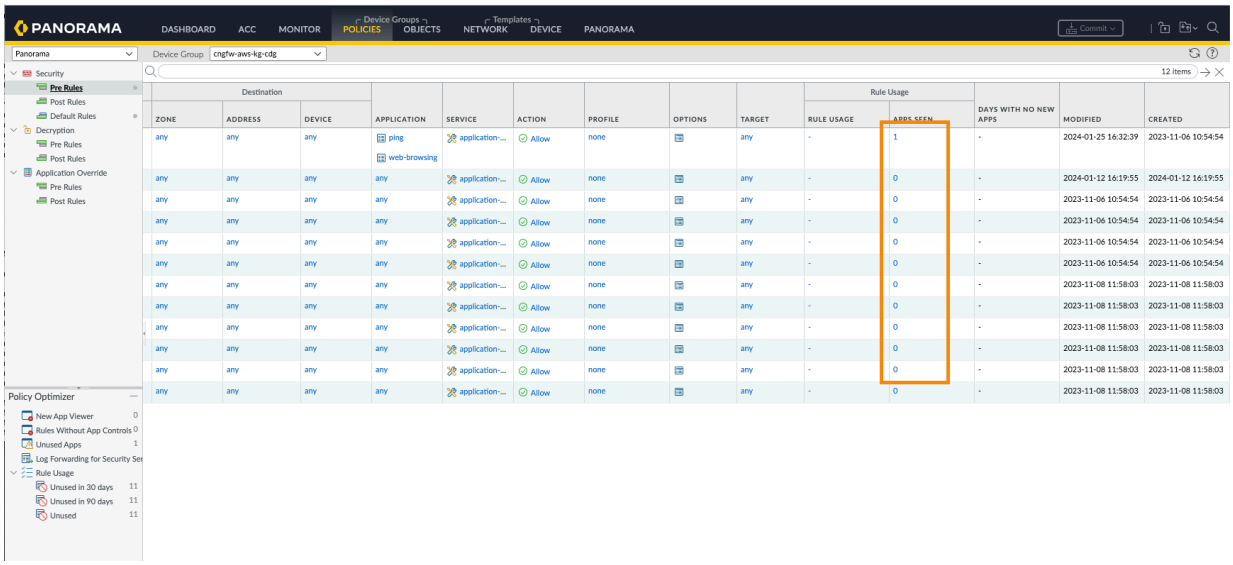
## Regelnutzung – Erkannte Apps und Richtlinienoptimierer

Sie können alle Ihre Anwendungen anzeigen, die in der Firewall erkannt und zugelassen wurden und mit Ihrer Sicherheitsrichtlinienregel übereinstimmen. Die Zahl in der Spalte **Apps Seen (Erkannte Apps)** gibt an, wie viele Anwendungen für die Regel erkannt wurden.

- Wechseln Sie in der Panorama-Konsole zur Registerkarte **Policies (Richtlinien)**.
- Wählen Sie im Abschnitt **Device Group (Gerätegruppe)** mithilfe der Dropdown-Liste die Cloud-Gerätegruppe aus.

- Wählen Sie eine Regel aus und klicken Sie auf **Apps Seen (Erkannte Apps)**.




Sie können jetzt die Anwendungen sehen, die in Ihrer Sicherheitsrichtlinienregel konfiguriert und angezeigt werden.

Weitere Informationen zu „Apps on Rule“ (Der Regel entsprechende Apps), „Apps seen“ (Erkannte Apps) und „App seen actions“ (Aktionen für erkannte Apps) finden Sie unter Anwendungen und Nutzung.

Im Abschnitt **Policy Optimizer (Richtlinienoptimierer)** können Sie auch die Anzahl der Regeltreffer für alle Ihre konfigurierten Cloud-Gerätegruppen in Panorama anzeigen. Policy Optimizer bietet einen einfachen Workflow zum Migrieren Ihrer alten Sicherheitsrichtlinien-Regelbasis in eine auf App-IDs basierenden Regelbasis, die Ihre Sicherheit verbessert, indem sie die Angriffsfläche reduziert und Einblick in Anwendungen erhält, damit Sie sie sicher aktivieren können. Weitere Informationen finden Sie unter Sicherheitsrichtlinienregeln optimieren und Anwendungen und Nutzung.

# Panorama-Richtlinienverwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW ist die branchenweit einzige NGFW, die auf maschinellem Lernen (ML) basiert und als cloudnativer Dienst in AWS bereitgestellt wird. Mit Cloud NGFW können Sie mehr Apps sicher mit Cloud-Geschwindigkeit und im Cloud-Maßstab ausführen – mit echter cloudnativer Erfahrung. Sie erleben das Beste aus beiden Welten mit nativ integrierter Netzwerksicherheit, die als Dienst in AWS bereitgestellt wird.

Auf dieser Seite erfahren Sie, wie Sie Cloud NGFW für AWS mit Palo Alto Networks Panorama konfigurieren und integrieren.

Mit einer Panorama-Appliance können Sie einen gemeinsamen Satz von Sicherheitsregeln zentral auf Cloud NGFW-Ressourcen neben Ihren physischen und virtuellen Firewall-Appliances verwalten. Sie können außerdem alle Aspekte der Konfiguration gemeinsam genutzter Objekte und Profile verwalten, diese Regeln per Push übertragen und Berichte zu Verkehrsmustern oder Sicherheitsvorfällen Ihrer Cloud NGFW-Ressourcen erstellen – und das alles über eine einzige Panorama-Konsole.

Panorama bietet einen einzigen Standort für die zentrale Richtlinien- und Firewallverwaltung von Hardwarefirewalls, virtuellen Firewalls und Cloud-Firewalls. Dies erhöht die Betriebseffizienz bei der Verwaltung und Wartung eines hybriden Firewallnetzwerks.

**Wie funktioniert die Integration?**

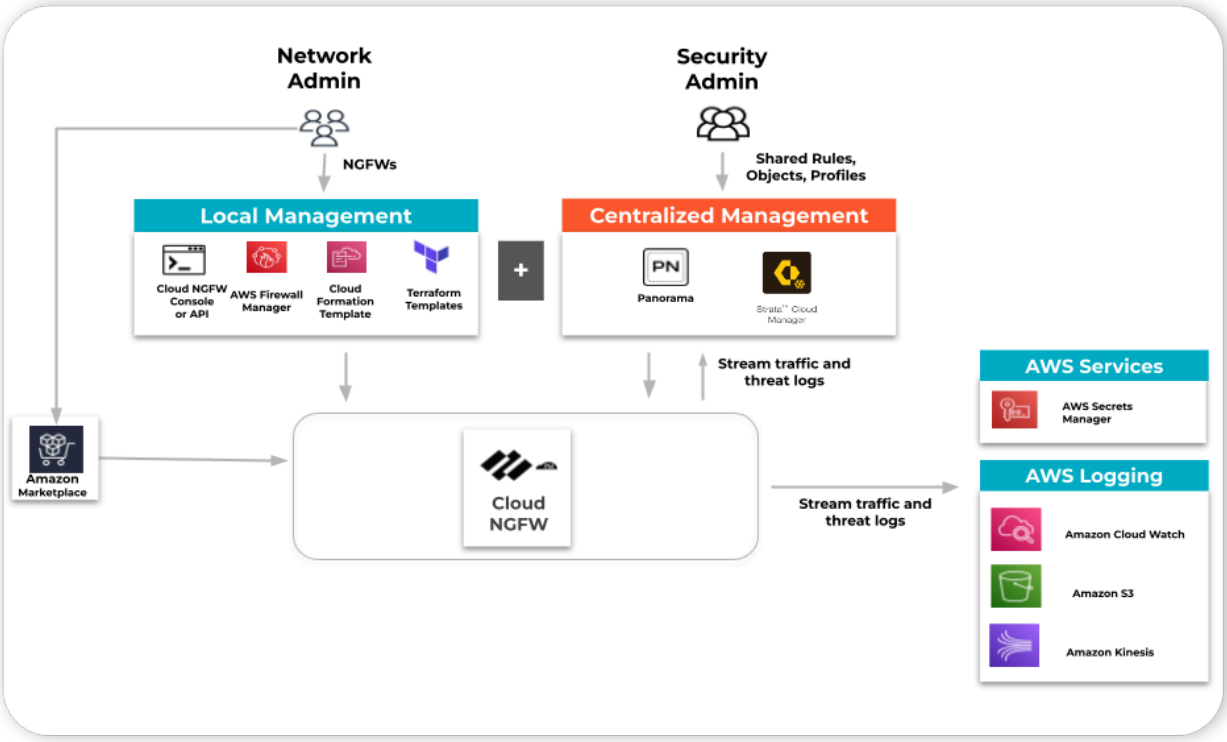
Sie werden weiterhin den Cloud NGFW-Dienst über AWS Marketplace abonnieren und einen Mandanten erstellen. Anschließend können Sie Ihren Cloud NGFW-Mandanten mit Ihren Panorama-Appliances verknüpfen. Sie können dann einen gemeinsamen Satz von Sicherheitsregeln zentral auf Cloud NGFW-Ressourcen verwalten, die Sie auf diesem Mandanten neben Ihren physischen und virtuellen Firewall-Appliances erstellen, und Sie können Protokollierung, Berichterstellung und Protokollanalyse verwenden – alles von einer Panorama-Konsole aus.

Ihre Panorama-Appliances können sich in jeder Cloud-Region oder in einer lokalen Umgebung befinden. Panorama verwendet das AWS-Plug-in, um Richtlinien und Objekte per Push an die NGFW-Ressourcen in AWS-Regionen zu übertragen.

Durch die Integration zwischen Cloud NGFW und Ihren Panorama-Appliances können Ihre Cloud NGFW-Ressourcen optional Protokolle an ein Konto des Strata-Protokollierungsdienstes streamen. Anschließend können Sie die Weboberfläche des Strata-Protokollierungsdienstes, den Panorama-Protokoll-Viewer oder das Application Command Center (ACC) verwenden, um die Protokolle des Strata-Protokollierungsdienstes anzuzeigen und zu analysieren. Panorama verwendet das Cloud Services-Plug-in, um die Protokolle Ihres Kontos beim Strata-Protokollierungsdienst abzufragen.

Sie können die Cloud NGFW-Ressourcen auch so konfigurieren, dass Protokolle an AWS-Protokollziele wie S3, CloudWatch und Kinesis-Streams gestreamt werden.




*Sie können mehrere Panorama- und Strata-Protokollierungsdienst-Paare mit dem Cloud NGFW-Mandanten verknüpfen.*

**Integrationskomponenten**

Die folgende Abbildung veranschaulicht, wie Cloud NGFW in Panorama integriert wird. Jede dieser Komponenten ist im folgenden Abschnitt beschrieben.

**Palo Alto Networks Policy Management** ist die primäre und obligatorische Komponente der Lösung. Sie müssen eine **Panorama**-Appliance verwenden, um Richtlinienregeln für Ihre Cloud NGFW-Ressourcen zu erstellen und zu verwalten. Die Richtlinienverwaltungskomponente hilft auch dabei, Ihre erstellten Richtlinienregeln und Objekte mit mehreren Cloud NGFW-Ressourcen in verschiedenen AWS-Regionen zu verknüpfen.

**Palo Alto Networks Log Management** ist keine obligatorische Komponente für diese Lösung. Sie können den Strata-Protokollierungsdienst verwenden, wenn Sie Protokolle lieber in der Panorama-Konsole anzeigen möchten. Alternativ können Sie Application Command Center (ACC) in der Panorama-Konsole verwenden, um Einblick in den Cloud NGFW-Datenverkehr zu erhalten oder Berichte in Panorama zu erstellen. Zu diesem Zweck müssen Sie Ihre Panorama-Instanz mithilfe des Cloud Services-Plug-ins in Panorama mit einem Cortex Data Lake-Konto verknüpfen. Sie können Cloud NGFW-Ressourcen so konfigurieren, dass Protokolle gleichzeitig an den Strata-Protokollierungsdienst und an eines der AWS-Protokollziele (S3, CloudWatch oder Kinesis-Stream) gesendet werden.

*1) Verknüpfen Sie Ihre Panorama-Instanz mit dem Strata-Protokollierungsdienst, bevor Sie sie mit Ihrem Cloud NGFW-Mandanten verknüpfen. 2) Wenn Sie mehrere Panorama-Instanzen mit demselben Cloud NGFW-Mandanten verwenden, stellen Sie sicher, dass jede Panorama-Instanz mit einzelnen Strata-Protokollierungsdienst-Instanzen verknüpft ist.*

Das **Panorama AWS-Plug-in** ist eine obligatorische Komponente dieser Lösung. Mit dem Panorama AWS-Plug-in können Sie Cloud-Gerätegruppen und Cloud-Vorlagenstacks erstellen, mit denen Sie Richtlinienregeln und Objekte auf NGFW-Ressourcen der mit Panorama verknüpften Cloud NGFW-Mandanten verwalten können. Das Panorama AWS-Plug-in verwendet intern das Cloud Connector-Plug-in, um mit den Cloud NGFW-Ressourcen zu kommunizieren.

**Cloud-Gerätegruppen (Cloud Device Groups)** sind Panorama-Gerätegruppen für spezielle Zwecke, mit denen Sie Regeln und Objekte für Cloud NGFW-Ressourcen erstellen können. Sie können Cloud-Gerätegruppen mithilfe der Benutzeroberfläche/APIs des Panorama AWS-Plug-ins erstellen, indem Sie den Cloud NGFW-Mandanten und die AWS-Regionsinformationen angeben. Eine Cloud-Gerätegruppe manifestiert sich als globaler Regelstapel in diesem Mandanten oder dieser Region.

- Mit dem Panorama AWS-Plug-in können Sie mehrere Cloud-Gerätegruppen erstellen.
- Sie können die Gerätegruppenseite der nativen Panorama-Weboberfläche verwenden, um Richtlinien- und Objektkonfigurationen in Cloud-Gerätegruppen und die mit diesen verknüpften Objekte und Sicherheitsprofile zu verwalten.
- Sie können auch Ihre vorhandenen freigegebenen Objekte und Profile in Ihren vorhandenen Panorama-Gerätegruppen nutzen, indem Sie in den Sicherheitsregeln, die Sie in Ihren Cloud-Gerätegruppen erstellen, auf sie verweisen.
- Alternativ können Sie diese Cloud-Gerätegruppen zur Gerätegruppenhierarchie hinzufügen, die Sie in Ihrer Panorama-Instanz verwalten, um die Gerätegruppenregeln und -objekte zu vererben. Allerdings können Cloud NGFWs derzeit nicht alle von der Cloud-Gerätegruppe übernommenen Regeln durchsetzen, etwa solche, die Sicherheitszonen oder Benutzer verwenden.
- Sie können dieselbe Cloud-Gerätegruppe mit mehreren Regionen des Cloud NGFW-Mandanten verknüpfen. Diese Cloud-Gerätegruppe wird als dedizierter globaler Regelstapel in jeder AWS-Region Ihres Cloud NGFW-Mandanten manifestiert.

**Cloud-Vorlagenstacks (Cloud Template Stacks, Cloud TS)** sind Panorama-Vorlagenstacks für spezielle Zwecke, die es Ihren Sicherheitsregeln in Cloud-Gerätegruppen ermöglichen, auf Objekteinstellungen zu verweisen, die Sie in Panorama mithilfe von Vorlagen verwalten können. Beim Erstellen einer Cloud-Gerätegruppe können Sie mit dem Panorama AWS-Plug-in einen Cloud-Vorlagenstack erstellen oder angeben. Das Plug-in erstellt diesen Cloud-Vorlagenstack automatisch und fügt ihn der Cloud-Gerätegruppe als Referenzvorlagenstack hinzu. Von nun an können Sie die Seite „Template Stack“ (Vorlagenstack) der nativen Panorama-Weboberfläche verwenden, um Ihre Vorlagen zu konfigurieren und sie diesen Cloud-Vorlagenstacks hinzuzufügen.

- Der Cloud NGFW-Dienst von Palo Alto Networks verwaltet die meisten Geräte- und Netzwerkkonfigurationen in Ihren Cloud NGFW-Ressourcen. Daher ignoriert Cloud NGFW Infrastruktureinstellungen wie Schnittstellen, Zonen und Routing-Protokolle, wenn Sie diese in Vorlagen konfiguriert haben, die dem Cloud-Vorlagenstack hinzugefügt wurden.
- Cloud NGFW berücksichtigt derzeit die Zertifikatverwaltungs- und die Protokolleinstellungen in Ihren Vorlagen, wie durch die Konfiguration der Cloud-Gerätegruppen referenziert. Alle anderen Einstellungen werden ignoriert.

*Weisen Sie Cloud-Gerätegruppen und Cloud-Vorlagenstacks keine verwalteten Geräte zu.*

Die Integration von Cloud NGFW in Panorama erfordert nur wenige Schritte. Nachdem Sie Ihre virtuelle Panorama-Appliance eingerichtet und die Plug-ins installiert haben, müssen Sie Cloud NGFW über AWS Marketplace abonnieren und einen Mandanten erstellen. Nachdem Sie den Cloud NGFW-Mandanten erstellt haben, verknüpfen Sie ihn mit Ihrer virtuellen Panorama-Appliance. Sobald Sie Cloud NGFW erfolgreich verknüpft haben, verwenden Sie Panorama, um Sicherheitsobjekte und -regeln zu verwalten und Protokolle sowie Analysen zu überwachen.

## Panorama-Integration vorbereiten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

So integrieren Sie den Cloud NGFW-Dienst in Ihre virtuelle Panorama-Appliance:

- Stellen Sie sicher, dass Sie eine registrierte Panorama-Instanz mit Lizenzen installiert haben, die mit der Supportlizenz im Customer Support Portal (CSP) aktiviert wurde und die Softwareversion 10.2.3 (oder höher) verwendet.

*Installieren Sie das Gerätezertifikat auf dem Panorama-Verwaltungsserver, um Panorama erfolgreich mit dem Palo Alto Networks Customer Support Portal (CSP) zu authentifizieren und einen oder mehrere Cloud-Dienste zu nutzen.*

- Wenn Sie sich für die Verwendung von Palo Alto Log Management entscheiden, müssen Sie auch Panorama für den Strata-Protokollierungsdienst konfigurieren.
- Stellen Sie sicher, dass Sie Cloud NGFW erfolgreich abonniert haben, sodass ein Cloud NGFW-Mandant vorhanden ist. Verwenden Sie das Cloud NGFW-Abonnement für eine erfolgreiche Integration in Panorama.
- Stellen Sie sicher, dass in Ihrem Cloud NGFW-Mandanten die Rolle eines Mandantenadministrators vorhanden ist.
- Stellen Sie sicher, dass in Ihrer Panorama-Instanz die Rolle eines Panorama-Administrators vorhanden ist.
- Stellen Sie sicher, dass Sie ein Palo Alto Networks Customer-Support-Portal(CSP)-Konto besitzen, bei dem Ihre Organisation die Panorama-Appliance registriert hat.

  *Für das Cloud NGFW-Mandantenabonnement sollte die E-Mail-Adresse verwendet werden, die für die Registrierung beim CSP-Konto verwendet wurde. Wenn dies eine abweichende E-Mail-Adresse ist, können Sie Cloud NGFW nicht konfigurieren und nicht in Panorama integrieren.*
- Lassen Sie den Zugriff auf die Domäne https://storage.googleapis.com zu. Diese Domäne wird, unabhängig von Ihrem geografischen Standort, für den Zugriff auf die AIOps für die Cloud NGFW-Anwendung verwendet.

## Zusätzliche Anforderungen

So bereiten Sie Panorama für die Verknüpfung mit Cloud NGFW vor:

- Installieren Sie das Cloud Connector-Plug-in Version 2.0.1 oder höher

  *PAN-OS Version 11.1.x ist mit einem Cloud Connector-Plug-in (Version 2.1.0-c98) vorinstalliert. Diese Plug-in-Version verursacht Probleme bei der Verwaltung der Cloud NGFW-Ressource, die mit PAN-OS Version 11.1.x verknüpft ist. Wenn Sie PAN-OS Version 11.1.x verwenden, empfiehlt Palo Alto Networks, dass Sie ein **Downgrade** für das Cloud Connector-Plug-in auf Version 2.0.1 durchführen.*
- Installieren Sie das AWS-Plug-in Version 5.1.1 oder höher.
- Nachdem Sie die Cloud Connector- und AWS-Plug-ins installiert haben, verwenden Sie die Befehlszeilenschnittstelle von Panorama, um den Befehl `request plugins cloudconnector enable cloudngfw` auszuführen.
- Zeigen Sie installierte Plug-ins in Panorama mithilfe des **Dashboards** an.
- Verwenden Sie die Befehlszeilenschnittstelle von Panorama, um den Status eines Panorama-Plug-ins anzuzeigen. Geben Sie beispielsweise folgenden Befehl ein: `show plugins aws cngfw-status`.

```
Das CloudConnector-Plug-in show plugins aws cngfw-status wird
 aktiviert. Die Cloud NGFW-Funktionalität wird aktiviert.
```

## Wichtige Überlegungen

Für das AWS-Plug-in müssen Sie eine Konfigurationsänderung vornehmen, um die Cloud NGFW-Funktionalität mit Panorama zu starten. Dieser Commit ist nicht erforderlich, wenn Sie ein Upgrade für das AWS-Plug-in durchführen.

Bei Panorama HA-Bereitstellungen kann das Durchführen einer Konfigurationsänderung (beispielsweise eine Änderung an einer Cloud-Gerätegruppe) dazu führen, dass die virtuelle Panorama-Appliance hängen bleibt. Es wird eine Fehlermeldung angezeigt, die in etwa folgenden Inhalt hat: *Push kann nicht verarbeitet werden, Konfiguration wurde nicht vollständig hochgeladen. Bitte versuchen Sie es später erneut*. Um dieses Problem zu beheben, verwenden Sie `commit-force` und anschließend `commit-all`.

# Cloud NGFW mit Palo Alto Networks Management verknüpfen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Für die Verknüpfung haben Sie zwei Möglichkeiten:

1. Verknüpfen Sie Cloud NGFW mithilfe von Panorama ausschließlich für die Richtlinienverwaltung mit Palo Alto Networks.
2. Verknüpfen Sie den Cloud NGFW-Mandanten mit Panorama für die Richtlinienverwaltung und mit dem Strata-Protokollierungsdienst für die Protokollverwaltung.

*Sie müssen den Cloud NGFW-Dienst mithilfe von AWS Marketplace abonniert haben, um Cloud NGFW in Panorama zu integrieren. Nachdem Sie Ihren Cloud NGFW-Mandanten mit Panorama verknüpft haben, können Sie die Mandanten und Ressourcen zusammen mit ihrem Status in der Panorama-Konsole unter dem AWS-Plug-in anzeigen.*

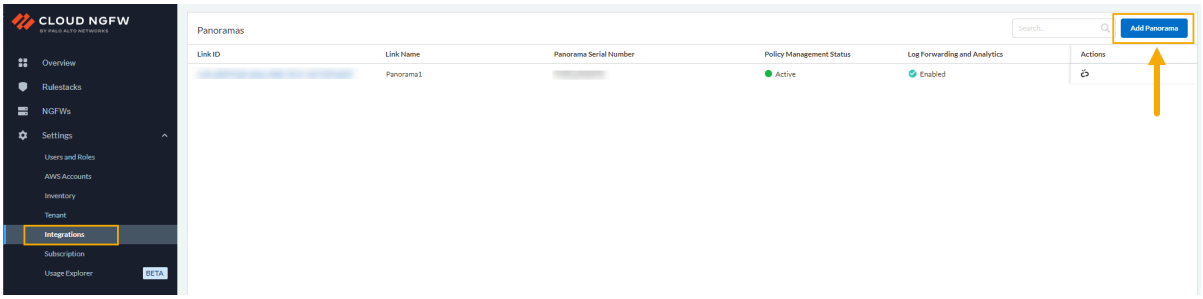
*Informationen zum Entfernen einer vorhandenen virtuellen Panorama-Appliance aus der Cloud NGFW-Ressource finden Sie unter Unlink from Panorama (Verknüpfung mit Panorama aufheben). Wenn Sie AWS Firewall Manager verwenden, können Sie die Verknüpfung von Panorama mit Ihrer Cloud NGFW-Ressource nicht aufheben. Weitere Informationen finden Sie unter Supportfall zum Aufheben der Verknüpfung von Panorama mit Cloud NGFW bei Verwendung von AWS Firewall Manager erstellen.*

So verknüpfen Sie Ihren Cloud NGFW-Mandanten mithilfe von Cloud NGFW mit Panorama:

**STEP 1 |** Wählen Sie **Integrations (Integrationen)** aus.

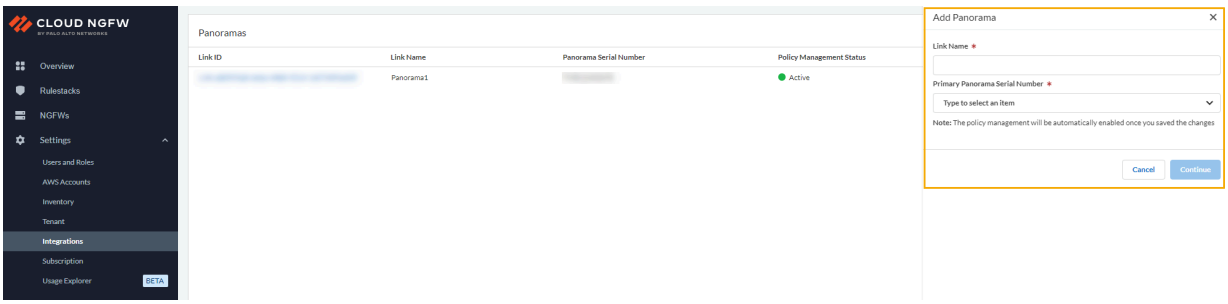
 

**STEP 2 |** Klicken Sie auf der Seite **Integrations (Integrationen)** auf **Add Panorama (Panorama hinzufügen)**.




Wenn Sie einen Mandanten verwenden, der mit Panorama verknüpft ist und mit dem AWS Firewall Manager erstellt wurde, können Sie die Verknüpfung der Cloud NGFW-Ressource nicht aufheben.

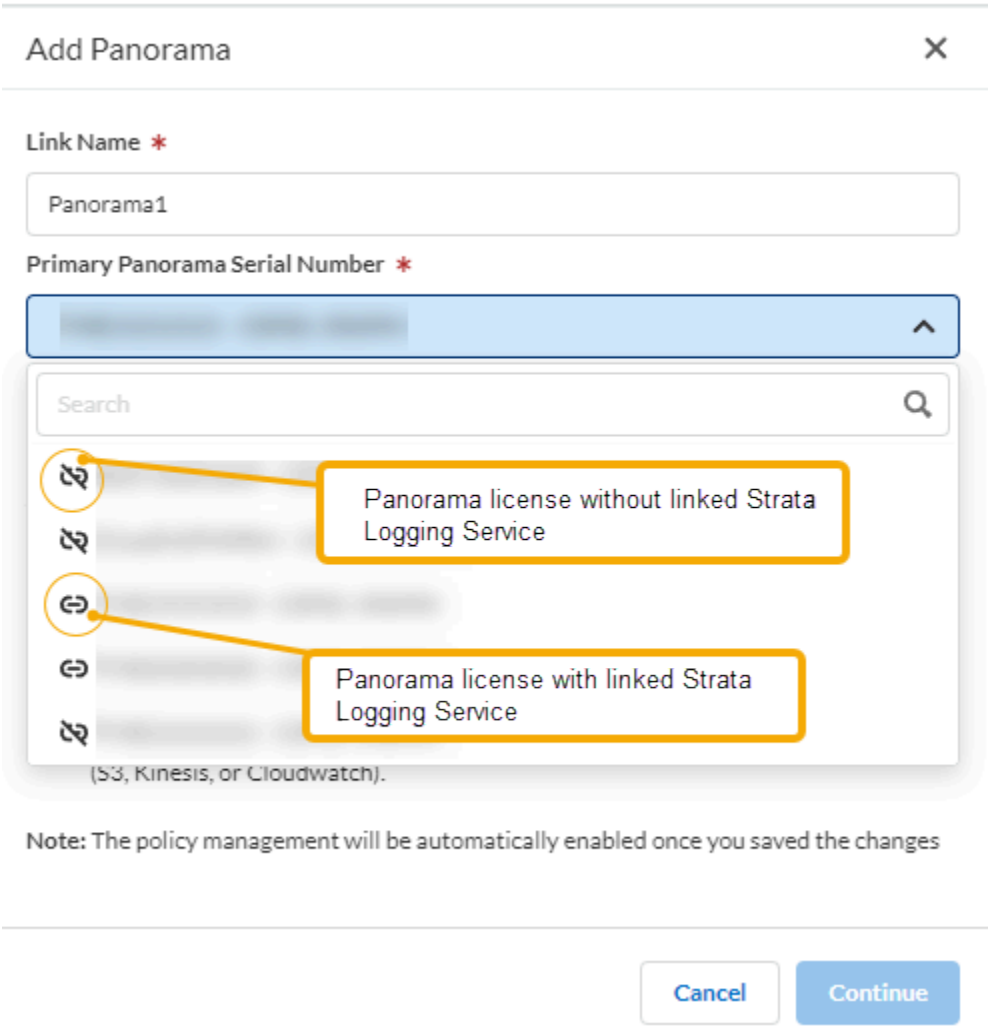
**STEP 3 |** Geben Sie im Bildschirm **Add Panorama (Panorama hinzufügen)** einen **Verknüpfungsnamen** ein. Wählen Sie aus der Dropdown-Liste die Option **Primary Panorama Serial Number (Primäre Panorama-Seriennummer)** aus. Wählen Sie für HA-Umgebungen aus der Dropdown-Liste die Option **Secondary Panorama Serial Number (Sekundäre Panorama-Seriennummer)** aus.




Auf diesem Bildschirm werden zwei verschiedene Symbole angezeigt, die den Status der Panorama-Lizenz beschreiben: eine mit dem Strata-Protokollierungsdienst verknüpfte Panorama-Lizenz und

eine Panorama-Lizenz, die nicht mit dem Strata-Protokollierungsdienst verknüpft ist. In der folgenden Abbildung sind diese Symbole veranschaulicht:



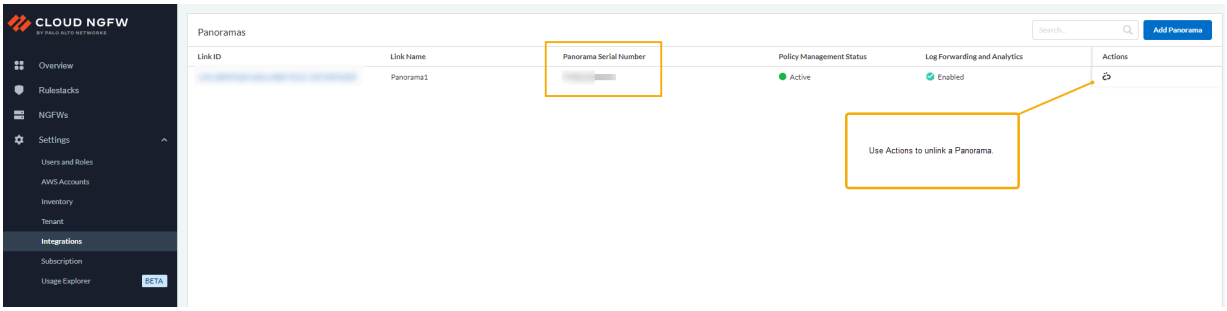

Wenn Sie eine Panorama-Seriennummer auswählen, die nicht mit dem Strata-Protokollierungsdienst verknüpft ist, haben Sie die Option, den Verknüpfungsvorgang abzubrechen. In diesem Fall stimmen Sie zu, eine Strata-Protokollierungsdienst-Lizenz zu erwerben und sie Ihrer Panorama-Appliance

zuzuordnen. Alternativ können Sie zustimmen, Panorama weiterhin nur zur Richtlinienverwaltung zu verwenden:

Wenn Sie eine Panorama-Lizenz auswählen, die bereits mit einem Strata-Protokollierungsdienst verknüpft ist, werden Sie aufgefordert, die Verknüpfung zu **bestätigen**, bevor Sie mit dem Integrationsprozess fortfahren.

Nachdem Sie die Panorama-Lizenz ausgewählt haben, klicken Sie auf **Continue (Weiter)**. Auf der Seite **Integrations (Integrationen)** werden die **Verknüpfungs-ID** und die verknüpfte **Panorama-Seriennummer** angezeigt:

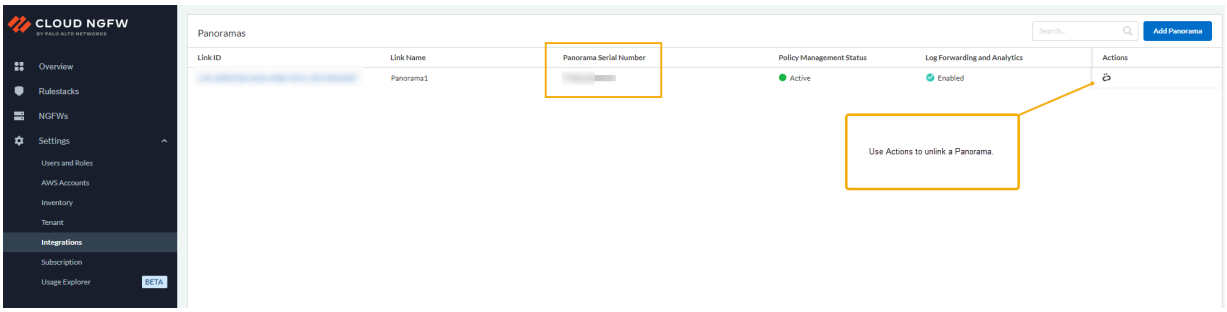



Der Cloud NGFW-Mandant ruft die Informationen zum Strata-Protokollierungsdienst automatisch aus Panorama ab. Wenn Sie den Strata-Protokollierungsdienst nicht verwenden möchten, können Sie

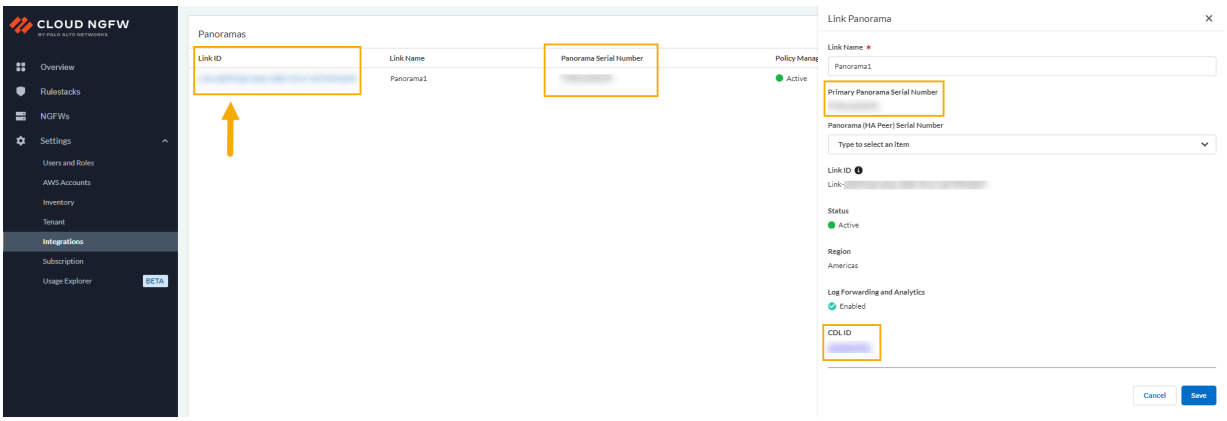
 

Protokolle an AWS senden. Weitere Informationen finden Sie unter Protokollierung in Cloud NGFW für AWS konfigurieren.

Auf der Seite **Integrations (Integrationen)** werden die **Verknüpfungs-ID** und die verknüpfte **Panorama-Seriennummer** angezeigt.




Klicken Sie auf der Seite **Integrations (Integrationen)** auf die **Verknüpfungs-ID**, um weitere Informationen zu erhalten, einschließlich der Strata-Protokollierungsdienst-ID, die der verknüpften Panorama-Instanz zugeordnet ist. Das Fenster **Link Panorama (Panorama verknüpfen)** wird angezeigt:



## Abonnement eines Cloud NGFW-Mandanten im AWS Marketplace kündigen

So kündigen Sie das Abonnement eines Cloud NGFW-Mandanten im AWS Marketplace:

**STEP 1 |** Melden Sie sich bei der AWS Management Console an.

**STEP 2 |** Wechseln Sie auf die Seite **My Subscriptions (Meine Abonnements)**.

**STEP 3 |** Wählen Sie das Abonnement für das Produkt aus, das Sie kündigen möchten.

**STEP 4 |** Wählen Sie **Cancel subscription (Abonnement kündigen)** aus. Nachdem Sie Ihr Abonnement gekündigt haben, können Sie Ihre Anwendung nicht mehr starten.

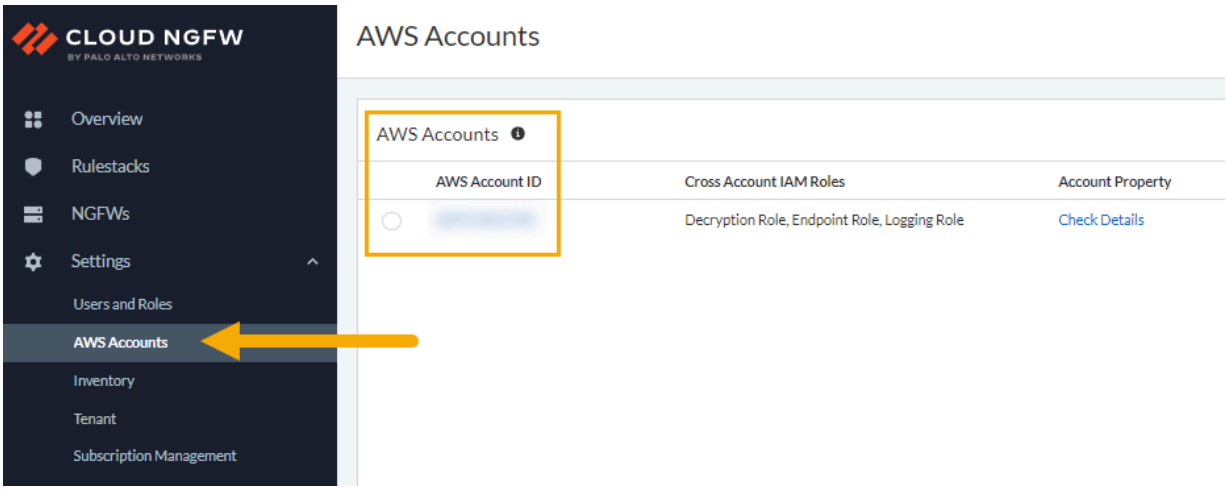
Weitere Informationen finden Sie auf der Seite zur Kündigung Ihres Abonnements.

## Supportfall zum Aufheben der Verknüpfung von Panorama mit Cloud NGFW bei Verwendung von AWS Firewall Manager erstellen

Wenn Sie AWS Firewall Manager verwenden und eine Cloud NGFW-Ressource mit Panorama verknüpft haben, müssen Sie sich an den Support von Palo Alto Networks wenden, um die Verknüpfung der Cloud NGFW-Ressource mit Panorama aufzuheben. Beim Erstellen des Supportfalls werden Sie möglicherweise aufgefordert, zusätzliche Informationen anzugeben, z. B. die AWS-Konto-ID und die Mandanten-ID für die Ressource.

So erstellen Sie einen Supportfall mithilfe der Cloud NGFW-Konsole:

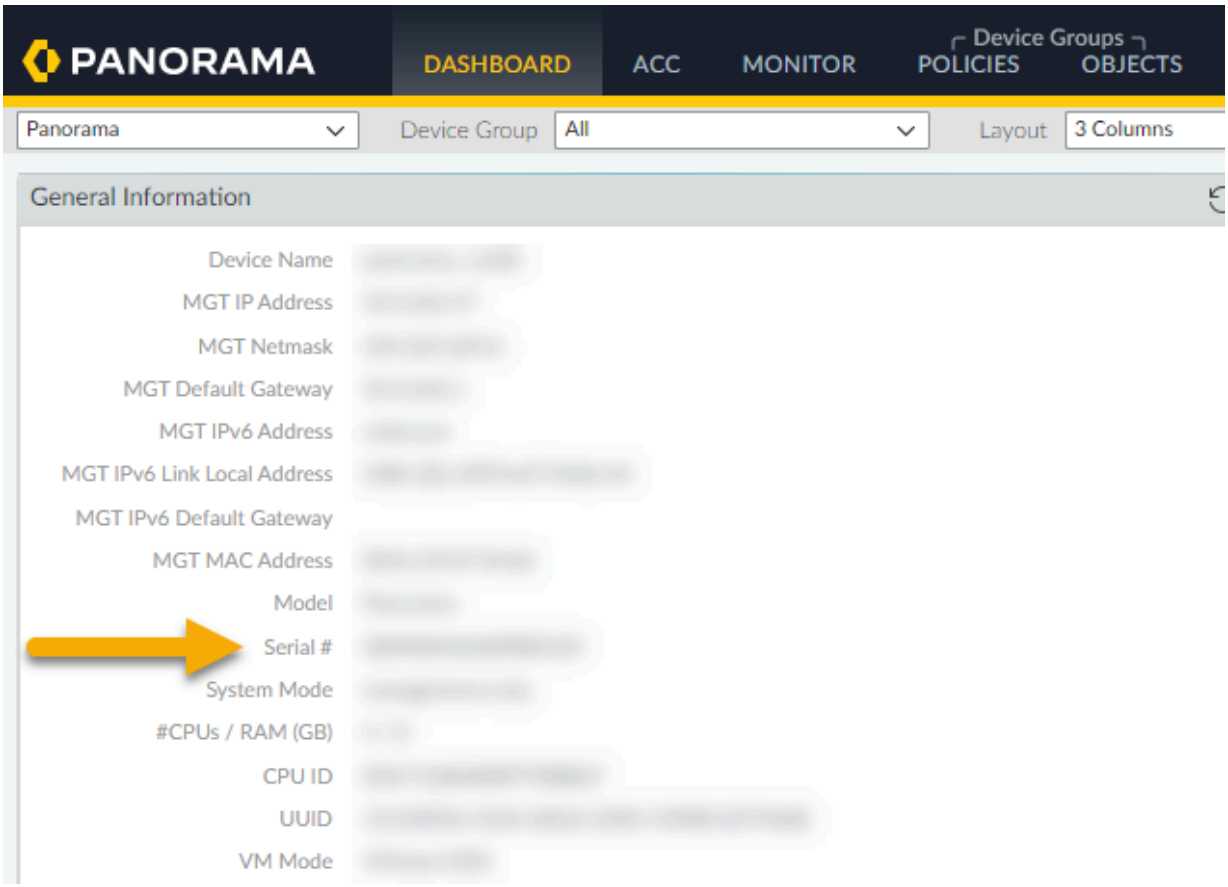
**STEP 1 |** Suchen Sie Ihre **AWS-Konto-ID**. Wählen Sie **AWS Accounts (AWS-Konten)** aus.



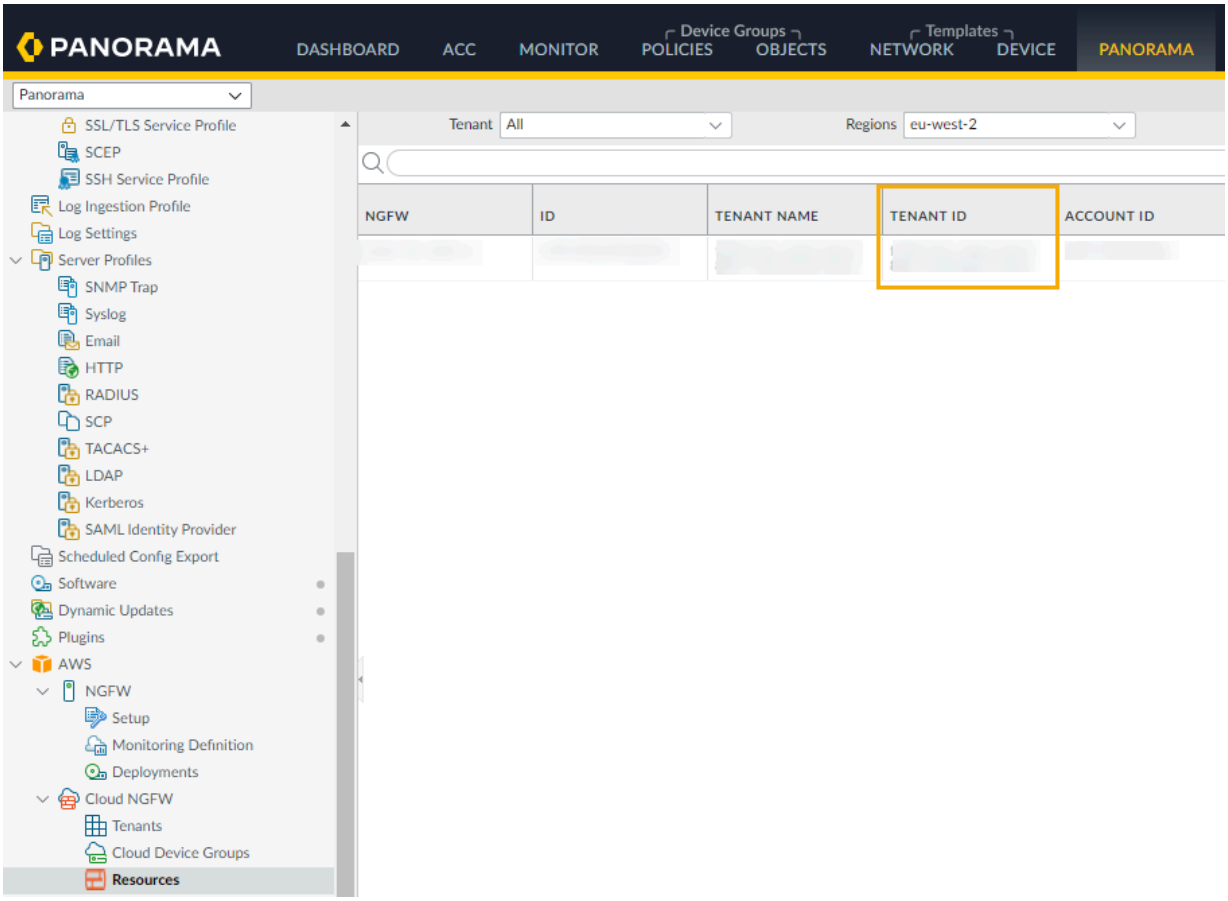
**STEP 2 |** Verwenden Sie bei Bedarf die Panorama-Konsole, um zusätzliche Informationen für den Supportfall zu ermitteln, beispielsweise die Mandanten-ID oder die Panorama-Seriennummer.

Suchen Sie die **Panorama-Seriennummer** mithilfe des **Dashboards**:




Suchen Sie die **Mandanten-ID** für die Cloud NGFW-Ressource:

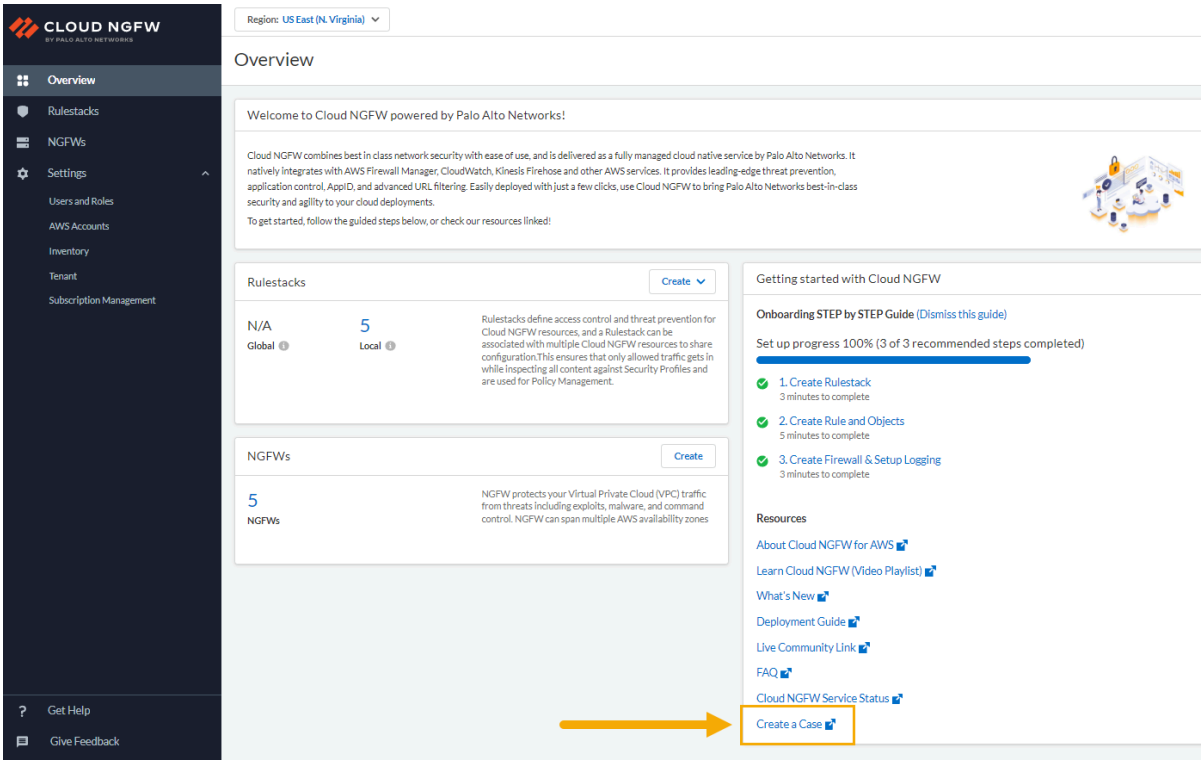
 



**STEP 3 |** Klicken Sie auf der Seite **Overview (Übersicht)** in der Cloud NGFW-Konsole auf **Create a case (Fall erstellen)**.



# Verknüpfte Panorama-Instanz der Cloud NGFW-Ressource zuordnen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Bevor Sie mehrere Panorama-Instanzen mit einem Cloud NGFW-Mandanten verknüpfen können, müssen Sie Ihre Cloud NGFW-Ressource in die virtuelle Panorama-Appliance integrieren. Bereiten Sie zunächst Ihre Panorama-Appliance für diese Integration vor, indem Sie die Plug-ins installieren. Dann müssen Sie die Cloud NGFW-Konsole verwenden, um sie mit Ihrer Panorama-Appliance zu verknüpfen. Nachdem Sie Cloud NGFW erfolgreich verknüpft haben, verwenden Sie Panorama, um Sicherheitsobjekte und -regeln zu verwalten und um Protokolle und Analysen zu überwachen.

**STEP 1 |** Bereiten Sie Ihre Panorama-Instanz vor.

**STEP 2 |** Verknüpfen Sie Ihre Panorama-Instanz.

Nachdem Sie Ihre Panorama-Instanz mit Ihrer Cloud NGFW-Ressource verknüpft haben, können Sie sie einem anderen Cloud NGFW-Mandanten zuordnen.

## Verknüpfen mehrerer Panorama-Instanzen mit einem Cloud NGFW-Mandanten

So verknüpfen Sie mehrere Panorama-Instanzen mit demselben Cloud NGFW-Mandanten:

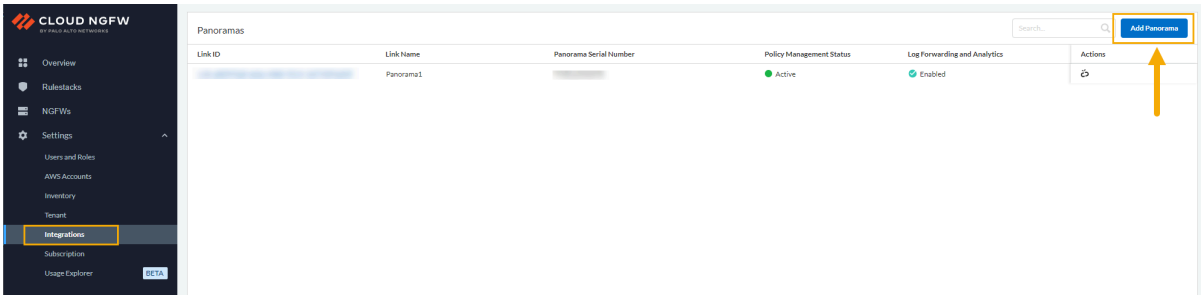
**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Wählen Sie **Integrations (Integrationen)** aus.

Auf der Seite **Integrations (Integrationen)** werden Informationen zur aktuell verknüpften Panorama-Instanz angezeigt. Wenn eine Panorama-Instanz derzeit nicht mit einem Cloud NGFW-Mandanten verknüpft ist, ist diese Seite leer.

**STEP 3 |** Verwenden Sie die Seite **Integrations (Integrationen)**, um eine zusätzliche Panorama-Instanz hinzuzufügen. Klicken Sie auf **Add Panorama (Panorama hinzufügen)**.

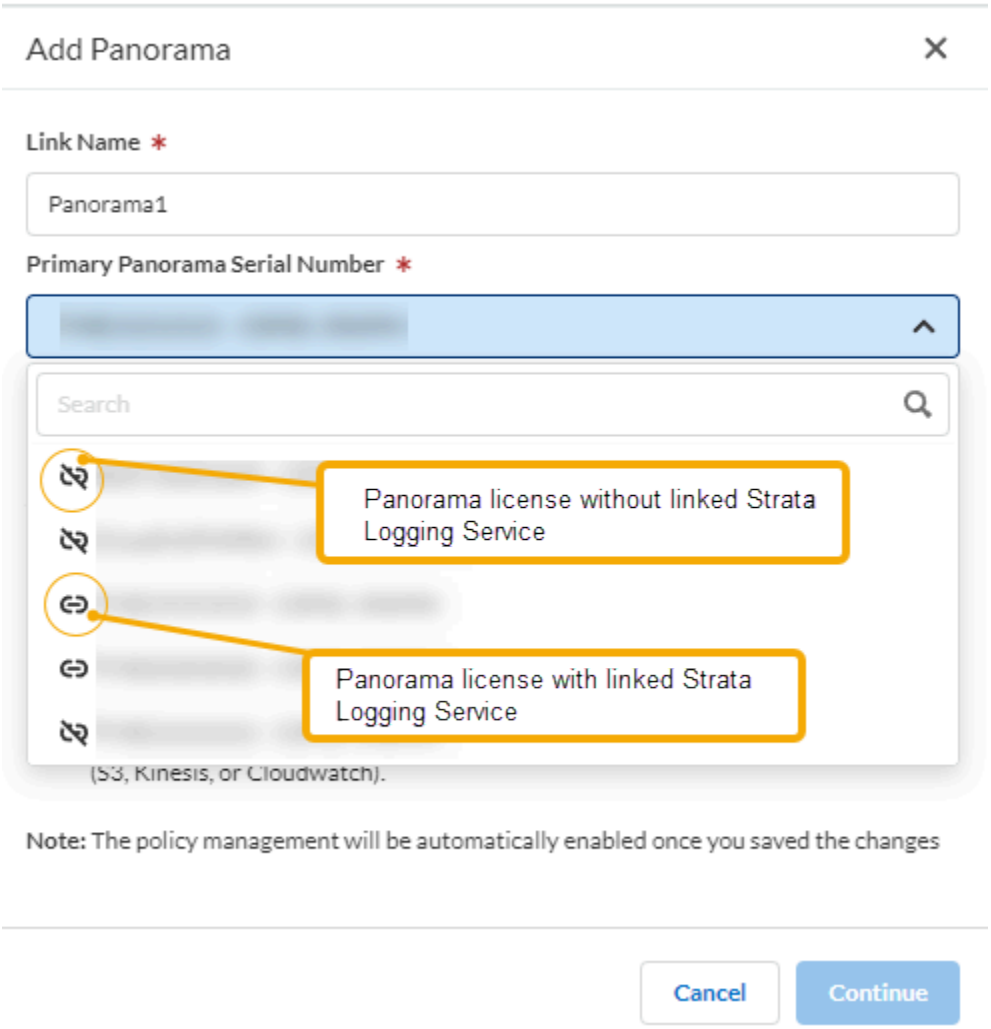



**STEP 4 |** Geben Sie im Bildschirm **Add Panorama (Panorama hinzufügen)** einen **Verknüpfungsnamen** ein. Wählen Sie aus der Dropdown-Liste **Primary Panorama Serial Number (Primäre Panorama-Seriennummer)** eine aktuell verknüpfte Panorama-Instanz aus. Wählen Sie für HA-Umgebungen aus der Dropdown-Liste die Option **Secondary Panorama Serial Number (Sekundäre Panorama-Seriennummer)** aus.

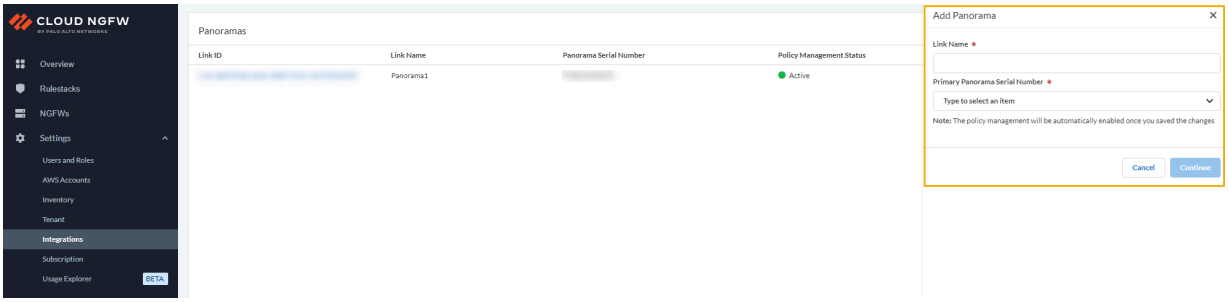
Auf diesem Bildschirm werden zwei verschiedene Symbole angezeigt, die den Status der Panorama-Lizenz beschreiben: eine mit dem Strata-Protokollierungsdienst verknüpfte Panorama-Lizenz und

eine Panorama-Lizenz, die nicht mit dem Strata-Protokollierungsdienst verknüpft ist. In der folgenden Abbildung sind diese Symbole veranschaulicht:



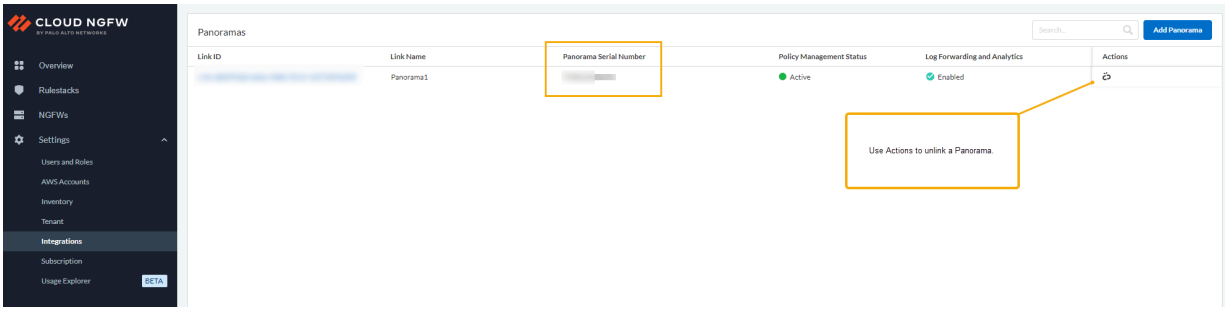

Wenn Sie eine Panorama-Seriennummer auswählen, die nicht mit dem Strata-Protokollierungsdienst verknüpft ist, haben Sie die Option, den Verknüpfungsvorgang abzubrechen. In diesem Fall stimmen Sie zu, eine Strata-Protokollierungsdienst-Lizenz zu erwerben und sie mit Ihrer Panorama-Appliance zu verknüpfen. Alternativ können Sie zustimmen, Panorama weiterhin nur zur Richtlinienverwaltung zu verwenden:




Wenn Sie eine Panorama-Lizenz auswählen, die bereits mit dem Strata-Protokollierungsdienst verknüpft ist, werden Sie aufgefordert, die Verknüpfung zu **bestätigen**, bevor Sie mit dem Integrationsprozess fortfahren.

**STEP 5 |** Nachdem Sie die Panorama-Lizenz ausgewählt haben, klicken Sie auf **Continue (Weiter)**. Auf der Seite **Integrations (Integrationen)** werden nun die **Verknüpfungs-ID** und die verknüpfte **Panorama-Seriennummer** angezeigt:




**STEP 6 |** Nachdem Sie Cloud NGFW eine weitere Panorama-Instanz hinzugefügt haben, klicken Sie auf **NGFWs** und wählen Sie die Firewall aus, die Sie Panorama zuordnen möchten.

**STEP 7 |** Wählen Sie die Registerkarte **Firewall Settings (Firewall-Einstellungen)** aus.

**STEP 8 |** Scrollen Sie nach unten zum Abschnitt **Policy Management (Richtlinienverwaltung)**. Wählen Sie **Panorama** aus.

**STEP 9 |** Wählen Sie im Dropdown-Menü die **verknüpfte Panorama-Instanz** aus, die Sie der Firewall zuordnen möchten.

**STEP 10 |** Klicken Sie auf **Save (Speichern)**.

**STEP 11 |** Wiederholen Sie die Schritte 6 bis 10, um der Ressource eine weitere Panorama-Instanz hinzuzufügen.

# Verknüpfung von Cloud NGFW mit Panorama aufheben

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Bevor Sie die Verknüpfung Ihrer Cloud NGFW-Ressource mit der virtuellen Panorama-Appliance aufheben, empfiehlt Palo Alto Networks, dass Sie der Cloud NGFW-Ressource oder entsprechenden Regionen zugeordnete *Cloud-Gerätegruppen* löschen oder ihre Zuordnung zur Cloud NGFW-Ressource bzw. den entsprechenden Regionen aufheben. Weitere Informationen finden Sie unter Löschen einer Cloud-Gerätegruppe und unter Zuordnung einer Cloud-Gerätegruppe zu einer Ressource aufheben.

So heben Sie die Verknüpfung einer virtuellen Panorama-Appliance mit einer Cloud NGFW-Ressource auf:

**STEP 1 |** Wählen Sie auf der Seite „Firewall“ oder „Rulestacks“ (Regelstapel) die Region aus, zum Beispiel **us-east-1**.

**STEP 2 |** Wählen Sie in der Cloud NGFW-Konsole die Option **Integrations (Integrationen)** aus.

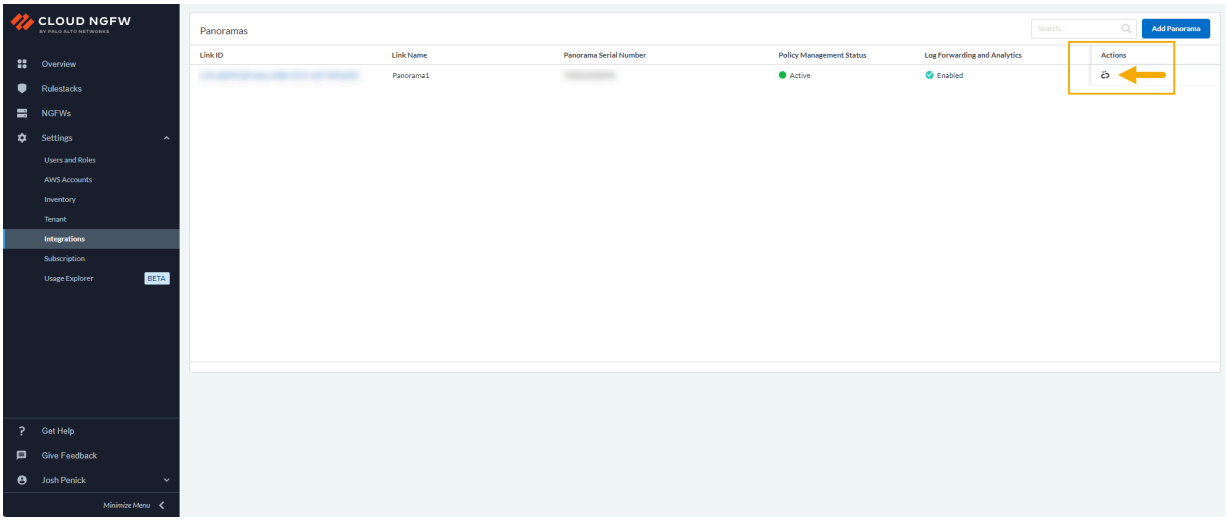
**STEP 3 |** Suchen Sie auf der Seite **Integrations (Integrationen)** den Abschnitt **Actions (Aktionen)**. Eine bereits verknüpfte Panorama-Instanz wird ausgegraut angezeigt.

**STEP 4 |** Klicken Sie auf das Symbol **Unlink (Verknüpfung aufheben)**, um mit dem Aufheben der Verknüpfung zu beginnen.

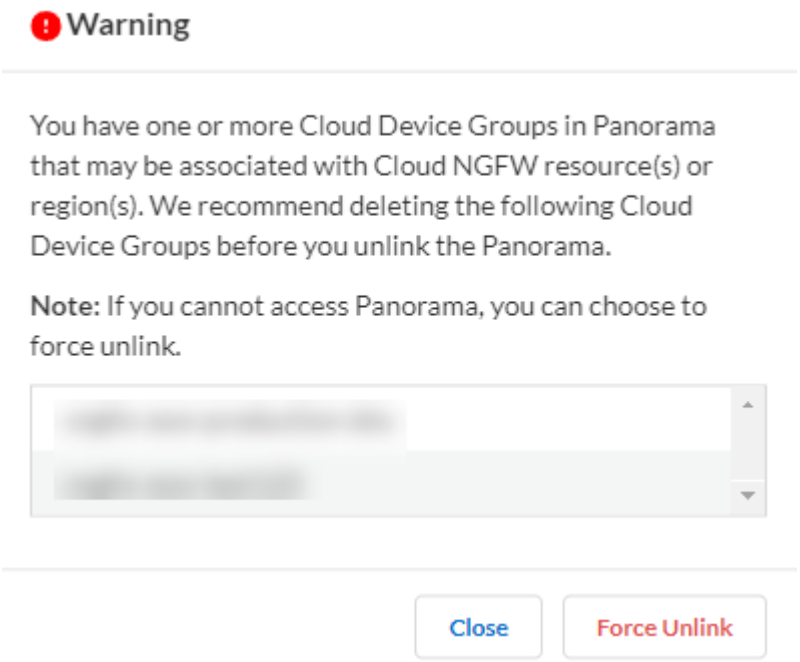
Wenn ein HA-Paar konfiguriert ist, wird das Paar getrennt.



**STEP 5 |** Wenn Sie die Verknüpfung einer virtuellen Panorama-Appliance mit Ihrem Cloud NGFW-Mandanten aufheben, werden Sie möglicherweise aufgefordert, eine oder mehrere Cloud-Gerätegruppen zu löschen, die der Cloud NGFW-Ressource oder -Region zugeordnet sind, deren Verknüpfung Sie aufheben. In solchen Fällen wird eine Fehlermeldung mit einer Liste der Cloud-Gerätegruppen angezeigt, die der mit Panorama verknüpften Cloud NGFW-Ressource zugeordnet sind. Vor dem Aufheben einer Verknüpfung müssen Sie eine Cloud-Gerätegruppe aus einer Ressource löschen oder die Zuordnung einer Cloud-Gerätegruppe zu einer Ressource aufheben. Wenn Sie keinen Zugriff auf Panorama haben, um diese Cloud-Gerätegruppen zu entfernen, klicken Sie auf **Force Unlink (Aufheben der Verknüpfung erzwingen)**.




**STEP 6 |** **Bestätigen** Sie das Aufheben der Verknüpfung. Wenn bei Ihnen Panorama einem Konto des Strata-Protokollierungsdienstes zugeordnet ist, wird diese Zuordnung aufgehoben und Protokolle werden nach Ablauf der Aufbewahrungsfrist gelöscht.

Nachdem Sie die Anforderung zur Aufhebung der Verknüpfung bestätigt haben, wird auf der Seite **Integrations (Integrationen)** der Status der Cloud NGFW-Ressource angezeigt.

Palo Alto Networks empfiehlt, dass Sie die auf Panorama konfigurierten **Überwachungsdefinitionen** entfernen.

Mit der Option **Force Unlink (Aufheben der Verknüpfung erzwingen)** werden **Überwachungsdefinitionen** nicht automatisch aus Panorama entfernt.

Sie können die Überwachungsdefinitionen der Mandanten anzeigen und löschen, indem Sie die folgenden Befehle ausschließlich über die Befehlszeilenschnittstelle ausführen:

```
request plugins dau plugin-name cloud_services unblock-device-push
 yes request plugins dau plugin-name cloudconnector unblock-device-
push yes request plugins dau plugin-name vm_series unblock-device-
push yes request plugins dau plugin-name aws unblock-device-push
 yes
```

# Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden

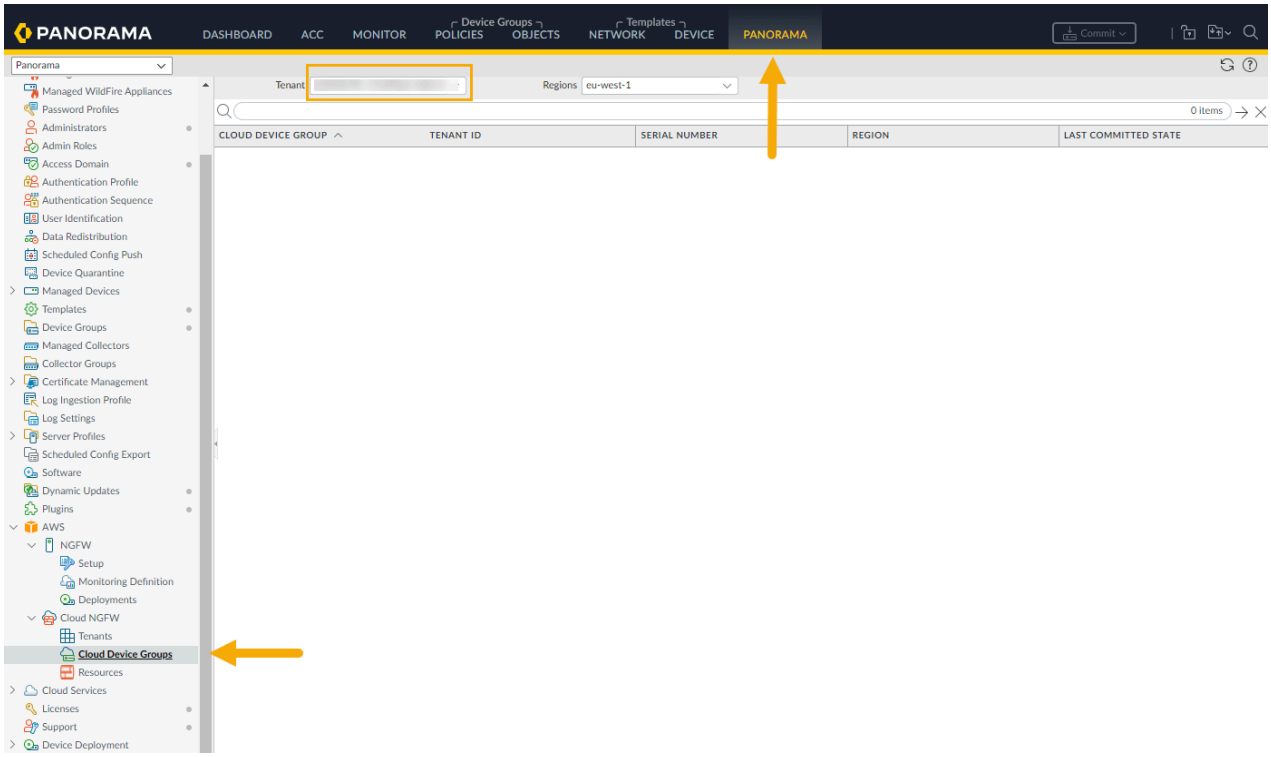
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Nachdem Sie Ihren Cloud NGFW-Mandanten mit der virtuellen Panorama-Appliance verknüpft haben, können Sie die Integration für Aufgaben der Richtlinienverwaltung verwenden, z. B. zum Hinzufügen von Gerätegruppen und Anwenden von Richtlinien auf die Gerätegruppe für den Cloud NGFW-Mandanten mithilfe der Panorama-Konsole.

Wenn Sie die Panorama-Konsole zum Konfigurieren der Cloud NGFW verwenden, speichert der Browser lokale Informationen wie die Cloud-Gerätegruppe, den Vorlagenstack und die Region im Cache, sodass beim Wechseln zwischen Panorama-Aufgaben zwischengespeicherte Cloud NGFW-Informationen in der Panorama-Konsole angezeigt werden.

Wenn Sie einen Mandanten aus dem Knoten **Cloud Device Groups (Cloud-Gerätegruppen)** auswählen und zu einer anderen Konfigurationsoption in Panorama navigieren, bleibt bei der Rückkehr zum Knoten **Resources (Ressourcen)** die zuvor ausgewählte Mandantenansicht erhalten. Wenn Sie beispielsweise einen einzelnen Mandanten in einer Region auswählen, werden die für diesen Mandanten konfigurierten Cloud-Gerätegruppen angezeigt.

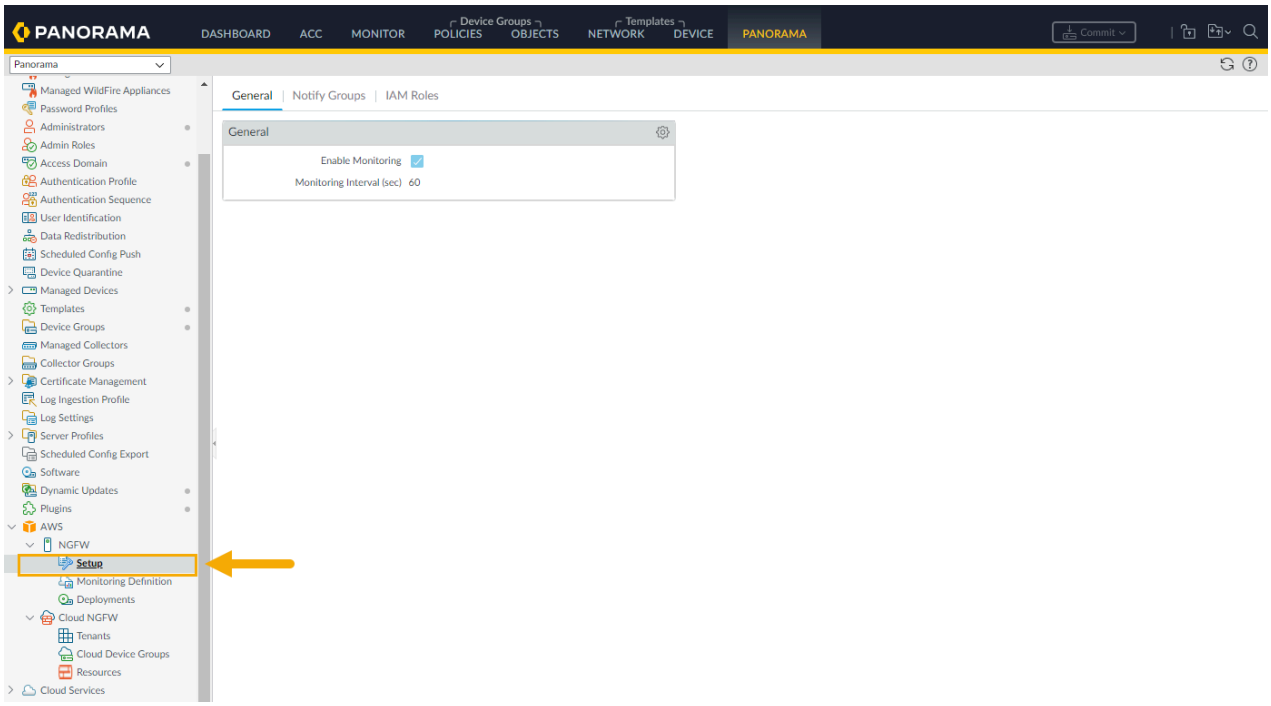
 




Wenn Sie zu einem anderen Bereich in der Panorama-Konsole navigieren und dann zu **Cloud NGFW > Cloud Device Groups (Cloud-Gerätegruppen)** zurückkehren, zeigt die Konsole den einzelnen

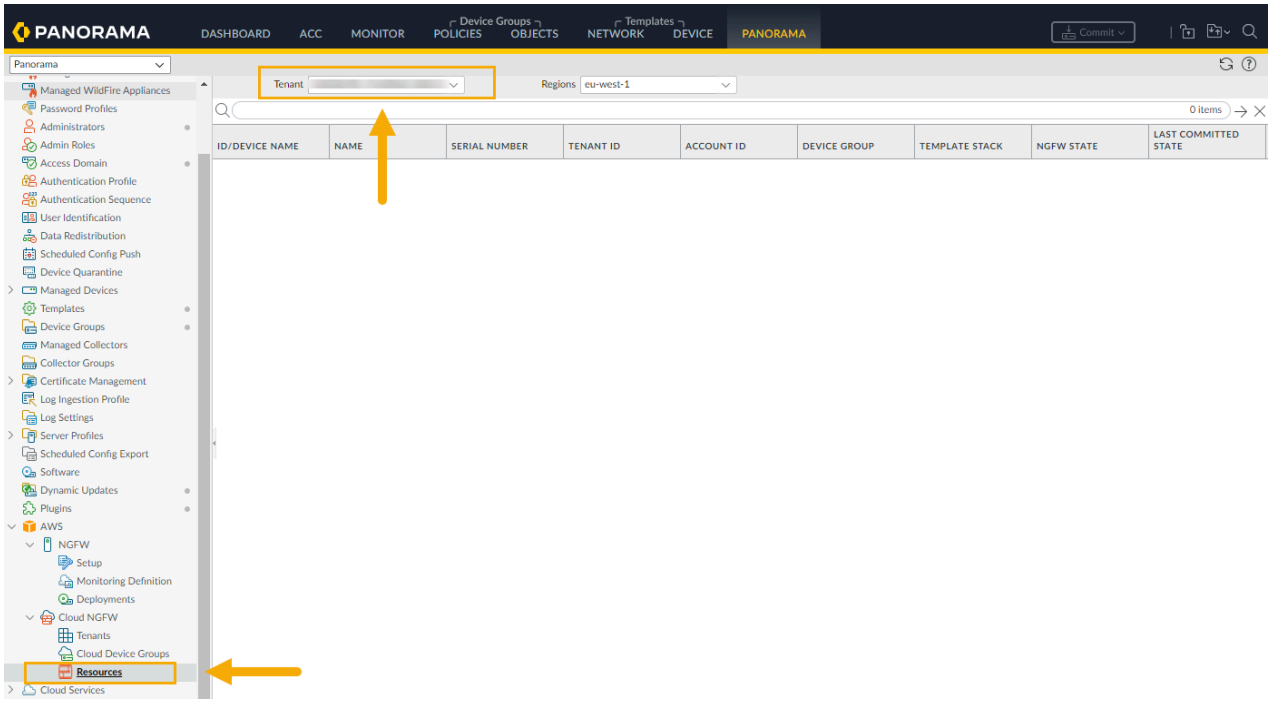
 

Mandanten an, den Sie zuvor ausgewählt haben. Wählen Sie beispielsweise nach der Anzeige der Cloud-Gerätegruppen für einen Mandanten **AWS > Setup (Einrichten)** aus.




Wenn Sie zum Bildschirm **Cloud NGFW > Resources (Ressourcen)** zurückkehren, merkt sich die Panorama-Konsole den zuvor ausgewählten Mandanten, anstatt alle der Cloud NGFW-Ressource zugeordneten Mandanten anzuzeigen.

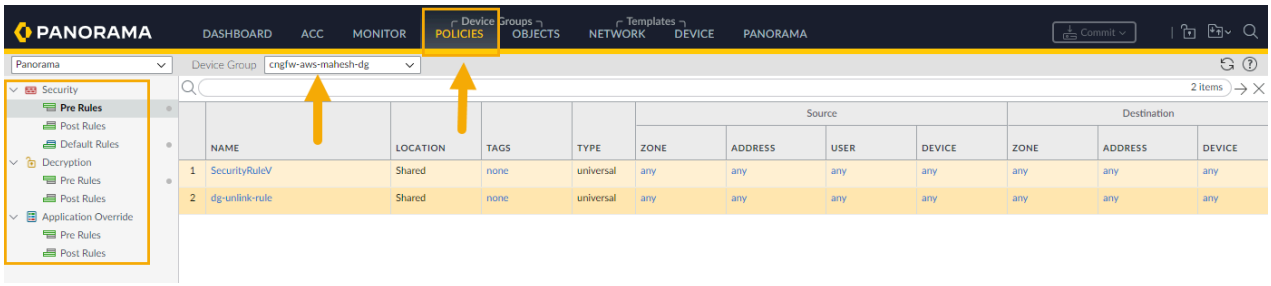



*Aktualisieren Sie den Browser, um die Anzeige dynamisch zu aktualisieren.*

Die Panorama-Integration zeigt nur die Konfigurationsoptionen an, die für die Cloud NGFW-Ressource verfügbar sind. Wählen Sie beispielsweise **Policies (Richtlinien)** aus, um die für die Cloud NGFW-

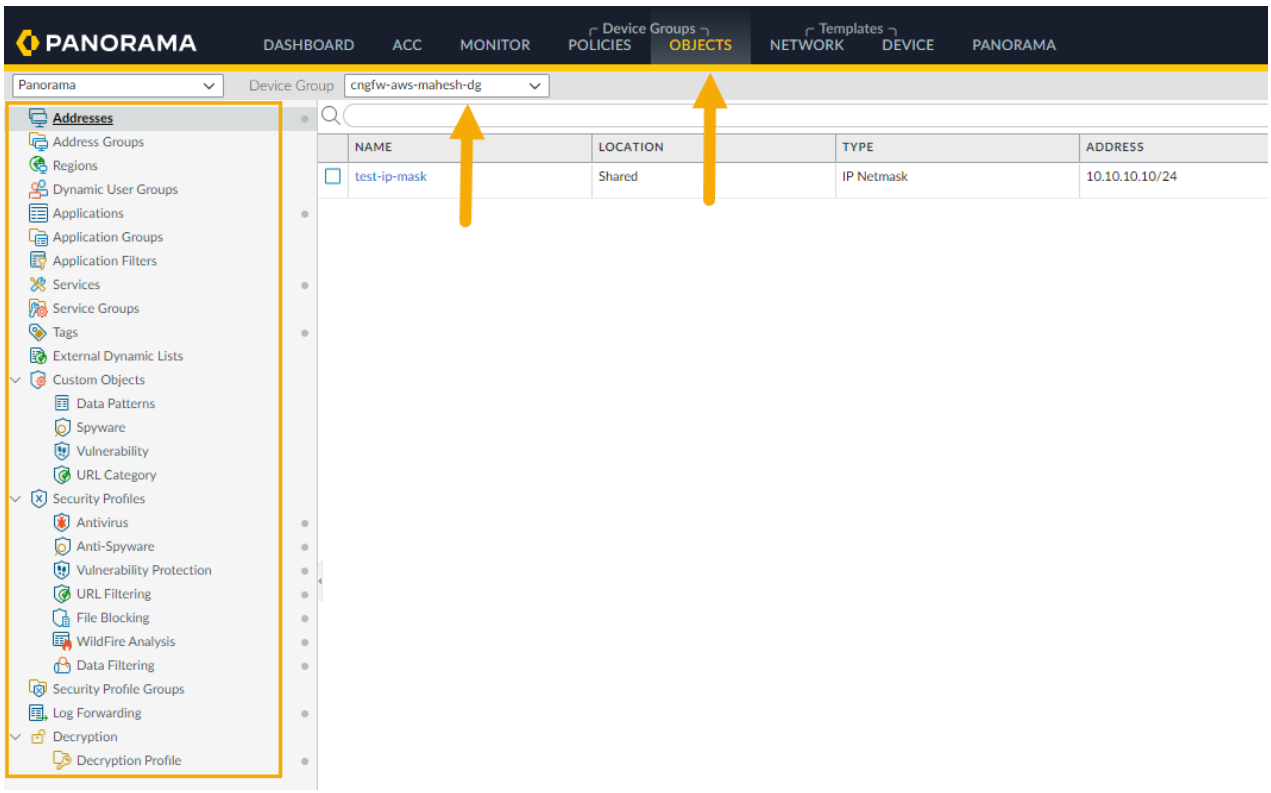
Ressource verfügbaren Richtlinienoptionen anzuzeigen. Die Panorama-Konsole zeigt nur Richtlinien an, die für die Cloud-Gerätegruppe in Cloud NGFW verfügbar sind.




*Der Gerätegruppenname weist das Präfix* `cngfw-aws` *auf.*

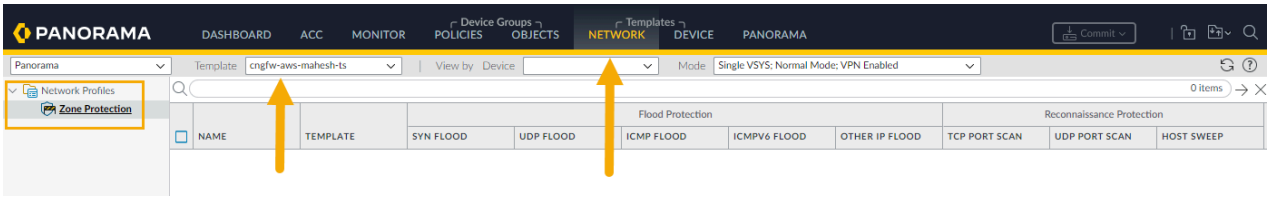
Um von der Cloud NGFW-Ressource unterstützte Gerätegruppenobjekte anzuzeigen, wählen Sie **Objects (Objekte)** aus. In der Panorama-Konsole werden nur die von Cloud NGFW unterstützten Objekte angezeigt.




Um von der Cloud NGFW-Ressource unterstützte Vorlagen anzuzeigen, wählen Sie **Network (Netzwerk)** aus. Es werden nur die von Cloud NGFW unterstützten Cloud-Vorlagen angezeigt.




### Überlegungen zu Regelstapeln

Wenn Sie eine Cloud NGFW-Ressource mit einem lokalen Regelstapel bereitstellen, können Sie sie keiner Cloud-Gerätegruppe in Panorama zuordnen. Die Firewall wird in der Panorama-Konsole ausgegraut angezeigt. Um dieses Problem zu beheben, können Sie den lokalen Regelstapel mithilfe der Cloud NGFW-Konsole trennen oder eine neue Firewall-Ressource ohne lokalen Regelstapel bereitstellen und sie einer Cloud-Gerätegruppe in Panorama zuordnen. Alternativ können Sie einen globalen Regelstapel verwenden.

Bei Firewalls, die mit dem AWS Firewall Manager Service (FMS) erstellt wurden, kann der Regelstapel in der Panorama-Konsole nicht abgewählt werden. Wählen Sie aus der FMS-Konsole einen von Panorama per Push übertragenen globalen Regelstapel aus. Bei diesem Vorgang wird der zugeordnete Regelstapel entfernt und die Firewall wird mit einem von Panorama per Push übertragenen globalen Regelstapel aktualisiert. Weitere Informationen finden Sie in der AWS FMS-Dokumentation.

### Cloud-Gerätegruppen hinzufügen

Mit Panorama gruppieren Sie Firewalls in Ihrem Netzwerk in logische Einheiten, die *Gerätegruppen* genannt werden. Eine Gerätegruppe ermöglicht die Gruppierung basierend auf Netzwerksegmentierung, geografischem Standort, Organisationsfunktion oder einem anderen gemeinsamen Aspekt von Firewalls, bei dem ähnliche Richtlinienkonfigurationen erforderlich sind.

Mithilfe von Gerätegruppen können Sie Richtlinienregeln und die von ihnen referenzierten Objekte konfigurieren. Organisieren Sie Gerätegruppen hierarchisch mit gemeinsamen Regeln und Objekten an der Spitze und gerätegruppenspezifischen Regeln und Objekten auf nachfolgenden Ebenen. So können Sie eine Hierarchie von Regeln erstellen, die erzwingen, wie Firewalls mit dem Datenverkehr umgehen.

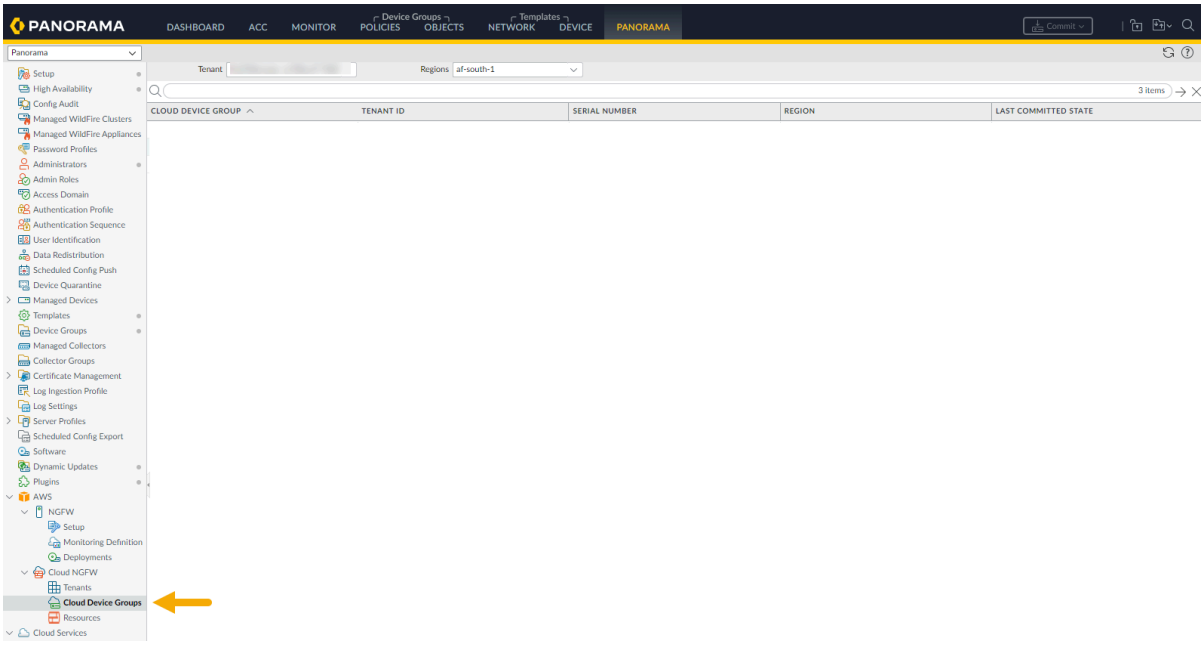
*Weitere Informationen finden Sie unter* Gerätegruppen verwalten.

So fügen Sie mithilfe der Panorama-Konsole eine Cloud-Gerätegruppe hinzu:

**STEP 1 |** Wählen Sie im **AWS**-Plug-in die Option **Cloud Device Groups (Cloud-Gerätegruppen)** aus. Wenn Sie die Tabelle „Cloud Device Group“ (Cloud-Gerätegruppe) zum ersten Mal auswählen, ist sie leer.

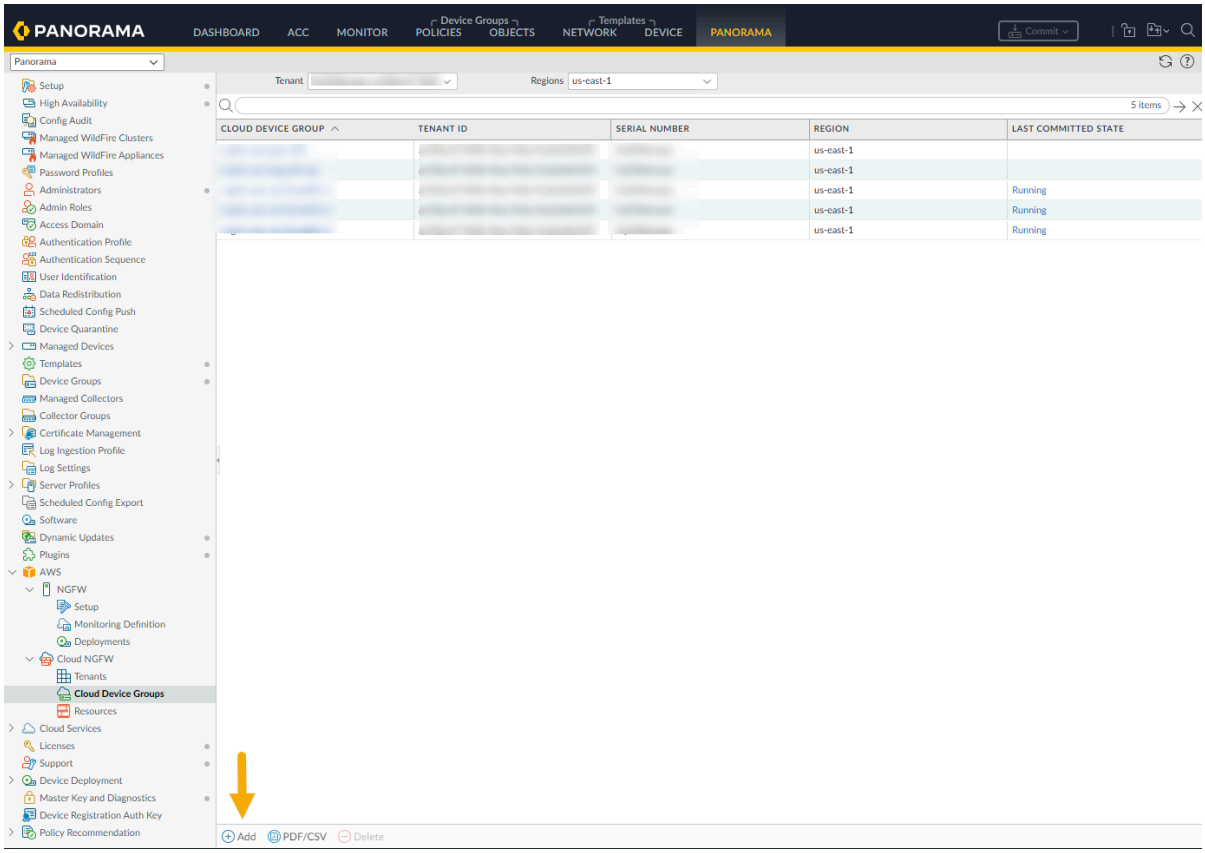
Zuvor erstellte Cloud-Gerätegruppen werden angezeigt, wenn sie mit AWS für den Cloud NGFW-Mandanten eingerichtet wurden.



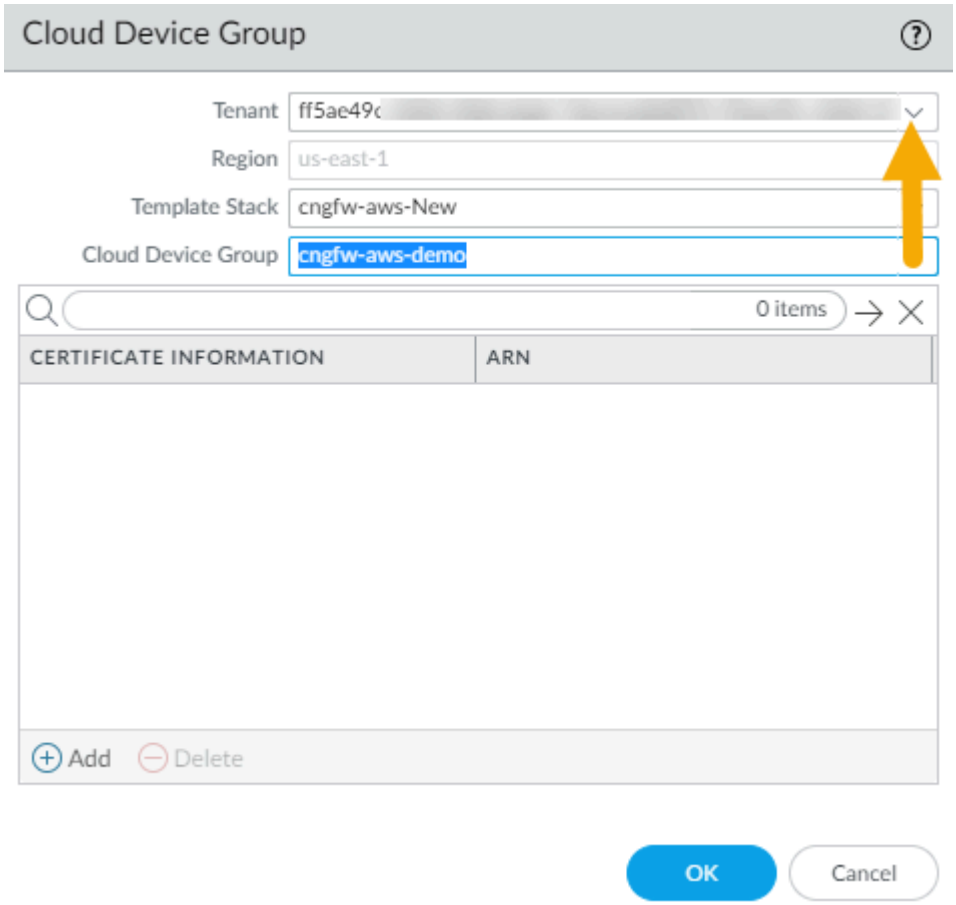
**STEP 2 |** Klicken Sie unten links auf **Add (Hinzufügen)**.



**STEP 3 |** Wählen Sie im Bildschirm **Cloud Device Group (Cloud-Gerätegruppe)** über das Dropdown-Menü den zu verwendenden **Mandanten** aus.

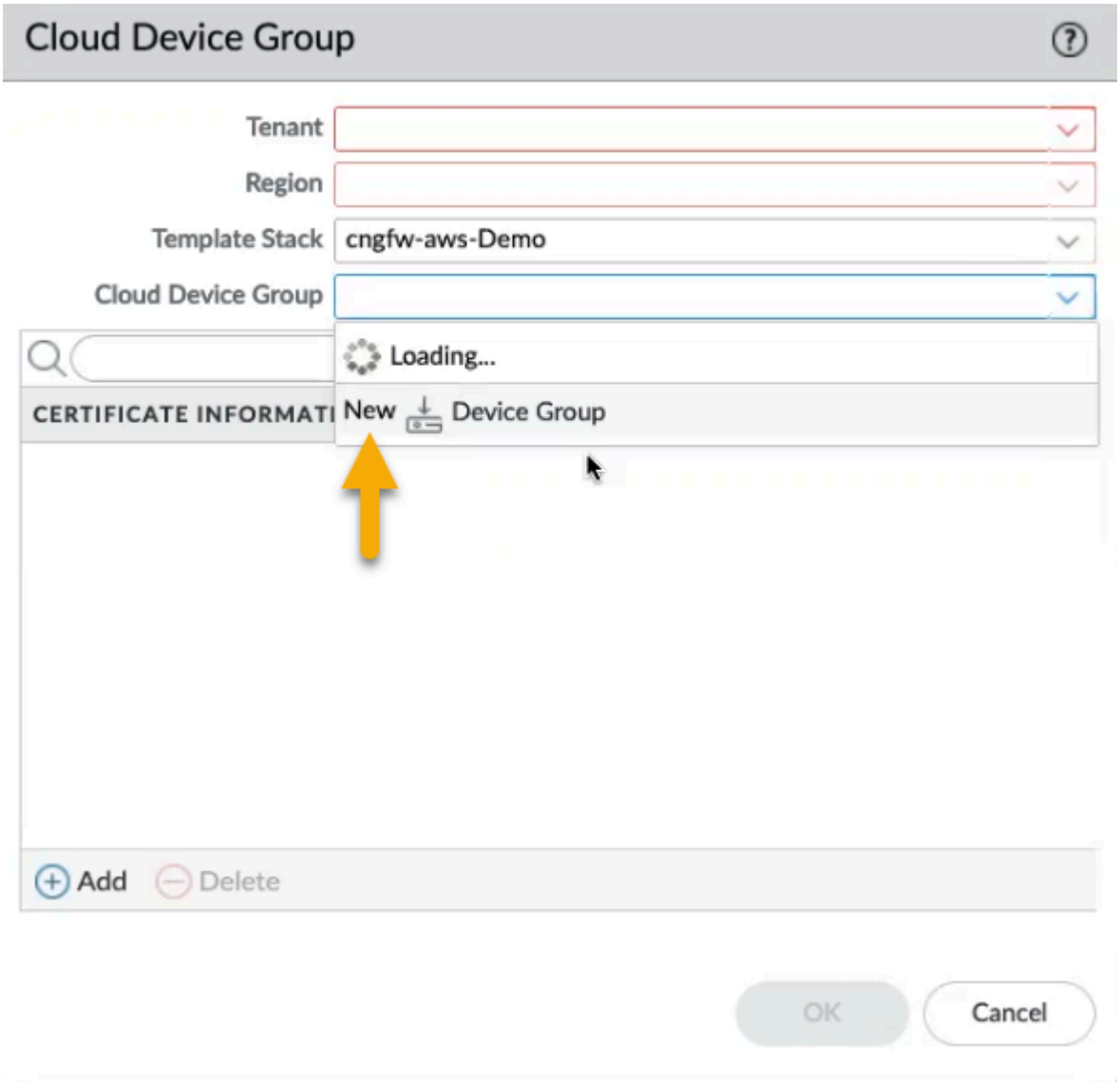



Die **Region** wird automatisch mit der Region gefüllt, in der sich der Mandant befindet.

**STEP 4 |** Erstellen Sie einen neuen **Vorlagenstack**, oder verwenden Sie das Dropdown-Menü, um einen vorhandenen Vorlagenstack auszuwählen.

**STEP 5 |** Wählen Sie das Dropdown-Menü **Cloud Device Group (Cloud-Gerätegruppe)** aus und klicken Sie auf **New (Neu)**:




**STEP 6 |** Geben Sie einen **Gerätegruppennamen** für die Gerätegruppe ein und klicken Sie auf **Create (Erstellen)**.

**STEP 7 |** Klicken Sie auf **OK**, um die Cloud-Gerätegruppe auf den Mandanten anzuwenden.

**STEP 8 |** Sie können ein natives Panorama-Zertifikat zuordnen oder eine ARN-Zuordnung angeben. Nach dem Hinzufügen eines Zertifikats zu Cloud NGFW für AWS geben Sie den Namen des Zertifikats ein und geben Sie alternativ die ARN-Zuordnung an.

**STEP 9 |** Führen Sie einen Commit für die Änderung aus.

## Cloud-Gerätegruppe aus einer Ressource löschen

Verwenden Sie die Panorama-Konsole, um eine Cloud-Gerätegruppe zu löschen. Sie können eine Cloud-Gerätegruppe nur löschen, wenn ihr keine Firewalls zugeordnet sind.

So löschen Sie eine Cloud-Gerätegruppe mithilfe der Panorama-Konsole:

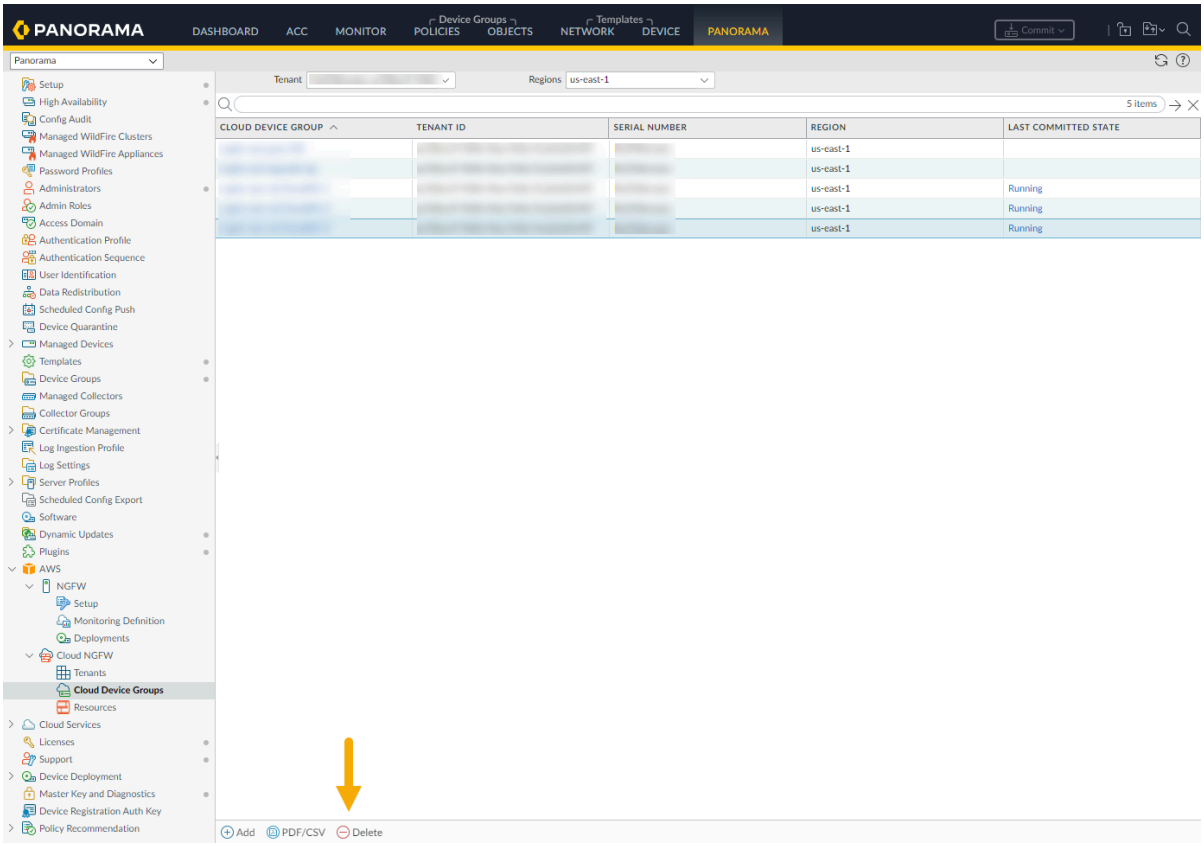
**STEP 1 |** Wählen Sie in **Panorama** die Option **Cloud Device Groups (Cloud-Gerätegruppen)** aus.

**STEP 2 |** Wählen Sie die **Cloud Device Group (Cloud-Gerätegruppe)** aus, die Sie entfernen möchten.

**STEP 3 |** Klicken Sie im unteren Bereich der Panorama-Konsole auf **Delete (Löschen)**.



**STEP 4 |** Klicken Sie auf **Yes (Ja)**, um den Löschvorgang zu bestätigen.

**STEP 5 |** Führen Sie einen Commit für die Änderung aus.

## Cloud-Gerätegruppe einer Ressource zuordnen

Verwenden Sie die Panorama-Konsole, um eine Cloud-Gerätegruppe einer Cloud NGFW-Ressource zuzuordnen. Sie können eine Cloud-Gerätegruppe per Push übertragen, ohne sie einer Ressource zuzuordnen. Sie müssen die Cloud-Gerätegruppe jedoch zuordnen, wenn die Ressource die Cloud-Gerätegruppenkonfiguration verwenden soll.

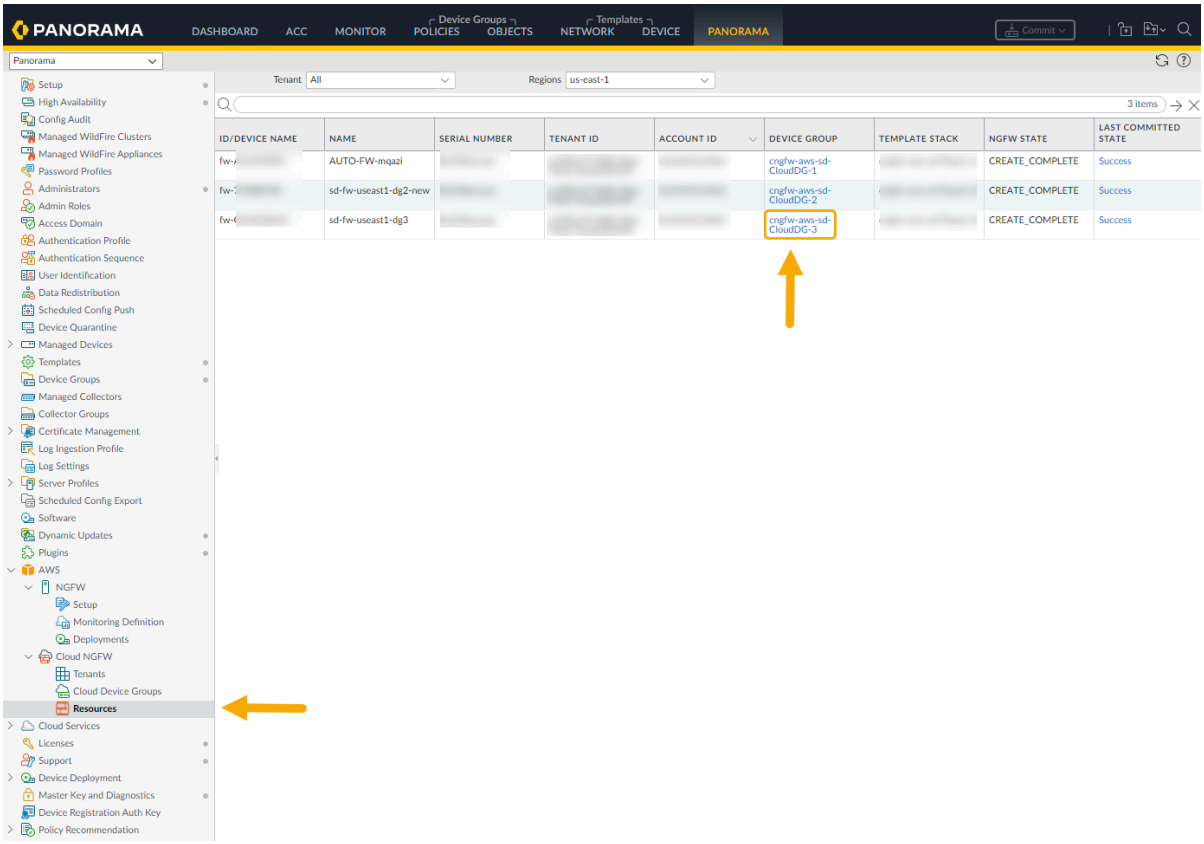
So ordnen Sie eine Cloud-Gerätegruppe mithilfe der Panorama-Konsole einer Cloud NGFW-Ressource zu:

**STEP 1 |** Wählen Sie in **Panorama** die Option **Resources (Ressourcen)** aus.

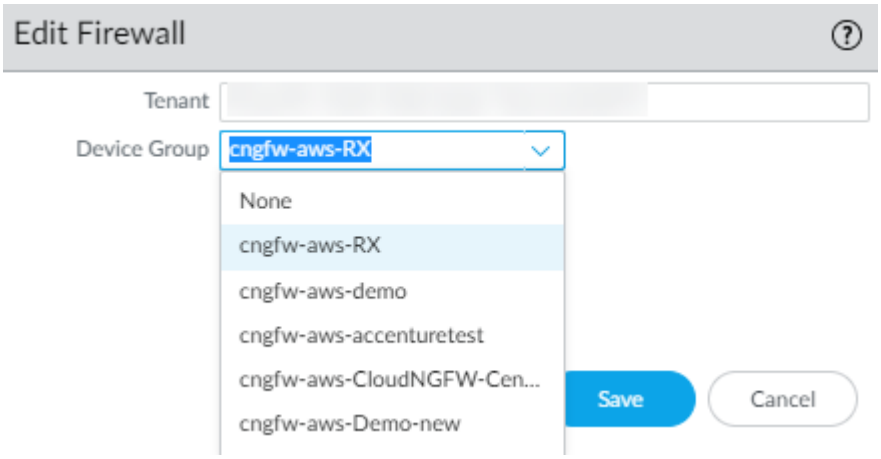
**STEP 2 |** Wählen Sie die **Gerätegruppe** aus.



**STEP 3 |** Wählen Sie im Bildschirm **Edit Firewall (Firewall bearbeiten)** im Dropdown-Menü die Cloud-Gerätegruppe aus, die Sie der Cloud NGFW-Ressource zuordnen möchten.




**STEP 4 |** Klicken Sie auf **Save (Speichern)**.

**STEP 5 |** Führen Sie einen **Commit** für die Änderungen aus.

**STEP 6 |** Übertragen Sie die Änderungen per **Push** auf Ihr Gerät.

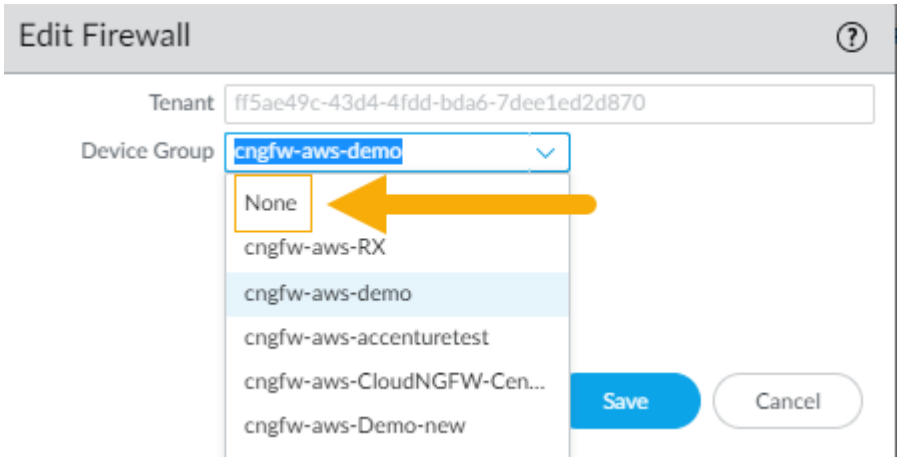
## Zuordnung einer Cloud-Gerätegruppe zu einer Ressource aufheben

So heben Sie die Zuordnung einer Cloud-Gerätegruppe zu einer Cloud NGFW-Ressource mithilfe der Panorama-Konsole auf:

**STEP 1 |** Wählen Sie in **Panorama** die Option **Resources (Ressourcen)** aus.

**STEP 2 |** Wählen Sie die **Gerätegruppe** der NGFW-Ressource aus.

**STEP 3 |** Wählen Sie im Bildschirm **Edit Firewall (Firewall bearbeiten)** aus der Dropdown-Liste **Device Group (Gerätegruppe)** die Option **None (Keine)** aus. Klicken Sie auf **Save (Speichern)**.




## Richtlinie anwenden

Cloud-Gerätegruppen auf Panorama ermöglichen Ihnen die zentrale Verwaltung von Firewall-Richtlinien. Sie erstellen Richtlinien auf Panorama entweder als Vor-Regeln oder Nach-Regeln. Vor-Regeln und Nach-

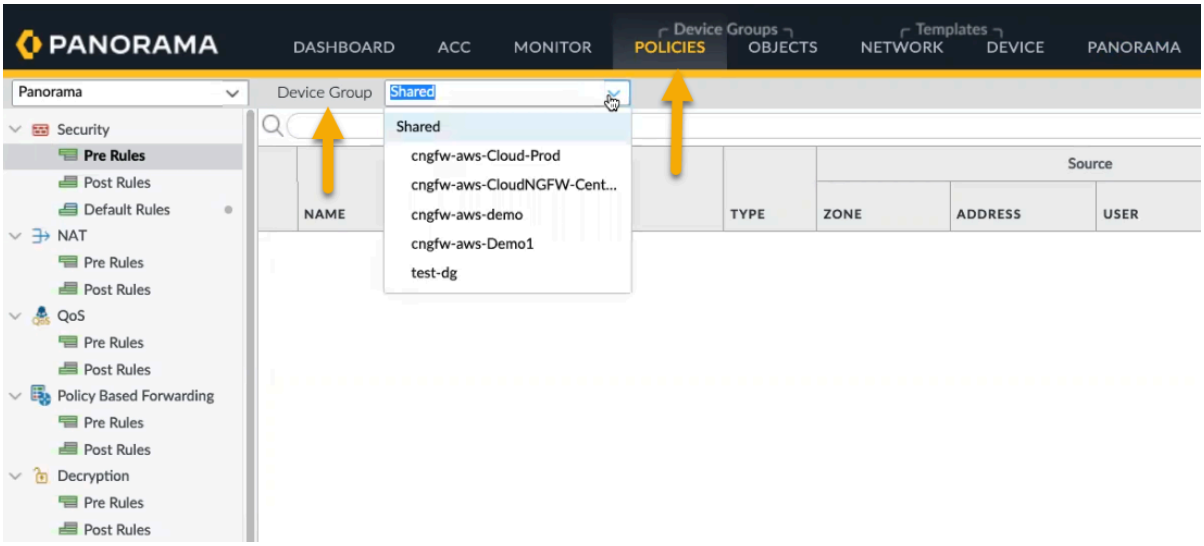
Regeln ermöglichen Ihnen einen mehrschichtigen Ansatz zur Implementierung von Richtlinien. Weitere Informationen finden Sie unter Richtlinien auf Panorama definieren.

*Eine auf Panorama erstellte Richtlinie erstellt einen globalen Regelstapel. Für eine Firewall können Regeln nicht sowohl auf Panorama noch auf dem Mandanten generiert werden. Regeln müssen entweder in Cloud NGFW oder Panorama erstellt werden.*

So konfigurieren Sie Richtlinien für die Cloud-Gerätegruppe in Panorama:

**STEP 1 |** Wählen Sie **Policies (Richtlinien)** aus.

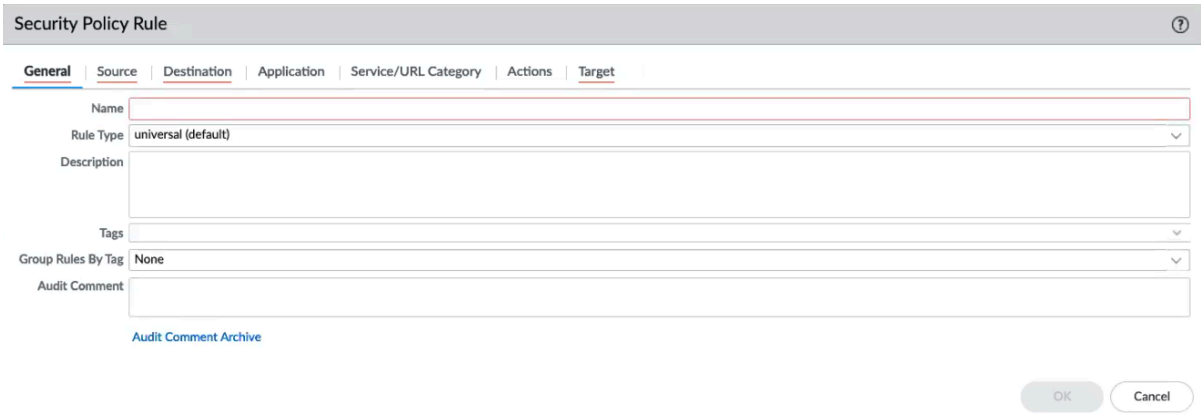
**STEP 2 |** Wählen Sie im Abschnitt **Device Group (Gerätegruppe)** über das Dropdown-Menü die zuvor erstellte **Cloud-Gerätegruppe** aus. Wenn Sie eine Gerätegruppe für Cloud NGFW erstellen, beginnt der Name mit *cngfw*. Beispiel: *cngfw-aws-demo*.




**STEP 3 |** Klicken Sie unten links in der Konsole auf **Add (Hinzufügen)**.

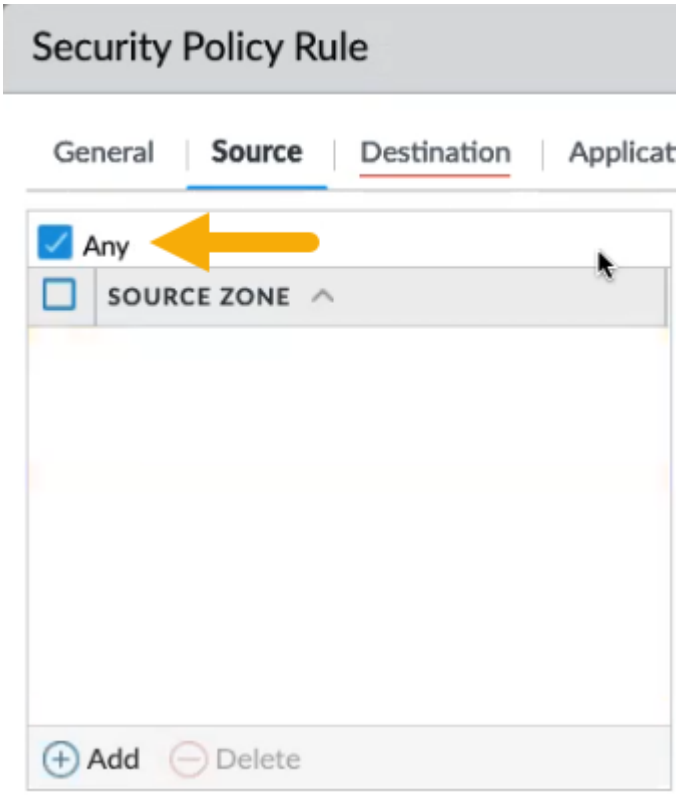
**STEP 4 |** Konfigurieren Sie im Bildschirm Security Policy Rule (Sicherheitsrichtlinienregel) die Elemente der Richtlinie, die Sie auf die Gerätegruppe anwenden möchten:




**STEP 5 |** Geben Sie auf der Registerkarte **General (Allgemein)** einen **Namen** für die Richtlinie ein.

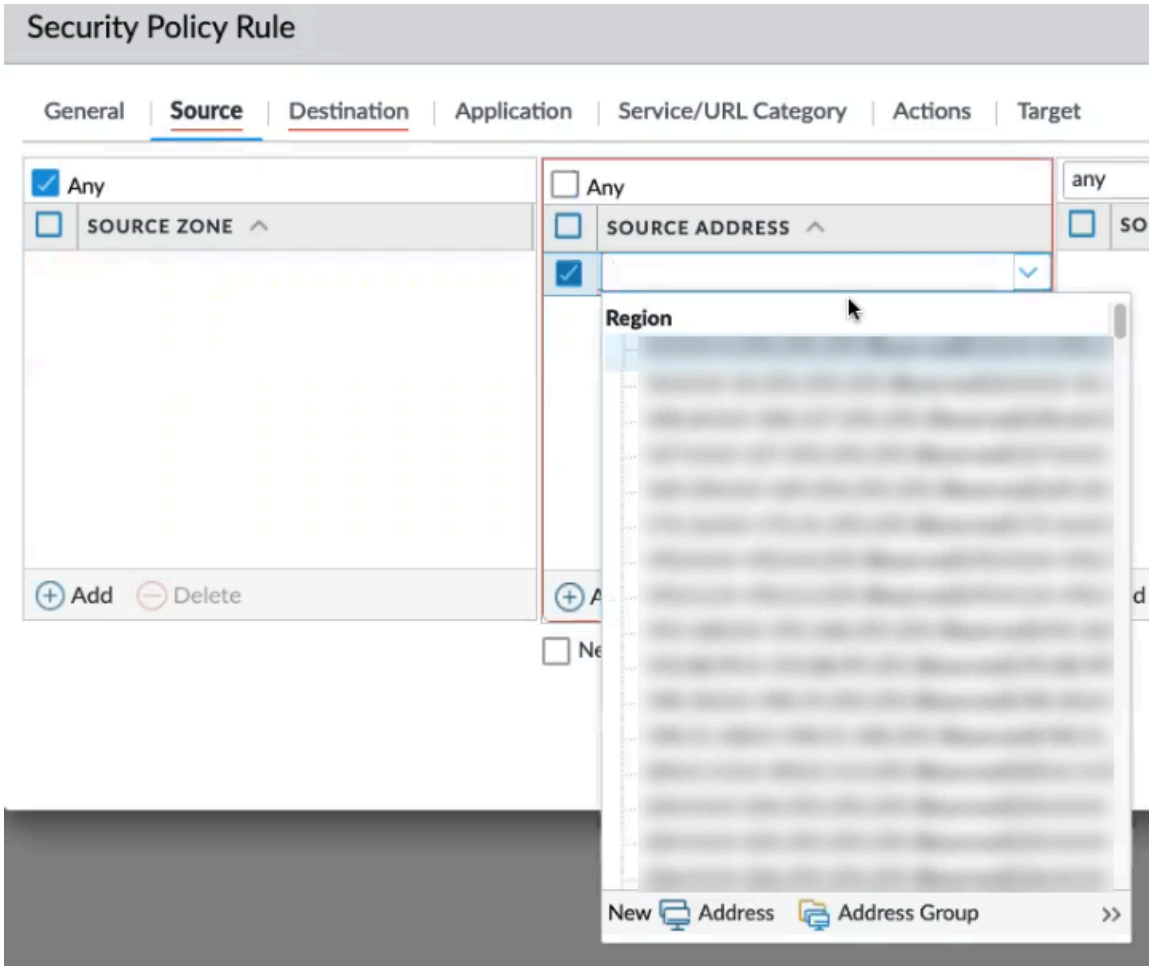
**STEP 6 |** Konfigurieren Sie auf der Registerkarte **Source (Quelle)** eine Quellrichtlinie. Die **Quellrichtlinie** definiert die Quellzone oder Quelladresse, von der der Datenverkehr ausgeht. Klicken Sie für **Source Zone (Quellzone)** auf **Any (Beliebig)**. Sie können keine spezifische Quelladresse hinzufügen.




1. Fahren Sie mit der Anwendung der **Quellrichtlinien** fort, indem Sie die **Quelladresse** einschließen. Klicken Sie auf **Any (Beliebig)** oder verwenden Sie das Dropdown-Menü, um eine

vorhandene Adresse auszuwählen, oder verwenden Sie die entsprechenden Optionen, um eine neue Adresse oder Adressgruppe hinzuzufügen.



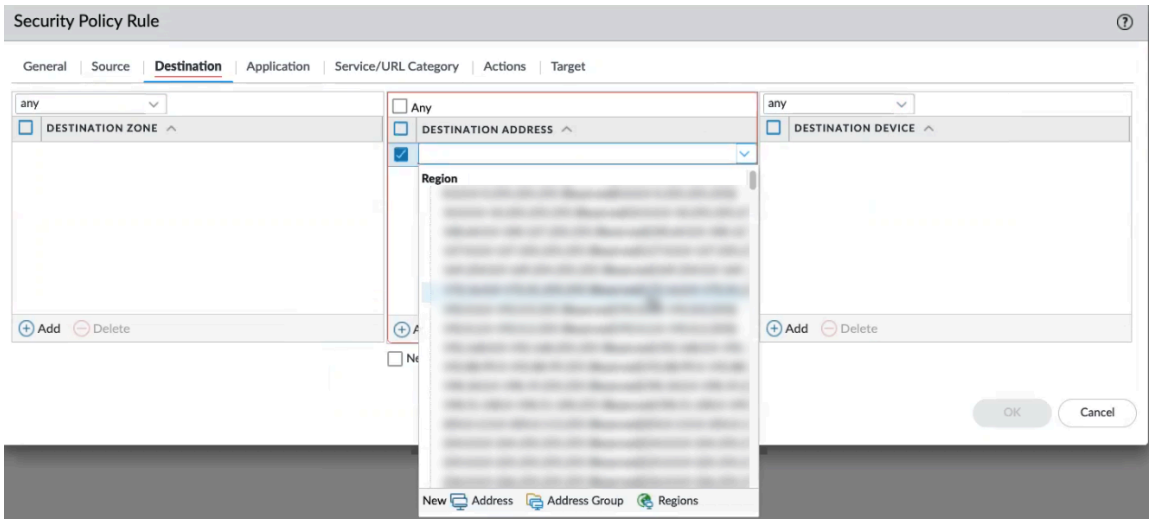

2. Klicken Sie für die Richtlinien **Source User (Quellbenutzer)** und **Source Device (Quellgerät)** auf **Any (Beliebig)**. In Cloud NGFW wird die Angabe bestimmter Quellbenutzer oder Quellgeräte nicht unterstützt

**STEP 7 |** Die **Zielrichtlinie** definiert die Zielzone oder Zieladresse für den Datenverkehr. Verwenden Sie das Dropdown-Menü, um eine vorhandene Adresse auszuwählen, oder verwenden Sie die Optionen, um eine neue Adresse oder Adressgruppe hinzuzufügen. Die Zielrichtlinie umfasst Felder für Zone, Adresse und Gerät.

1. Klicken Sie für **Destination Zone (Zielzone)** auf **Any (Beliebig)**. Cloud NGFW unterstützt das Hinzufügen einzelner Zielzonen nicht.

2. Klicken Sie für **Destination Address (Zieladresse)** auf **Any (Beliebig)** oder verwenden Sie das Dropdown-Menü, um eine vorhandene Zone auszuwählen. Klicken Sie auf **New (Neu)**, um eine neue Adresse, Adressgruppe oder Region hinzuzufügen.
3. Klicken Sie für **Destination Device** auf **Any**. Cloud NGFW unterstützt das Hinzufügen einzelner Zielgeräte nicht.

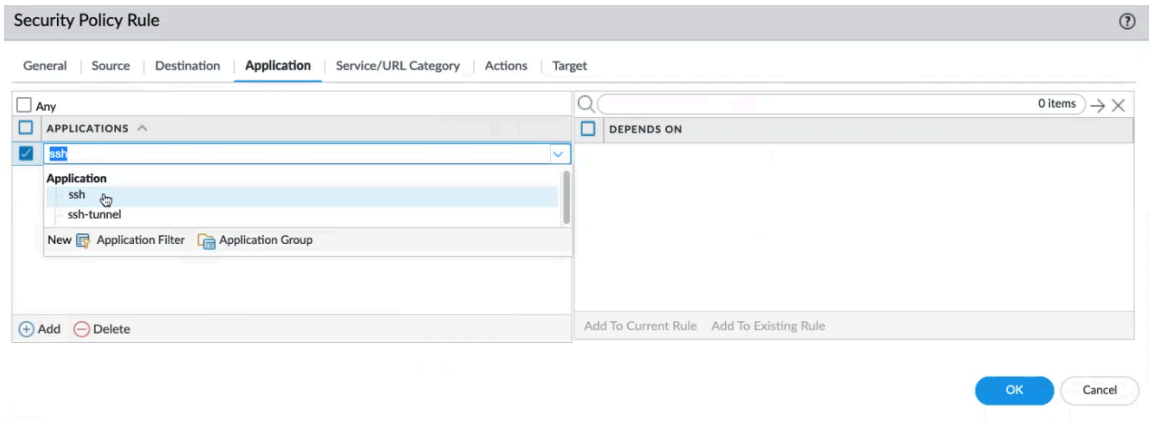



**STEP 8 |** Konfigurieren Sie die Richtlinie vom Typ **Application (Anwendung)** so, dass die Richtlinienaktion basierend auf einer Anwendung oder Anwendungsgruppe ausgeführt wird. Ein Administrator kann auch eine vorhandene App-ID™-Signatur verwenden und sie anpassen, um proprietäre Anwendungen

oder bestimmte Attribute einer vorhandenen Anwendung zu erkennen. Benutzerdefinierte Anwendungen werden in **ObjectsApplications** definiert.

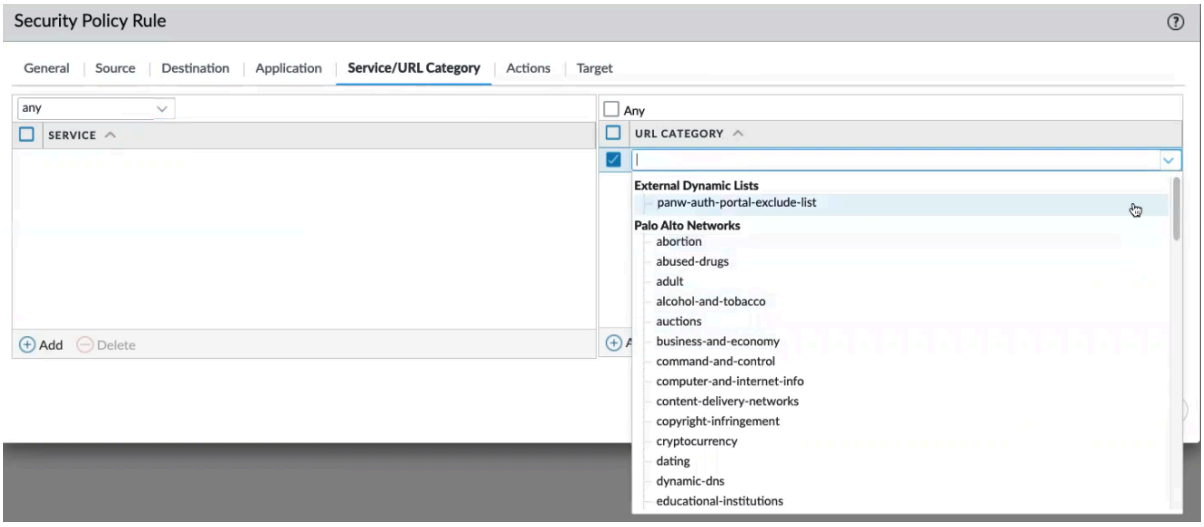
1. Klicken Sie im Bildschirm **Application (Anwendung)** auf **Any (Beliebig)** oder geben Sie eine bestimmte Anwendung an, beispielsweise SSH. Klicken Sie auf **Add (Hinzufügen)**, um eine neue Anwendungsrichtlinie einzuschließen:




**STEP 9 |** Konfigurieren Sie unter **Service/URL Category (Dienst-/URL-Kategorie)** Dienst-/URL-Kategorie-Richtlinien für die Firewall, um eine bestimmte TCP- und/oder UDP-Portnummer oder eine URL-Kategorie als Übereinstimmungskriterium in der Richtlinie anzugeben. Geben Sie Richtlinien auf **Dienstebene** oder **URL-Kategorie**-Richtlinien an, indem Sie **Any (Beliebig)** auswählen, oder verwenden Sie die Optionen im Dropdown-Menü, um die Richtlinienelemente, die Sie anwenden

möchten, einzeln auszuwählen. Klicken Sie auf **Add (Hinzufügen)**, um neue Richtlinien für den Dienst oder die URL/Kategorie zu erstellen.




**STEP 10 |** Konfigurieren Sie unter **Actions (Aktionen)** eine Aktionsrichtlinie, um die auszuführende Aktion basierend auf Datenverkehr zu bestimmen, der den definierten Richtlinienattributen entspricht.

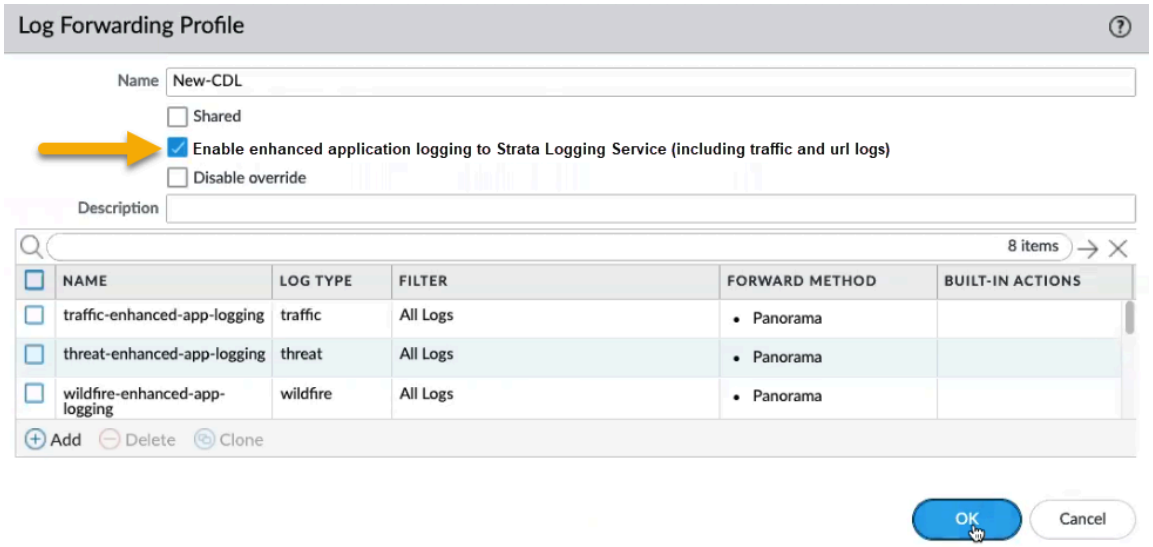
1. Wählen Sie im Bildschirm **Actions (Aktionen)** die auszuführende Aktion aus, z. B. „Allow“ (Zulassen) oder „Deny“ (Verweigern), legen Sie die **Profileinstellung** fest, konfigurieren Sie die **Protokolleinstellung** und weitere Einstellungen.

   Informationen zur Verwendung von Panorama-Protokollen finden Sie unter Zentralisierte Protokollierung und Berichterstattung und Protokolle anzeigen

2. Sie können Protokolle optional über den Bildschirm **Security Policy Rule (Sicherheitsrichtlinienregel)** an den Strata-Protokollierungsdienst weiterleiten. Wählen Sie im Feld **Log Setting (Protokolleinstellungen)** die Dropdown-Liste **Log Forwarding (Protokollweiterleitung)** aus und klicken Sie auf **New Profile (Neues Profil)**. Geben Sie im Protokollweiterleitungsprofil einen **Namen** für das Protokoll ein und wählen Sie **Enable enhanced application logging to Strata Logging Service (including traffic and url logs)**

**(Erweiterte Anwendungsprotokollierung für Strata-Protokollierungsdienst aktivieren (einschließlich Datenverkehrs- und URL-Protokolle))** aus. Klicken Sie auf **OK**.



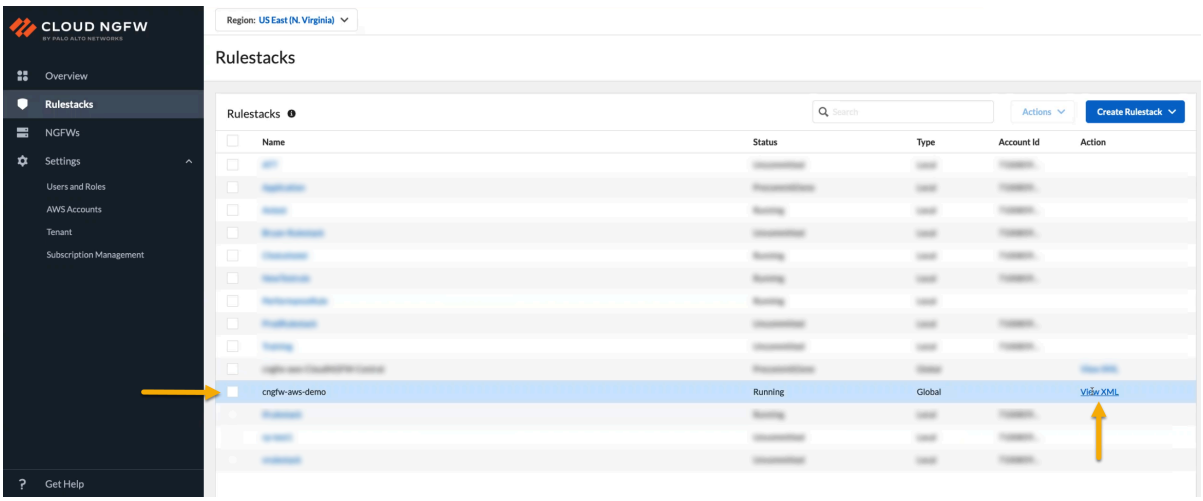

Weitere Informationen zum Strata-Protokollierungsdienst finden Sie unter Protokolle erkunden.

**STEP 11 |** Kehren Sie zur Cloud NGFW-Konsole zurück, um in Panorama erstellte Regeln anzuzeigen. Klicken Sie auf **View XML (XML anzeigen)**, um Informationen zu den Regeln anzuzeigen, die

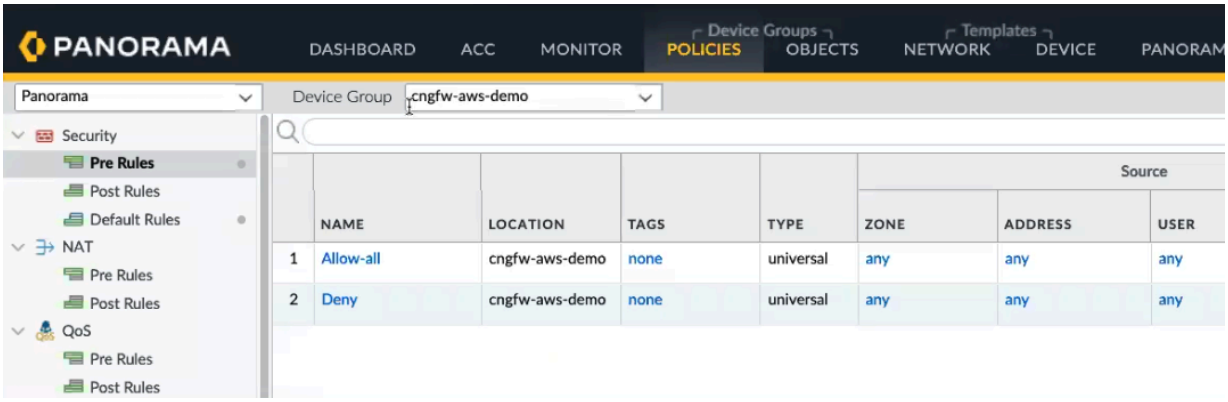
von Panorama in den globalen Regelstapel übertragen wurden, der auf die Cloud-Gerätegruppe angewendet wird:



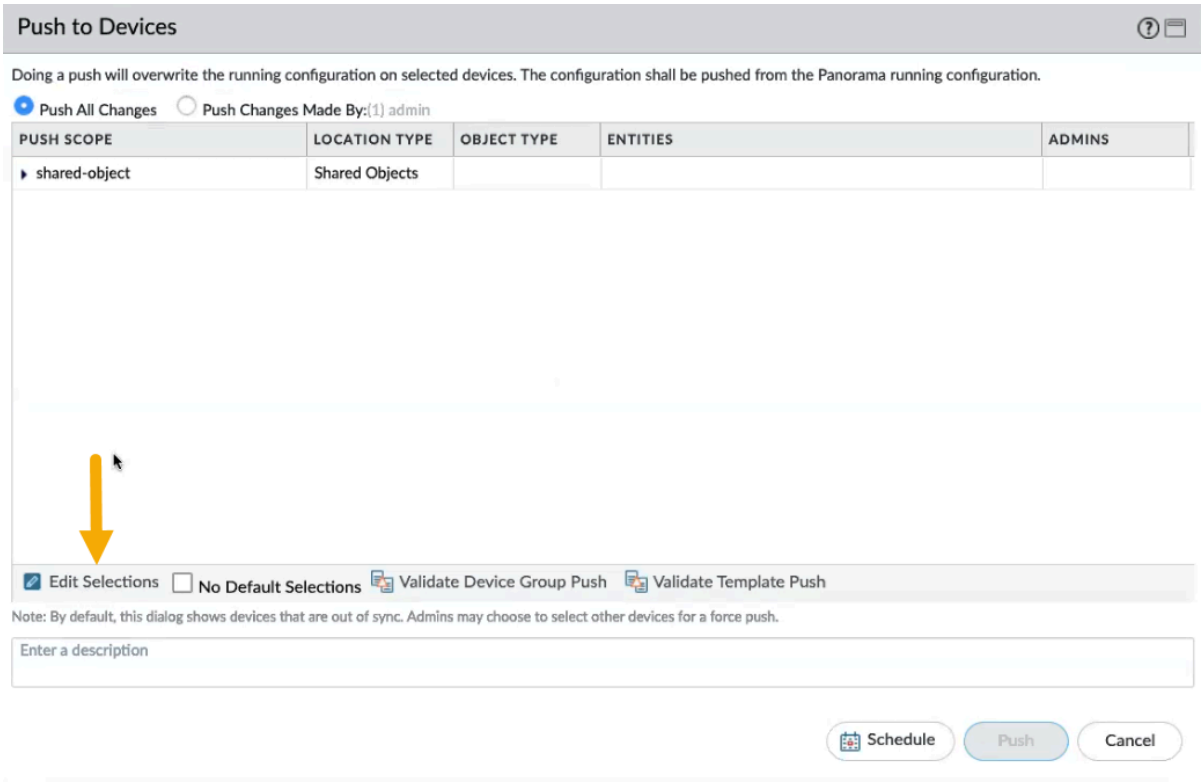
Der Regelstapel ist jetzt den Richtlinien zugeordnet, die auf die in Panorama erstellte Cloud-Gerätegruppe angewendet werden:




**STEP 12 |** Nachdem Sie Richtlinien auf die Cloud-Gerätegruppe für den Cloud NGFW-Mandanten angewendet haben, übertragen Sie die Änderungen per Push in die Panorama-Konsole.

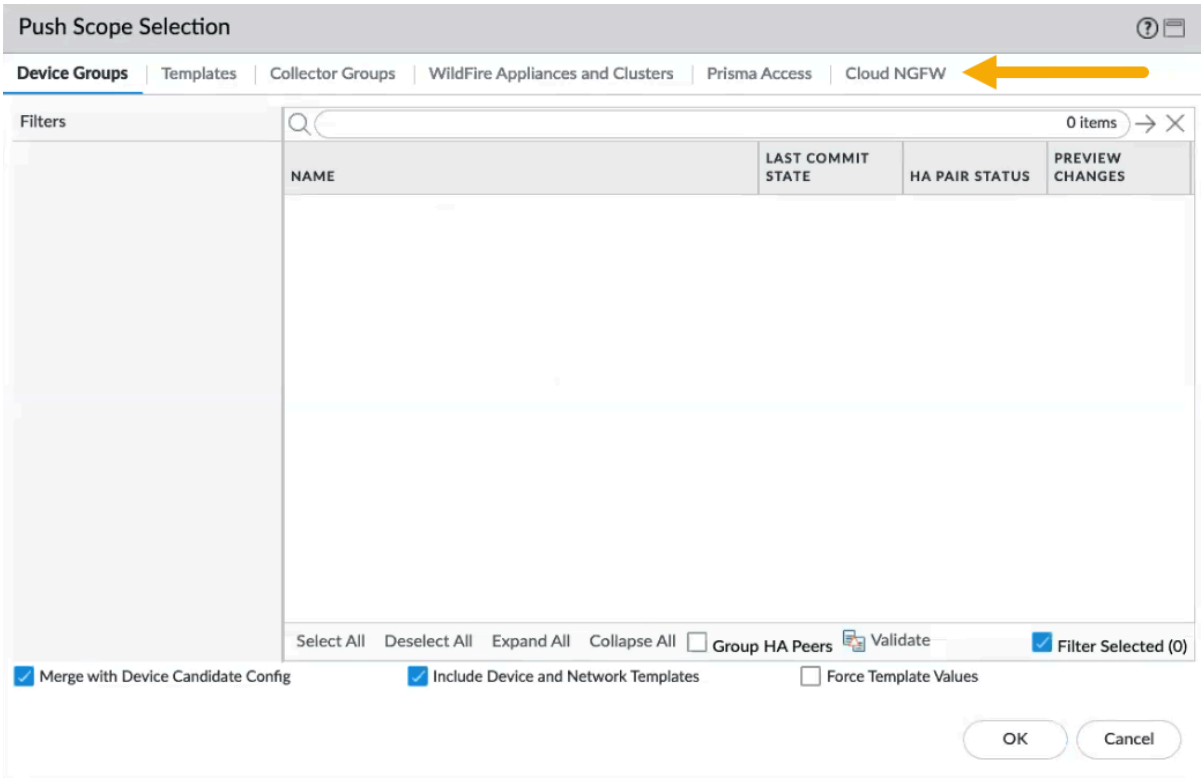
**STEP 13 |** Klicken Sie im Bildschirm **Push to Devices (Per Push auf Geräte übertragen)** auf **Edit Selections (Auswahl bearbeiten)**.




**STEP 14 |** Klicken Sie im Bildschirm **Push Scope Selection (Auswahl des Übertragungsumfangs)** auf **Cloud NGFW**. Der **Cloud NGFW**-Knoten wurde dem Bildschirm **Push Scope Selection (Auswahl des**

**Übertragungsumfangs)** hinzugefügt, um die Integration von Cloud NGFW und Panorama zu erleichtern.




**STEP 15 |** Wählen Sie die Cloud-Gerätegruppen aus, die Sie per Push an die Ressourcen übertragen möchten, klicken Sie auf **OK** und anschließend auf **Push (Per Push übertragen)**.

## Eine von Panorama per Push übertragene Gerätegruppe verwenden

Die Informationen in diesem Abschnitt richten sich an Benutzer, die den AWS Firewall Manager Service (FMS) zum Konfigurieren von Gerätegruppen verwenden, die von Panorama per Push übertragen wurden.

*Wenn Sie FMS verwenden, können Sie eine Cloud-Gerätegruppe nicht der Cloud NGFW von Panorama zuordnen. Die entsprechende Option ist in der Panorama-Konsole ausgegraut. Verwenden Sie die FMS AWS-Konsole, um diese Zuordnung zu erstellen.*

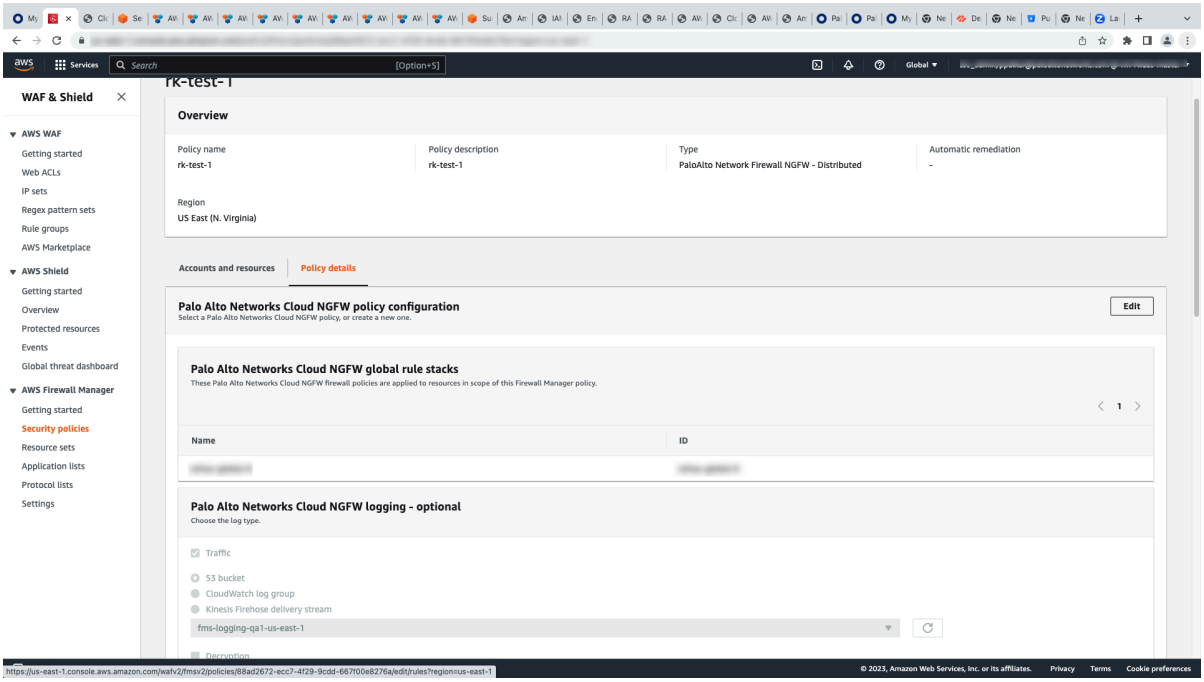
**STEP 1 |** Verknüpfen Sie einen Mandanten mit Panorama.

**STEP 2 |** Erstellen Sie eine Cloud-Gerätegruppe und übertragen Sie sie per Push an die Cloud NGFW. Benutzer, die FMS nicht verwenden, müssen genauso vorgehen.

**STEP 3 |** Navigieren Sie zur FMS AWS-Konsole und bearbeiten Sie die Richtlinie.

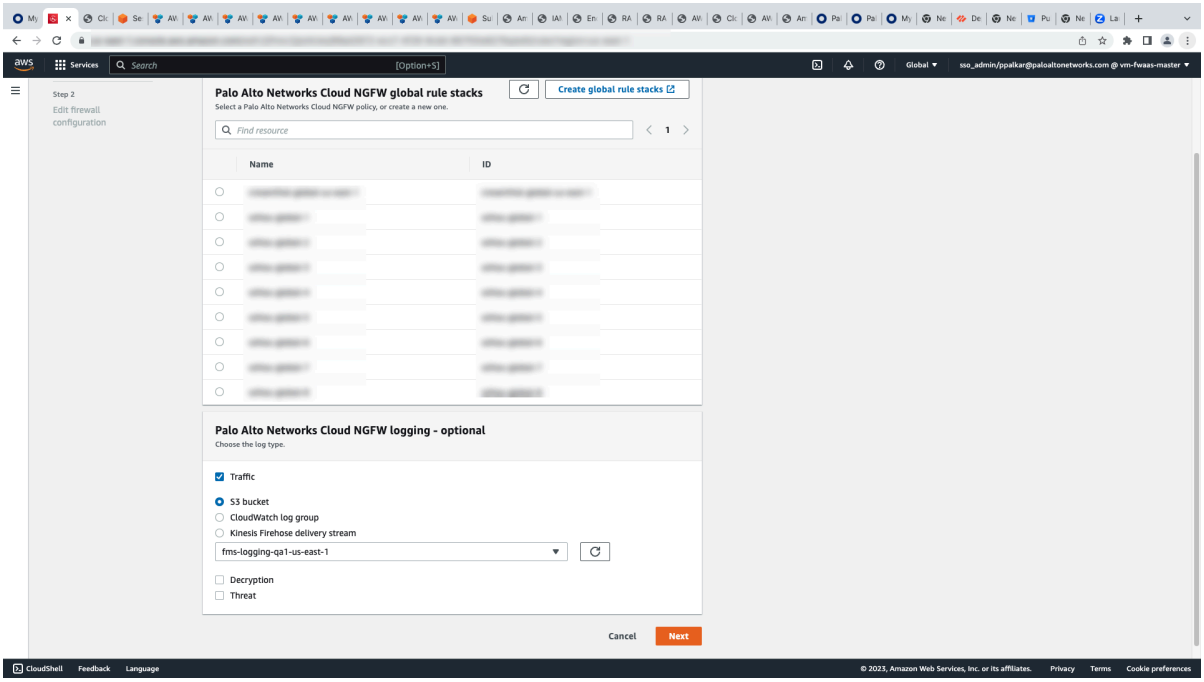
 



**STEP 4 |** Wählen Sie den globalen Regelstapel aus, der von Panorama per Push übertragen wurde.



**STEP 5 |** Speichern Sie Ihre Änderungen.

## Verwenden mehrerer Panorama-Instanzen mit Ihrer Cloud NGFW-Ressource

So verwenden Sie mehrere Panorama-Instanzen mit derselben Cloud NGFW-Ressource

**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Wählen Sie **Integrations (Integrationen)** aus. Auf der Seite **Integrations (Integrationen)** werden Informationen zur aktuell verknüpften Panorama-Instanz angezeigt. Wenn eine Panorama-Instanz derzeit nicht mit einem Cloud NGFW-Mandanten verknüpft ist, ist diese Seite leer.

**STEP 3 |** Klicken Sie auf der Seite **Panoramas** auf **Add Panorama (Panorama hinzufügen)**.

**STEP 4 |** Geben Sie im Fenster **Add Panorama (Panorama hinzufügen)** einen **Verknüpfungsnamen** ein. Wählen Sie im Dropdown-Menü die **primäre Panorama-Seriennummer** aus.

Im Fenster **Add Panorama (Panorama hinzufügen)** werden neben jeder Panorama-Instanz, auf die Ihr Cloud NGFW-Mandant zugreifen kann, Symbole angezeigt. Diese Symbole geben an, ob die Panorama-Lizenz mit dem Strata-Protokollierungsdienst verknüpft ist. Weitere Informationen finden Sie unter Cloud NGFW mit Palo Alto Networks Management verknüpfen.

**STEP 5 |** Wählen Sie die sekundäre **Panorama-Seriennummer für das HA-Paar** aus.

**STEP 6 |** Klicken Sie auf **Continue (Weiter)**.

**STEP 7 |** Es wird eine **Benachrichtigung** angezeigt, die angibt, dass der Verknüpfungsvorgang abgeschlossen ist. Klicken Sie auf **Confirm (Bestätigen)**.

Auf der Seite **Integrations (Integrationen)** wird jetzt die mit dem Cloud NGFW-Mandanten verknüpfte Panorama-Instanz angezeigt. Klicken Sie auf die **Verknüpfungs-ID**, um Informationen anzuzeigen oder den Namen der Verknüpfung zu ändern. Klicken Sie auf **Save (Speichern)**, wenn Sie den Namen des Links ändern.

**STEP 8 |** Wählen Sie in der Cloud NGFW-Konsole **NGFWs** aus, um bereitgestellte Firewalls anzuzeigen.

Wählen Sie im oberen linken Bereich der Cloud NGFW-Konsole aus der Dropdown-Liste die **Region** aus, in der sich die Firewall befindet.

**STEP 9 |** Wählen Sie die Firewall aus, die Sie mit Panorama verwalten möchten.

**STEP 10 |** Klicken Sie auf die Registerkarte **Firewall Settings (Firewall-Einstellungen)**.

**STEP 11 |** Scrollen Sie nach unten zum Abschnitt **Policy Management (Richtlinienverwaltung)** und wählen Sie **Panorama** aus.

**STEP 12 |** Wählen Sie im Dropdown-Menü die **verknüpfte Panorama-Instanz** aus.

**STEP 13 |** Klicken Sie auf **Save (Speichern)**.

**STEP 14 |** Wiederholen Sie die Schritte 8 bis 13, um eine andere Panorama-Instanz für einen anderen NGFW-Mandanten zu verwalten.

**STEP 15 |** Klicken Sie auf **Integrations (Integrationen)**, um eine andere Panorama-Instanz zu verknüpfen.

**STEP 16 |** Klicken Sie auf der Seite **Panoramas** auf **Add Panorama (Panorama hinzufügen)**.

**STEP 17 |** Geben Sie im Fenster **Add Panorama (Panorama hinzufügen)** einen neuen **Verknüpfungsnamen** ein. Wählen Sie im Dropdown-Menü die **primäre Panorama-Seriennummer** aus.

**STEP 18 |** Wählen Sie die sekundäre **Panorama-Seriennummer für das HA-Paar** aus.

**STEP 19 |** Klicken Sie auf **Continue (Weiter)**.

**STEP 20 |** Es wird eine **Benachrichtigung** angezeigt, die angibt, dass der Verknüpfungsvorgang abgeschlossen ist. Klicken Sie auf **Confirm (Bestätigen)**.

Wenn Sie mehrere Panorama-Instanzen mit einem Cloud NGFW-Mandanten verknüpfen, werden diesem keine Regelstapel zugeordnet. Wenn Sie Panorama verwenden, um Cloud-Gerätegruppen per Push an die Firewall zu übertragen, ändert sich der Abschnitt **Rulestacks (Regelstapel)** auf der Seite der NGFWs, um die der NGFW zugeordnete Richtlinienverwaltung widerzuspiegeln.

**STEP 21 |** Es wird eine **Benachrichtigung** angezeigt, die angibt, dass der Verknüpfungsvorgang abgeschlossen ist. Klicken Sie auf **Confirm (Bestätigen)**.

# Tagbasierte Richtlinien konfigurieren

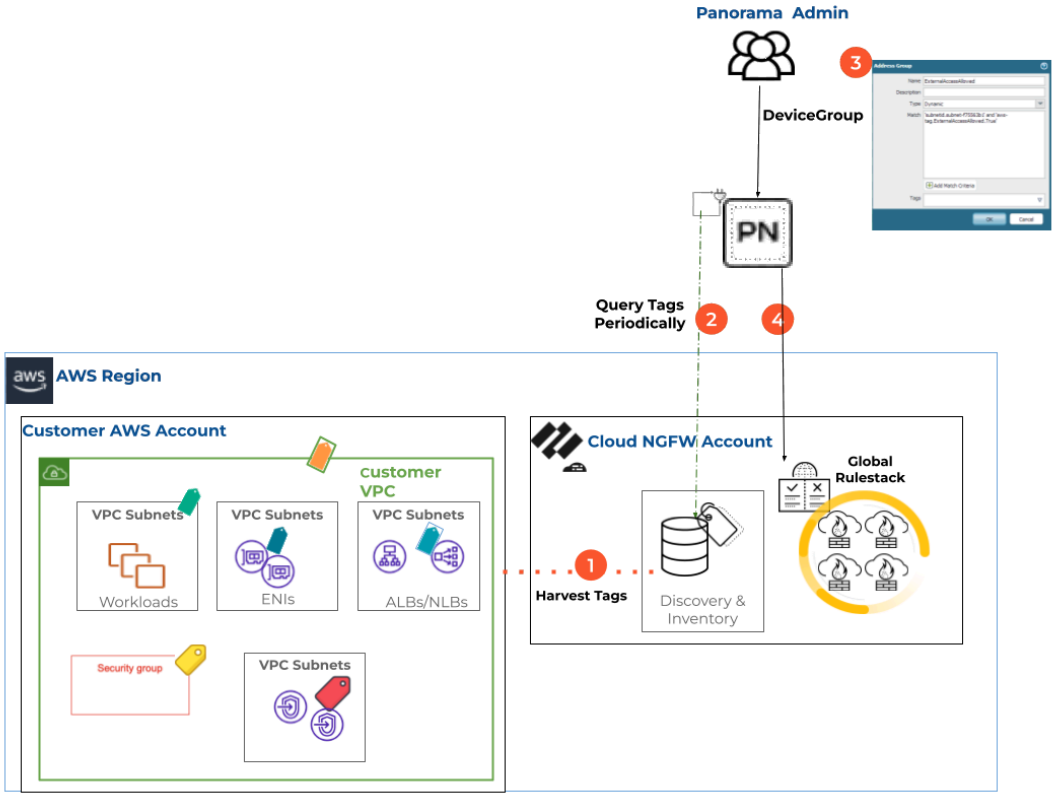
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Sie können die Sicherheitsrichtlinie für Ihre Palo Alto Networks Cloud NGFW-Ressourcen automatisch aktualisieren, sodass Sie den Datenverkehr zu diesen AWS-Assets absichern können, wenn Sie AWS-Assets (wie etwa EC2-Instanzen) in der öffentlichen AWS-Cloud bereitstellen oder beenden.

Um diese Funktion von Panorama aus zu aktivieren, müssen Sie das Panorama AWS-Plug-in so konfigurieren, dass es IPs/Tags abruft, die Ihr Cloud NGFW-Mandant von dem von Ihnen hinzugefügten AWS-Konto sammelt. Verwenden Sie dann das AWS Panorama-Plug-in, um diese Tags an die Cloud NGFW-Ressourcen zu übertragen, indem Sie die Überwachungsdefinition konfigurieren und sie den Gerätegruppen melden, die diesen Palo Alto Networks Firewalls entsprechen.

Sie können dann mithilfe von AWS-Ressourcentags Panorama Dynamic Address Group-Objekte in diesen Gerätegruppen erstellen. Wenn Sie in dynamischen Adressgruppen (Dynamic Address Groups, DAG) auf diese Tags verweisen und sie in Sicherheitsrichtlinienregeln mit ihnen abgleichen, können Sie die Richtlinie für alle in Ihren AWS-Konten bereitgestellten Assets konsistent durchsetzen.




### Voraussetzungen

Für die Aktivierung tagbasierter Richtlinienregeln für Cloud NGFW für AWS-Ressourcen gelten die folgenden Mindestsystemanforderungen:

- Installieren Sie das AWS-Plug-in, Version 5.1.0 oder höher, auf Ihrer Panorama-Instanz. Weitere Informationen finden Sie unter AWS-Plug-in installieren oder aktualisieren.
- Verwenden der Cloud NGFW-Konsole, um mit dieser AWS-Konten zu einem Cloud NGFW-Mandanten hinzuzufügen und Tags von diesen zu sammeln.
- Verwenden Sie das Panorama-Plug-in, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen.
- Konfigurieren Sie DAG-Objekte mit Tags in Gerätegruppen.

**Schlüsselkonzepte**

| Begriff | Definition |
|---|---|
| **Cloud-Asset-Tags** | Auf AWS-Ressourcen konfigurierte AWS-Tags. |
| **VPC-Gruppe** | Eine Reihe von AWS-VPCs von einem oder mehreren AWS-Konten. |
| **Überwachungsdefinition** | Ordnet eine VPC-Gruppe einer Benachrichtigungsgruppe zu. |
| **Benachrichtigungsgruppe** | Sie können eine Reihe von Panorama-Gerätegruppen zusammenfassen, die den gleichen Satz von Tags erfordern. |

Um tagbasierte Richtlinienregeln für Cloud NGFW für AWS-Ressourcen zu aktivieren, müssen Sie Ihre Panorama-Appliance für diese Integration vorbereiten, indem Sie das AWS-Plug-in der Version 5.1.0 oder höher installieren. Fügen Sie mithilfe der Cloud NGFW-Konsole Ihre AWS-Konten hinzu und sammeln Sie Tags aus den AWS-Ressourcen. Verwenden Sie dann das Panorama-Plug-in, um regelmäßig Tags von Ihrem Cloud NGFW-Mandanten abzufragen, und fügen Sie es den Panorama-Gerätegruppen hinzu, um DAG-Objekte und -Regeln zu verwalten.

So aktivieren Sie tagbasierte Cloud NGFW-Richtlinien in Ihrer Panorama-Appliance:

1. Fügen Sie AWS-Konten zum Cloud NGFW-Mandanten hinzu, um aus diesen Tags zu sammeln.
2. Verwenden Sie das Panorama-Plug-in, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen.
3. Konfigurieren Sie DAG-Objekte mit Tags in Gerätegruppen.

## AWS-Konten zum Cloud NGFW-Mandanten hinzufügen, um aus diesen Tags zu sammeln

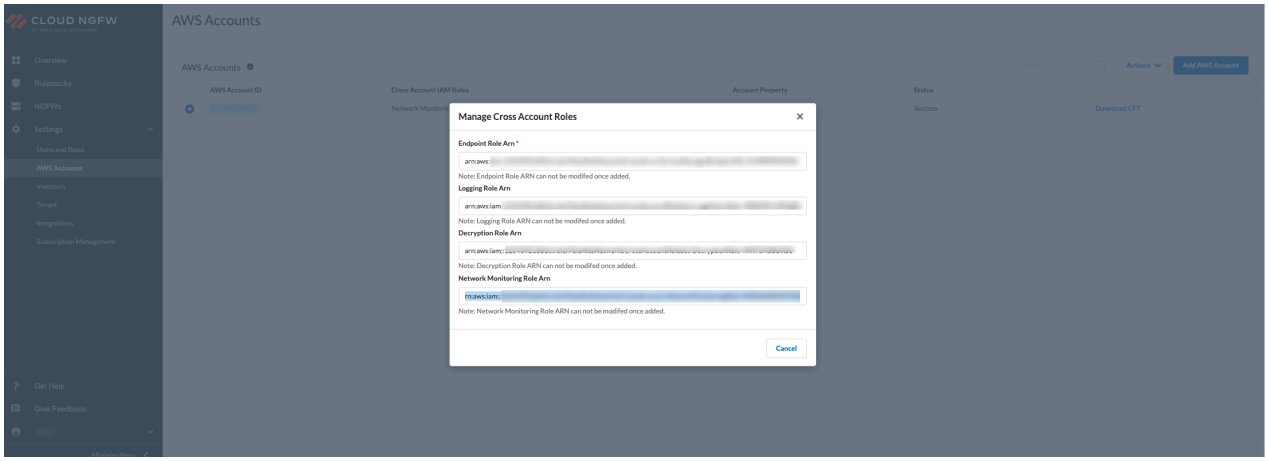
Binden Sie Ihr AWS-Konto in Ihren Cloud NGFW-Mandanten ein. Weitere Informationen finden Sie in **Schritt 10** unter Cloud NGFW-PAYG-SaaS-Abonnement.

Wenn Sie Ihr AWS-Konto bereits in den Cloud NGFW-Mandanten eingebunden haben, können Sie direkt mit dem Sammeln der Tags beginnen.

Der vorhandenen CloudFormation-Vorlage (CloudFormation Template, CFT) Ihres eingebundenen AWS-Kontos muss die Rolle `Network MonitoringRole Arn` hinzugefügt worden sein. Die Rolle

„Network Monitoring“ (Netzwerküberwachung) bietet Einblick in die Netzwerkleistung, die von AWS gehostete Anwendungen verbindet. Weitere Informationen finden Sie unter CloudFormation-Vorlage manuell hinzufügen.



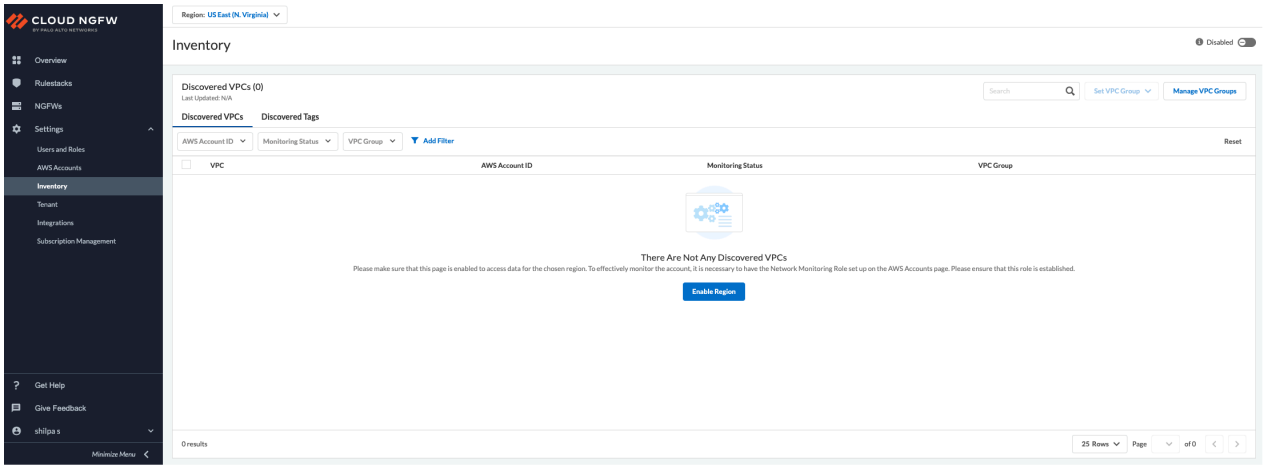
## Überwachung aktivieren

In der Cloud NGFW-Konsole können Sie die Erkennung von AWS-Ressourcentags für die gewünschten Regionen aktivieren. Cloud NGFW sammelt regelmäßig die folgenden Tags Ihrer AWS-Ressourcen (zum Beispiel: EC2, SG und LB) in verschiedenen AWS-Konten und registriert die Informationen bei Ihrem Cloud NGFW-Mandanten. Cloud NGFW zeigt die Ressourcentags für Ressourcen an, die nach VPCs in jedem AWS-Konto organisiert sind.

Zu diesem Zweck müssen Sie die Überwachung auf der Seite **Inventory (Inventar)** aktivieren, um auf die Daten für jede AWS-Region zuzugreifen und die Tagerkennung auszulösen.

Die Schaltfläche **Enable Region (Region aktivieren)** unter der Registerkarte **Discovered VPCs (Erkannte VPCs)** wird nur angezeigt, wenn Sie Ihr AWS-Konto zum ersten Mal einbinden. Wählen Sie aus der Dropdown-Liste die Option **Region** aus und klicken Sie auf **Enable Region (Region aktivieren)**, um die Tagüberwachung zu aktivieren.

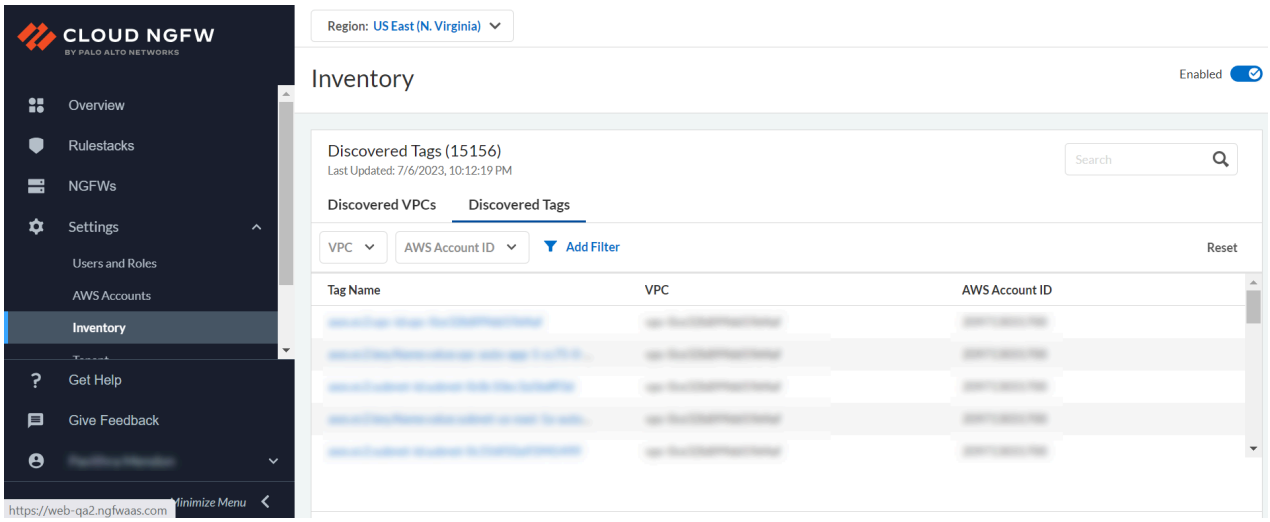
Alternativ können Sie aus der Dropdown-Liste auch eine **Region** auswählen und auf **Enable (Aktivieren)** klicken, um die Tagüberwachung zu aktivieren.



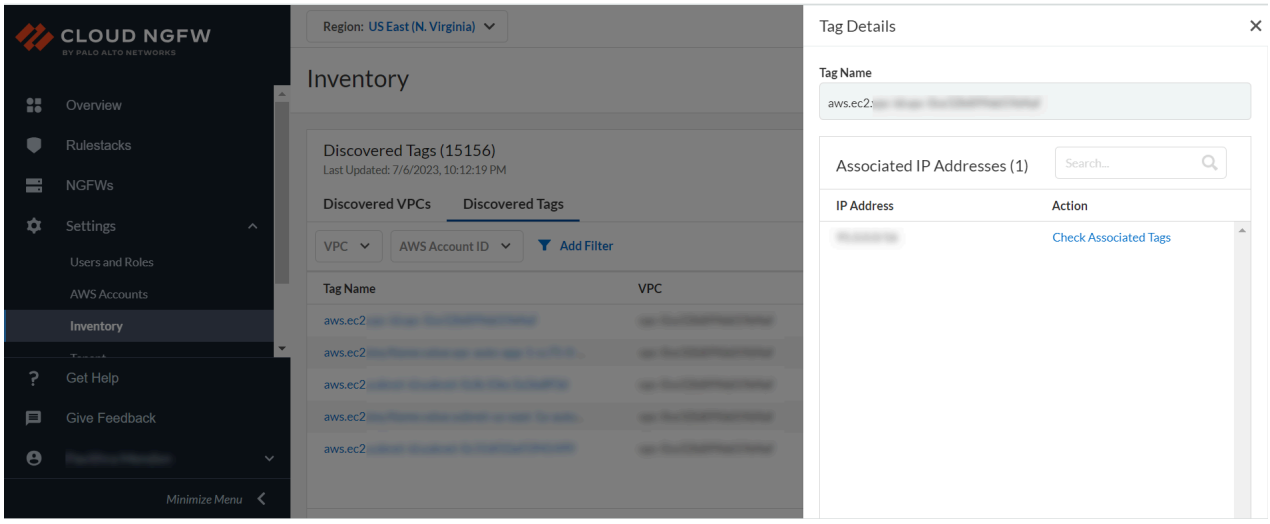
### Gesammelte Tags in der Cloud NGFW-Konsole anzeigen

Sie können die Gesamtzahl der erkannten Tags auf der Seite **Inventory (Inventar)** unter der Registerkarte **Discovered Tags (Erkannte Tags)** anzeigen.




Klicken Sie auf den **Tagnamen**, um die jedem Tag zugeordneten IPs aufzulisten.




Klicken Sie auf **Check Associated Tags (Zugeordnete Tags prüfen)**, um die der IP-Adresse zugeordneten Tags aufzulisten.

In der NGFW-Konsole können für ein Tag eines beliebigen AWS-Ressourcentyps (Schlüssel oder Wert kombiniert) maximal **127** Zeichen eingegeben werden. Die Tags, deren Schlüssel und Wert **mehr als 127** Zeichen aufweist, werden nicht zur Liste **DiscoveredTags (Erkannte Tags)** hinzugefügt. Weitere Informationen finden Sie unter Tageinschränkungen.

*Wenn Sie nicht über die **Inventaradministratorberechtigung** verfügen, können Sie weder eine **VPC-Gruppe festlegen** noch eine **neue VPC**-Gruppe erstellen.*

### *Panorama-Plug-in verwenden, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen*

Verwenden Sie das Panorama AWS-Plug-in, um Folgendes durchzuführen:

**STEP 1 |** VPC-Gruppen erstellen und verwalten.

**STEP 2 |** Tags mithilfe von Überwachungsdefinitionen und Benachrichtigungsgruppen zu Gerätegruppen hinzufügen.

> *Installieren und konfigurieren Sie das AWS-Plug-in 5.1.0 (oder höher) auf Panorama, um die in den Cloud NGFW-Mandanten gesammelten AWS-Asset-Tags abzufragen und sie den Cloud-Gerätegruppen hinzuzufügen.*

VPC-Gruppen erstellen und verwalten

Wenn Sie die Überwachung aktivieren, wird automatisch eine **Standard**-VPC-Gruppe erstellt. Sie können die **Standard**-VPC-Gruppe nicht **löschen**. Eine neu erkannte VPC wird immer in die **Standard**-VPC-Gruppe eingefügt. Wenn Sie möchten, können Sie diese dann in eine andere VPC-Gruppe verschieben.

> *Der Umfang einer in einer Region erstellten VPC-Gruppe gilt nur für diese Region. Beispielsweise kann auf die in Region X erstellte VPC-Gruppe A in Region Y nicht zugegriffen werden.*

Alternativ können Sie neue VPC-Gruppen erstellen und diese VPCs mit den folgenden Schritten in andere VPC-Gruppen verschieben:

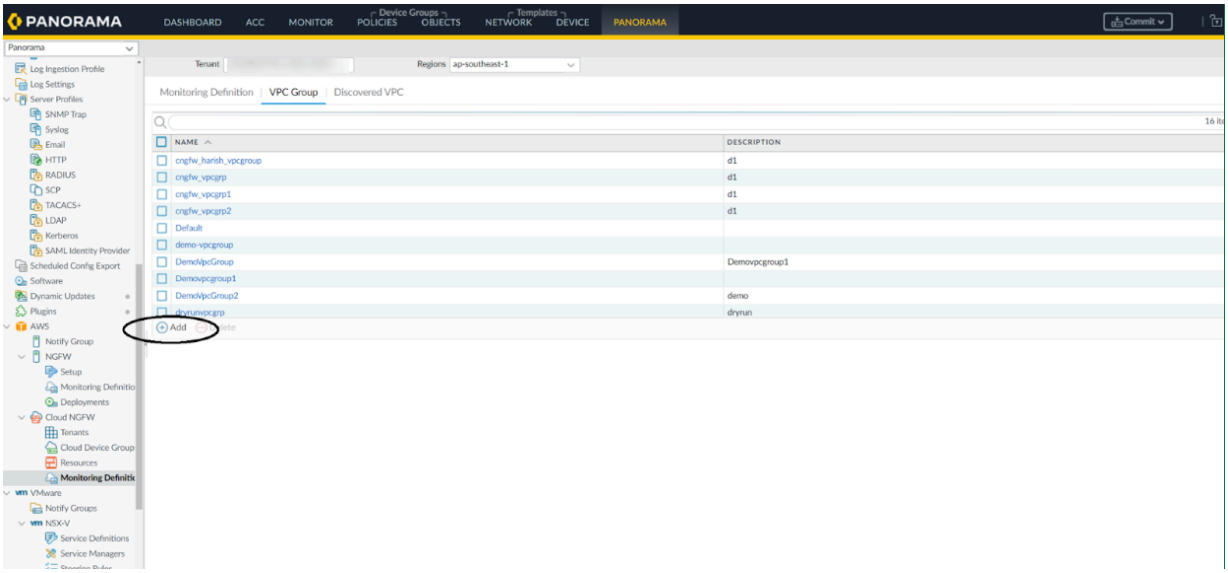
Wenn Sie eine neue, **vom Standard abweichende VPC-Gruppe** auf Panorama erstellen möchten, gehen Sie wie im folgenden Verfahren beschrieben vor:

**STEP 1 |** Wechseln Sie in der **Panorama**-Konsole auf die Registerkarte **Panorama** und klicken Sie anschließend auf **AWS**.

**STEP 2 |** Wählen Sie den **Mandanten** und die **Region** aus.

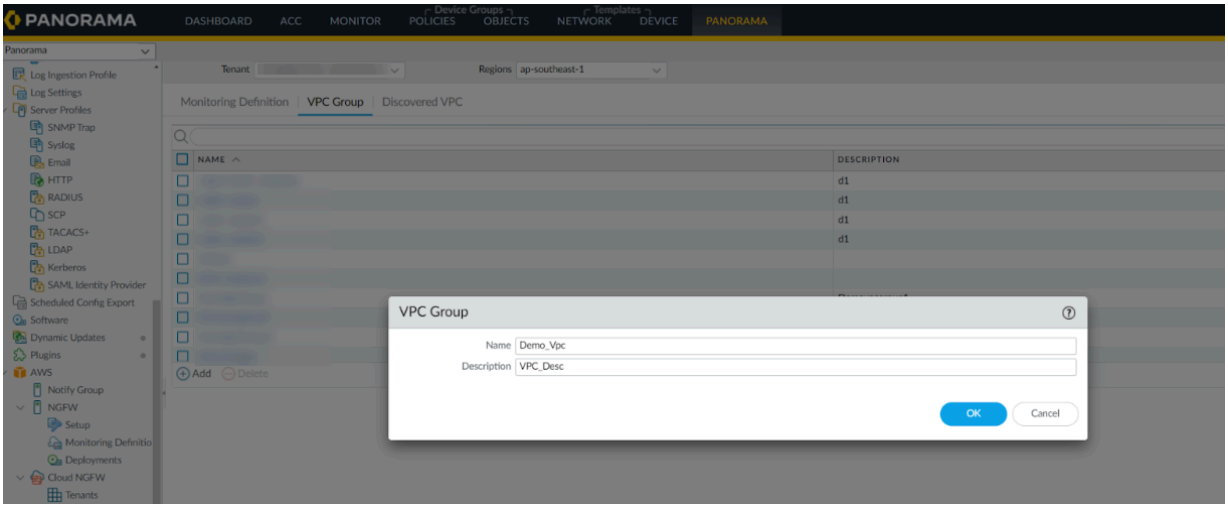
 

**STEP 3 |** Wechseln Sie zu **AWS** > **Cloud NGFW** > **Monitoring Definition (Überwachungsdefinition)** > **VPC Group (VPC-Gruppe)** > **Add (Hinzufügen)**.



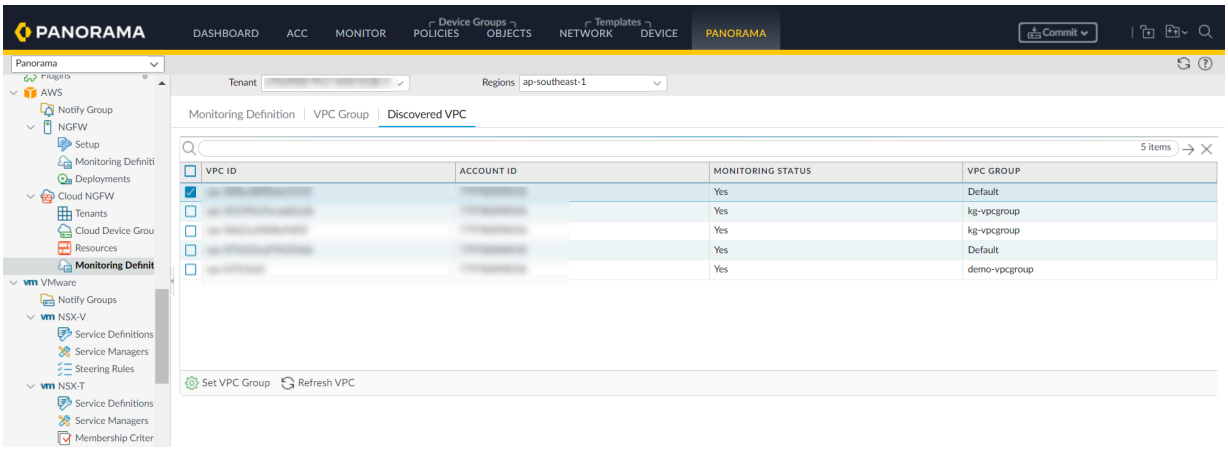
**STEP 4 |** Geben Sie den **Namen** und eine **Beschreibung** für die VPC-Gruppe ein.




**STEP 5 |** Klicken Sie auf **OK**.

**STEP 6 |** Wechseln Sie zu **AWS > Cloud NGFW > Monitoring Definition (Überwachungsdefinition) > Discovered VPC (Erkannte VPC)**.

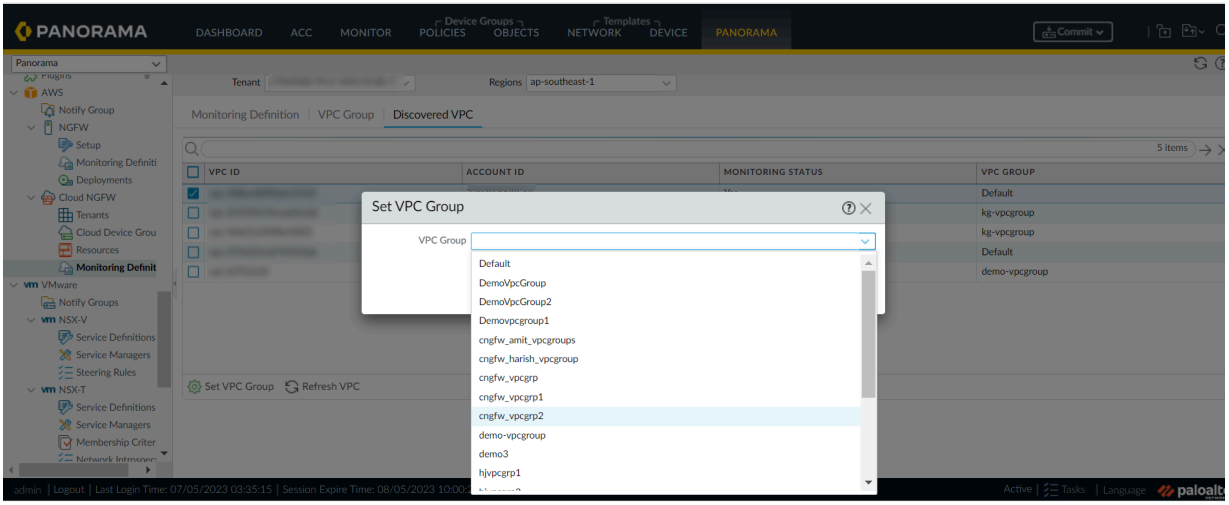



- *Sie können einer **VPC-Gruppe** maximal acht Gerätegruppen zuordnen. Für eine bessere Leistung konfigurieren Sie Überwachungsdefinitionen mit VPC-Gruppen so, dass einer bestimmten VPC-Gruppe (über Benachrichtigungsgruppen) nur acht Gerätegruppen zugeordnet sind.*
- *Die **Standard**-VPC-Gruppe wird automatisch erstellt. Sie können die **Standard**-VPC-Gruppe nicht **löschen**. Eine neu erkannte VPC wird immer in die **Standard**-VPC-Gruppe eingefügt. Bei Bedarf können VPCs in eine andere VPC-Gruppe verschoben werden.*

**STEP 7 |** Klicken Sie auf **Set VPC Group (VPC-Gruppe festlegen)**.

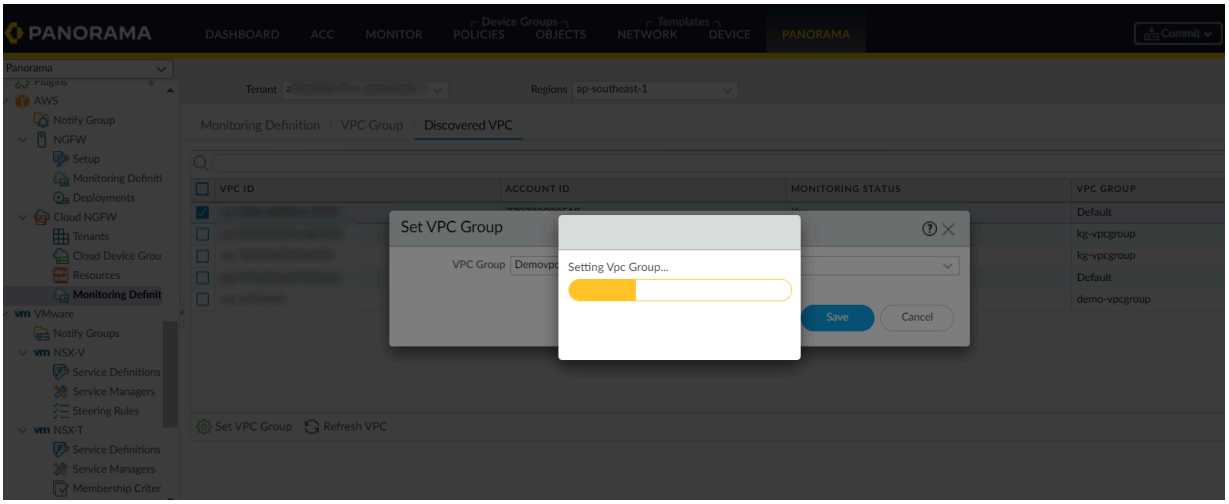
 

**STEP 8 |** Wählen Sie eine **VPC-Gruppe** aus.



**STEP 9 |** Klicken Sie auf **Save (Speichern)**.




*Tags mithilfe von Überwachungsdefinitionen und Gerätegruppen zu Gerätegruppen hinzufügen*

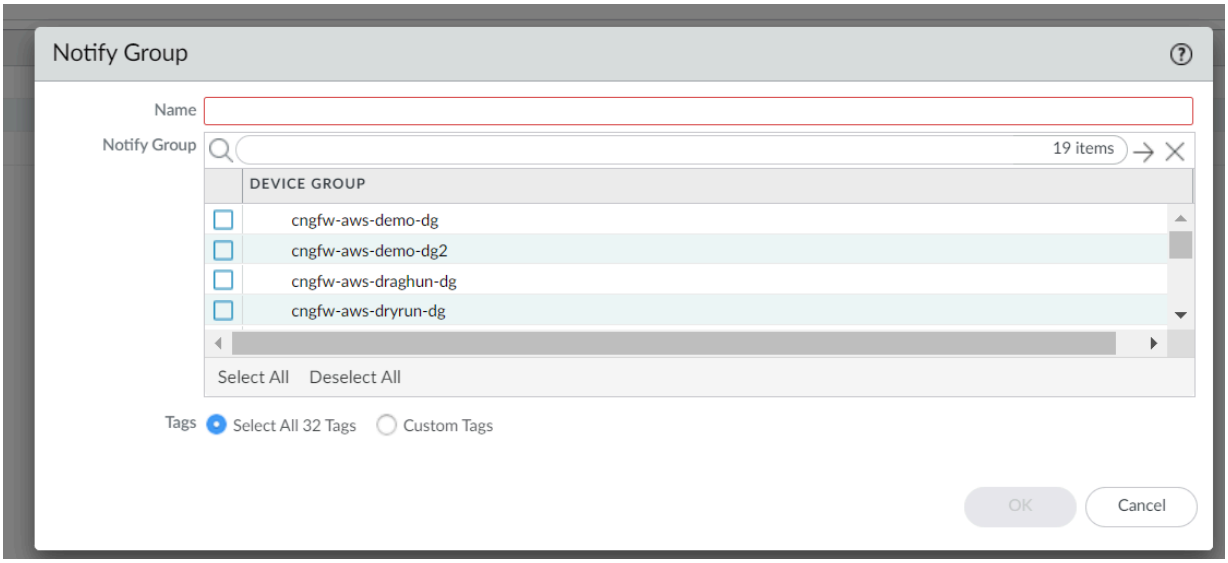
Um vom Cloud NGFW-Mandanten gelernte Tags an die Cloud NGFW-Ressourcen zu übertragen, müssen Sie die **Benachrichtigungsgruppen** und **Überwachungsdefinitionen** für die Gerätegruppen konfigurieren, die diesen Palo Alto Networks Firewalls entsprechen. Anschließend können Sie die vom Cloud NGFW-Mandanten gesammelten AWS-Kontotags in Panorama anzeigen.

Erstellen Sie mit den folgenden Schritten eine **Benachrichtigungsgruppe** für Ihre Cloud-Gerätegruppe:

**STEP 1 |** Wechseln Sie in der **Panorama-Plug-in**-Konsole zu **AWS > Notify Group (Benachrichtigungsgruppe)**.

**STEP 2 |** **Hinzufügen**.




**STEP 3 |** Geben Sie einen **Namen** ein.

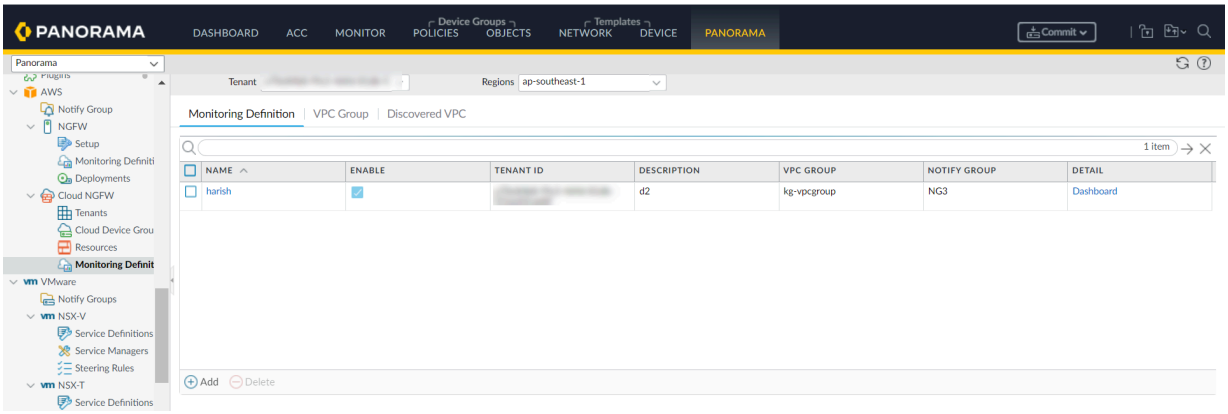
**STEP 4 |** Wählen Sie die **Gerätegruppe** und **Tags** aus.

**STEP 5 |** Klicken Sie auf **OK**.

Erstellen Sie eine Cloud-**Überwachungsdefinition**, die die erforderliche **VPC-Gruppe** und **Benachrichtigungsgruppe** mit von Cloud NGFW erlernten Tags verknüpft:

**STEP 6 |** Wechseln Sie in **Panorama** zu **AWS > Cloud NGFW > Monitoring Definition (Überwachungsdefinition)**.



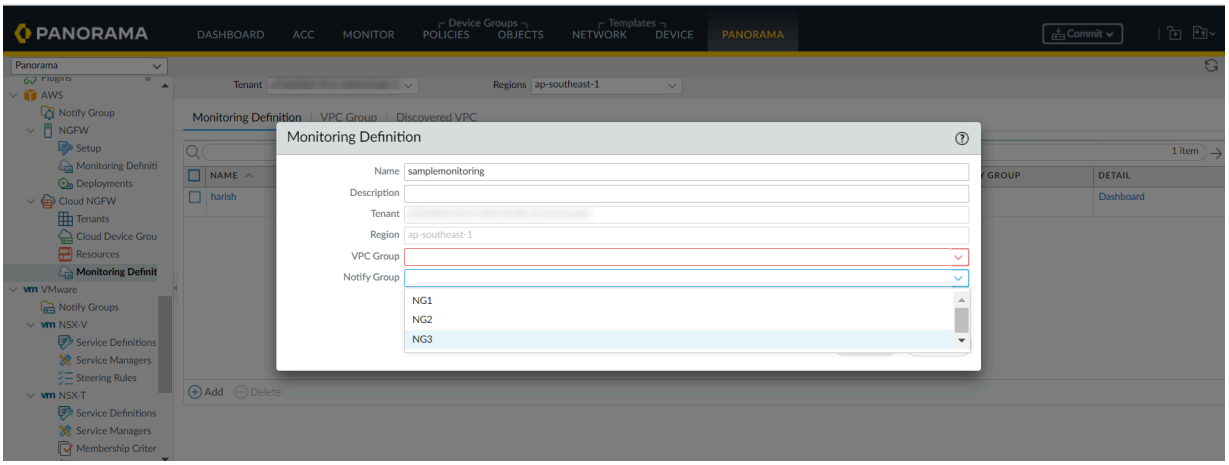

**STEP 7 |** Klicken Sie auf **Add (Hinzufügen)**.

**STEP 8 |** Geben Sie Ihren **Namen** und eine **Beschreibung** ein.

**STEP 9 |** Wählen Sie im Dropdown-Menü **VPC Group (VPC-Gruppe)** die erforderliche VPC-Gruppe aus.

**STEP 10 |** Wählen Sie im Dropdown-Menü **Notify Group (Benachrichtigungsgruppe)** die gewünschte Benachrichtigungsgruppe aus.

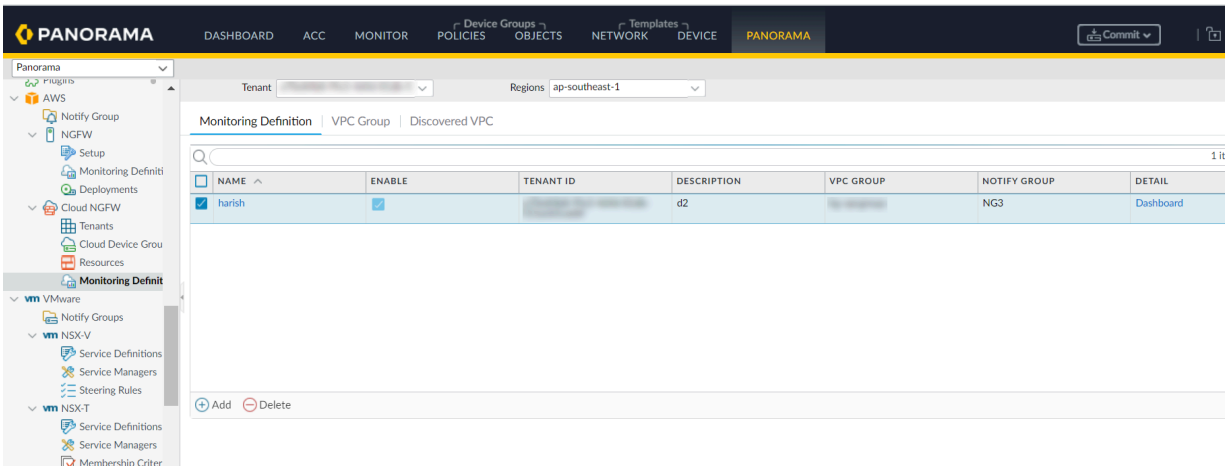



**STEP 11 |** Klicken Sie auf **OK**.

**STEP 12 |** Führen Sie einen **Commit** aus und übertragen Sie Ihre Änderungen per **Push** an Panorama.

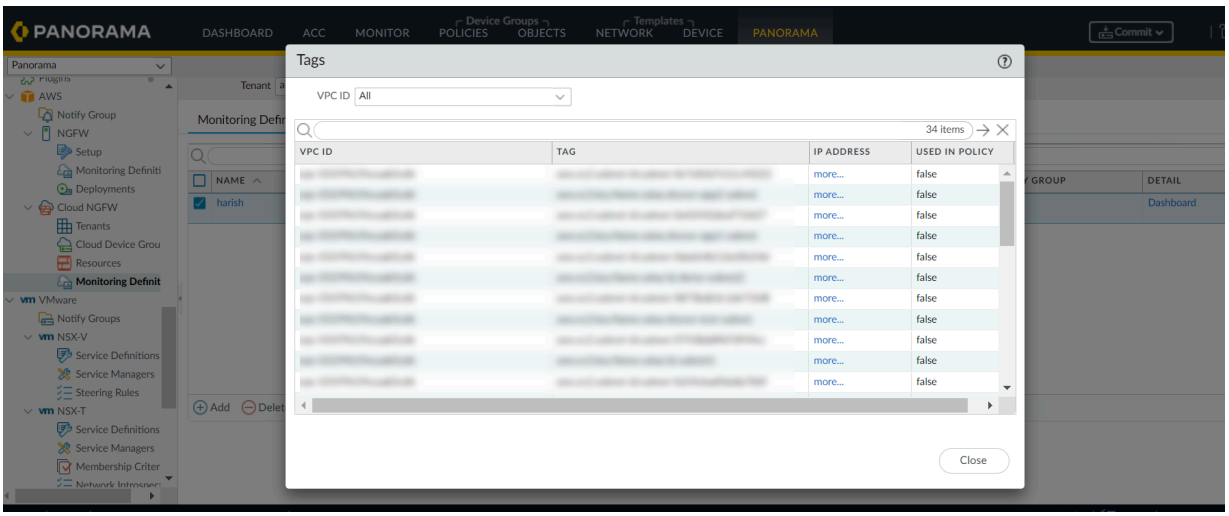
 

**STEP 13 |** Wählen Sie eine **Überwachungsdefinition** aus und klicken Sie auf **Dashboard**, um die vom Cloud NGFW-Mandanten gesammelten Tags anzuzeigen.




Sie können jetzt die im Cloud NGFW-Mandanten gesammelten Tags anzeigen:




*DAG-Objekte mit Tags in Gerätegruppen konfigurieren*

Sie können dynamische Adressgruppen mit gesammelten Cloud NGFW-Tags für Ihre Cloud-Gerätegruppe erstellen. Weitere Informationen finden Sie unter Dynamische Adressgruppen erstellen.

Im Folgenden finden Sie die Schritte zum Hinzufügen von Übereinstimmungskriterien für Ihre dynamischen Adressgruppen:

**STEP 1 |** Wählen Sie in **Panorama** die Registerkarte **Objekts (Objekte)** aus.

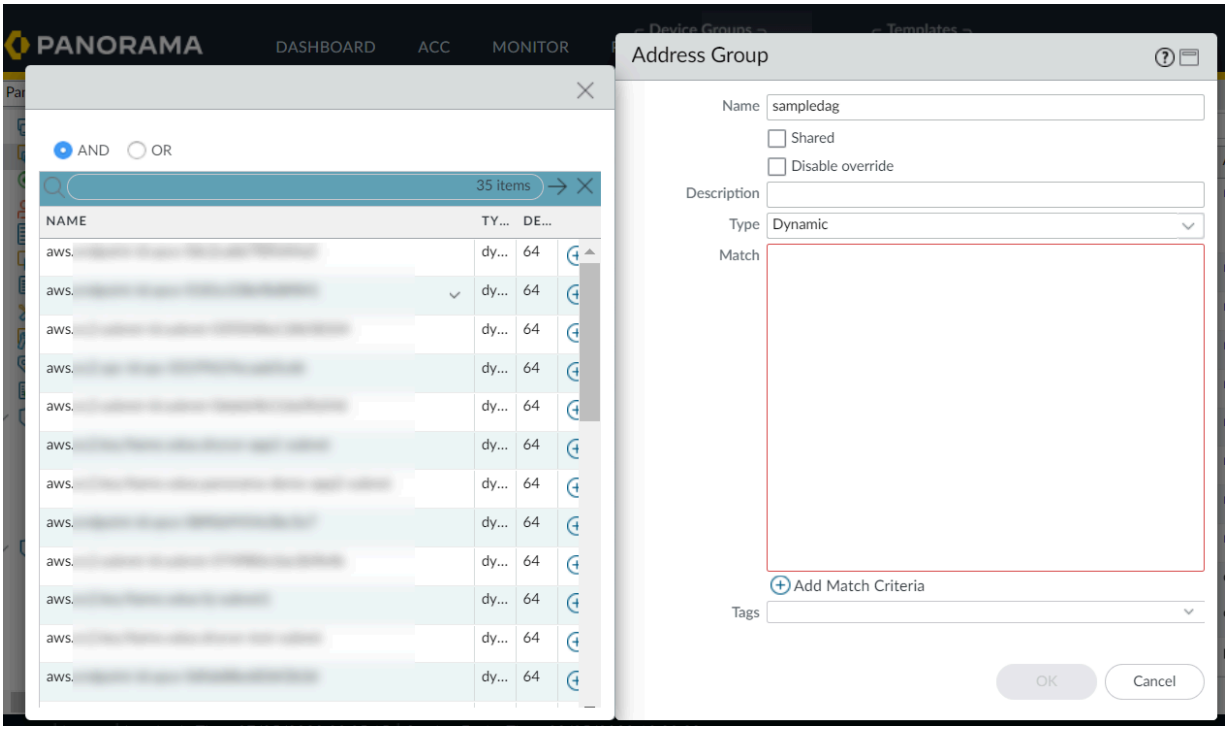
**STEP 2 |** Wechseln Sie im linken Bereich zu **Address Groups (Adressgruppen)**.

**STEP 3 |** Klicken Sie auf **Add (Hinzufügen)**.

**STEP 4 |** Geben Sie den **Namen** Ihrer Adressgruppe ein und wählen Sie den Typ **Dynamic (Dynamisch)** aus.

**STEP 5 |** Klicken Sie auf **Add match Criteria (Übereinstimmungskriterien hinzufügen)**.



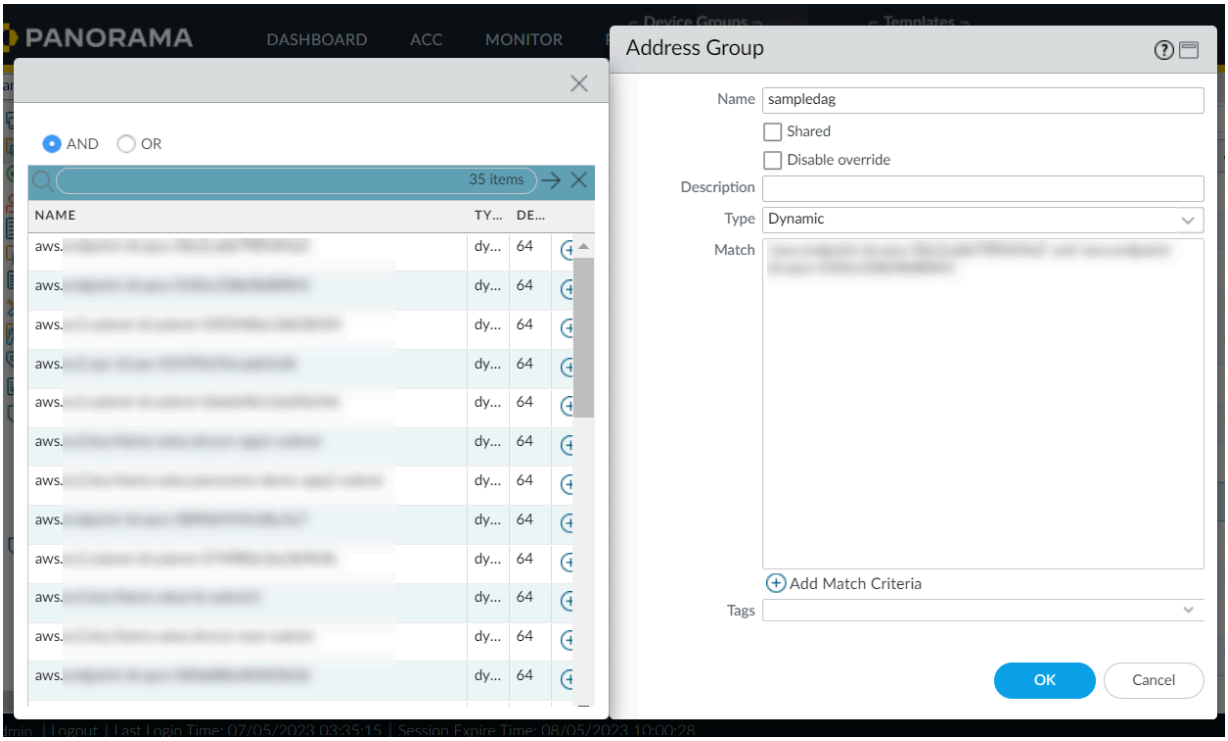

Sie können jetzt **Richtlinienregeln für dynamische Adressgruppen** erstellen, die auf die oben erstellten DAGs für Cloud-Gerätegruppen verweisen.

Sie können Tags aus verschiedenen Regionen zu Ihrem DAG-Objekt hinzufügen. Um Tags aus verschiedenen Regionen zu verwenden, müssen Sie in anderen Regionen eine Cloud-Gerätegruppe mit demselben Namen erstellen. Darüber hinaus müssen Sie in anderen Regionen eine

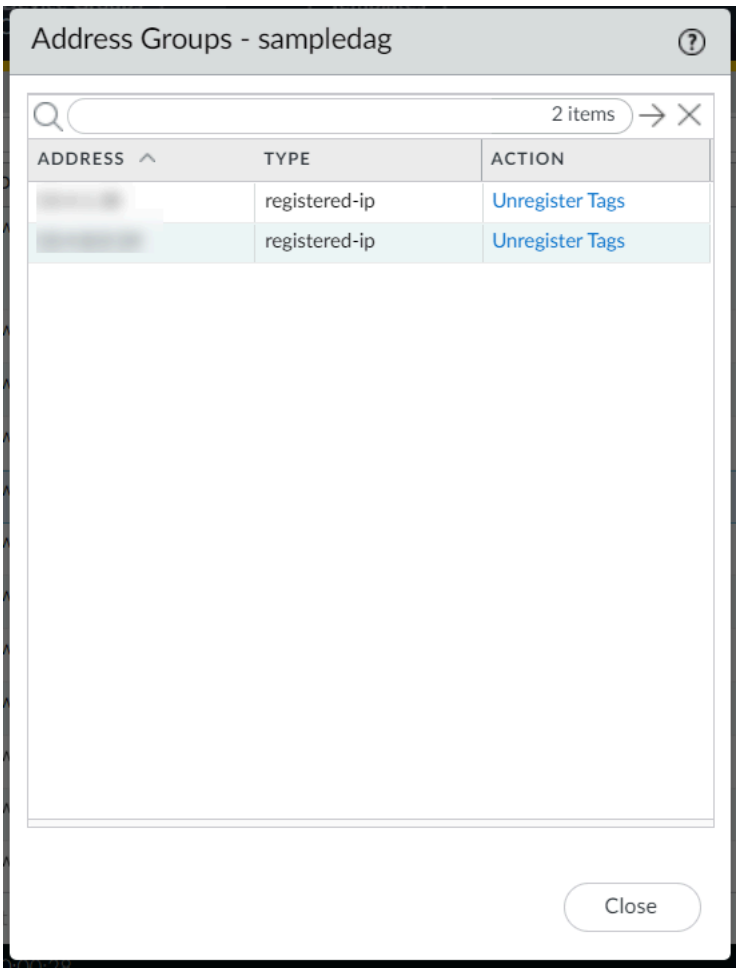
Überwachungsdefinition erstellen, die die Benachrichtigungsgruppe der VPC-Gruppe dieser Region zuordnet. Weitere Informationen finden Sie unter Tagbasierte Richtlinien für mehrere Regionen.

Das nachfolgende Beispiel veranschaulicht, wie DAGs mit dem Operator **AND** erstellt werden:



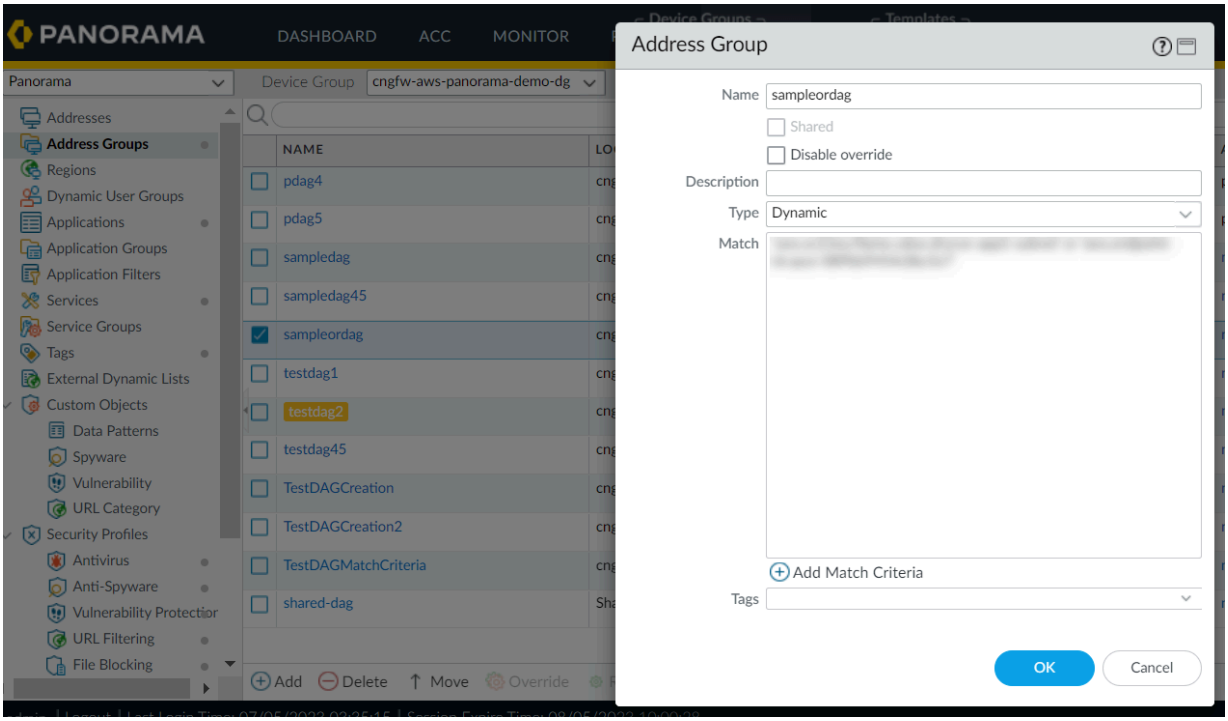

Die Adressgruppe zeigt die Liste der Adressen an, die beiden Übereinstimmungskriterien entsprechen:



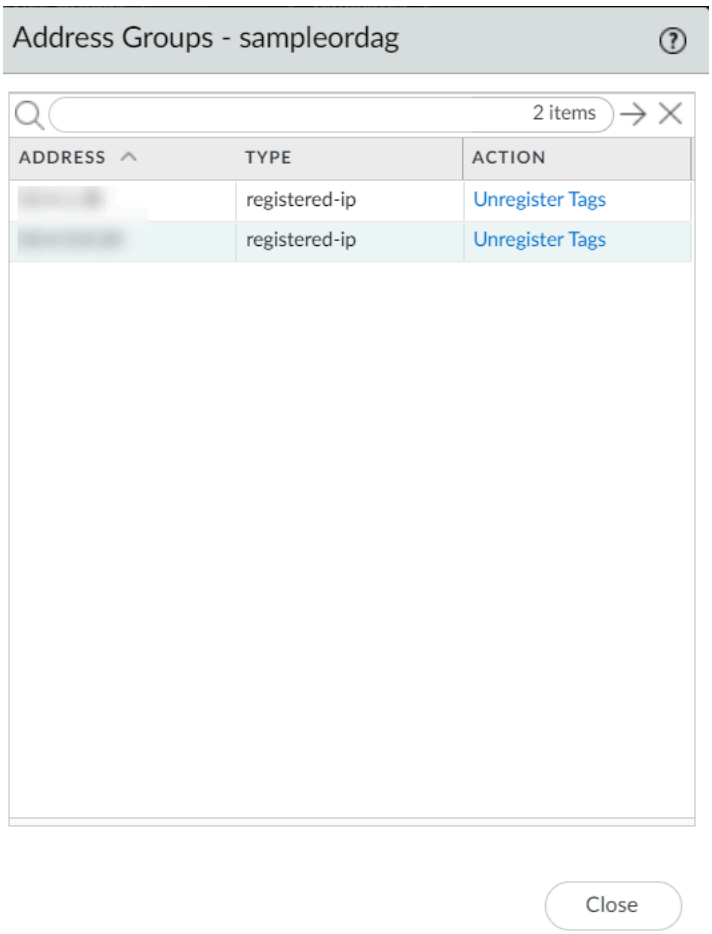

Das nachfolgende Beispiel veranschaulicht, wie DAGs mit dem Operator **OR** erstellt werden:




Die Adressgruppe zeigt die Liste der Adressen an, die einem der angegebenen Übereinstimmungskriterien entsprechen:

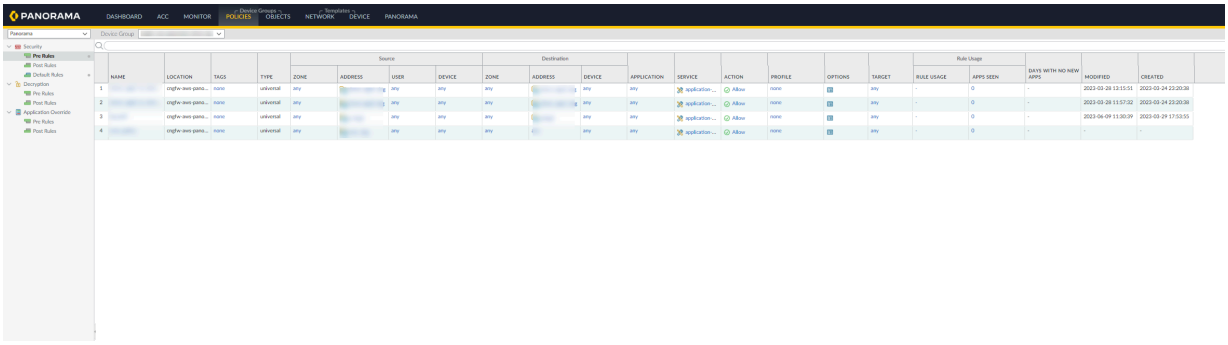



Gehen Sie wie folgt vor, um Richtlinienregeln für dynamische Adressen zu erstellen, die auf DAGs für Cloud-Gerätegruppen verweisen:

**STEP 6 |** Wechseln Sie in der **Panorama**-Konsole zur Registerkarte **Policies (Richtlinien)**.

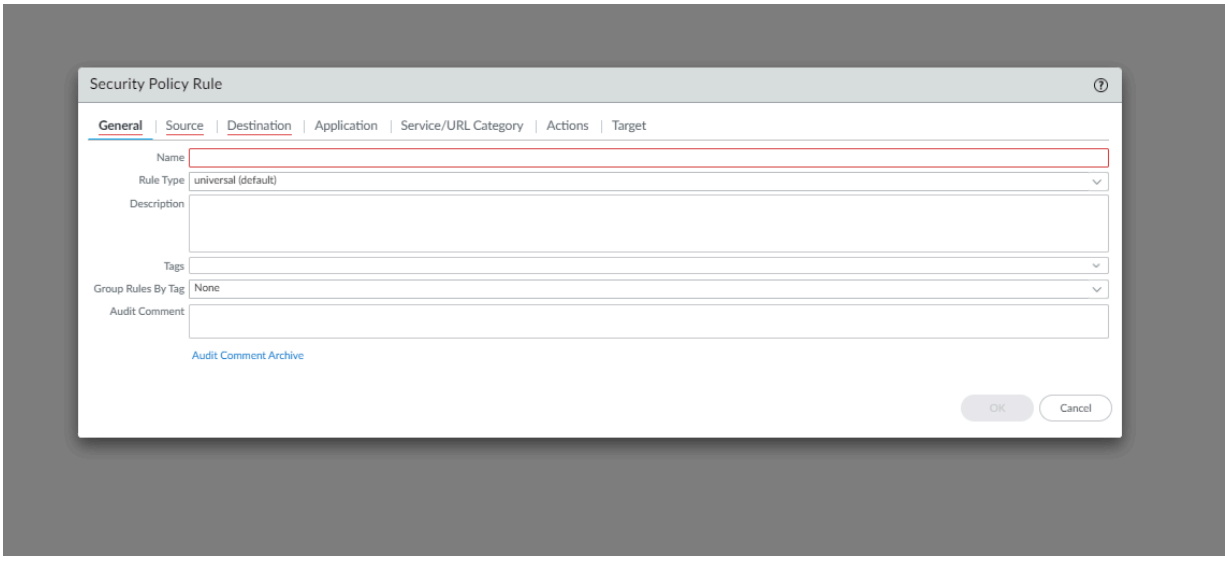
**STEP 7 |** Wechseln Sie zu **Security (Sicherheit) > Pre/Post/Default Rules (Vor-/Nach-/Standardregeln)**.




**STEP 8 |** Klicken Sie auf **Add (Hinzufügen)**.

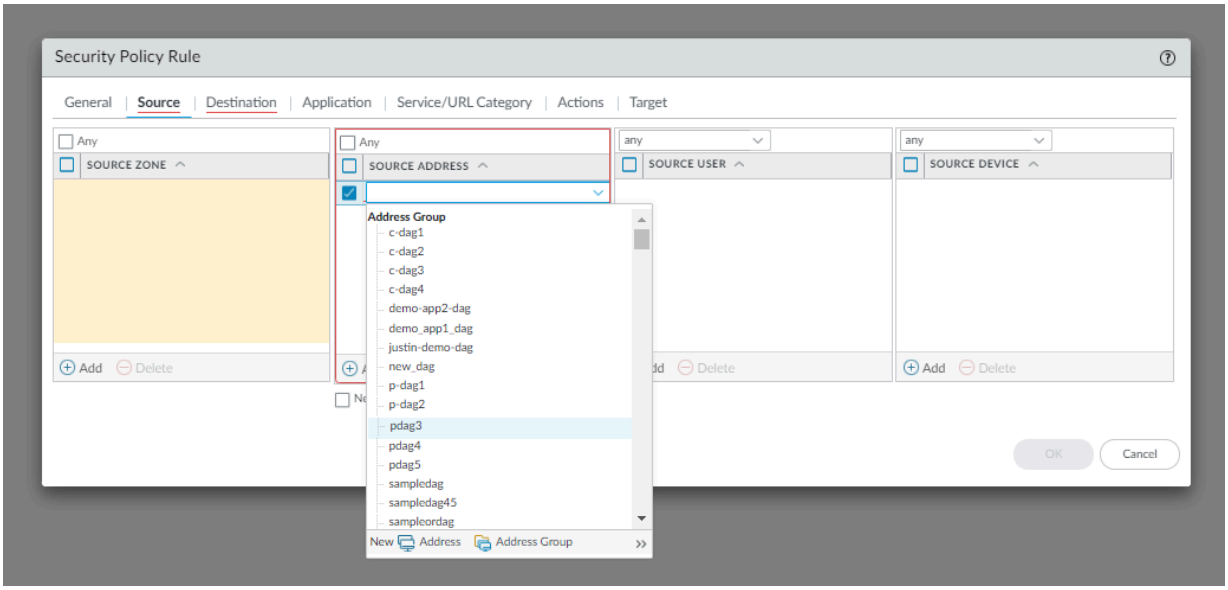
 

**STEP 9 |** Geben Sie im Dialogfeld **Security Policy Rule (Sicherheitsrichtlinienregel)** einen **Namen** für die Sicherheitsrichtlinienregel ein.



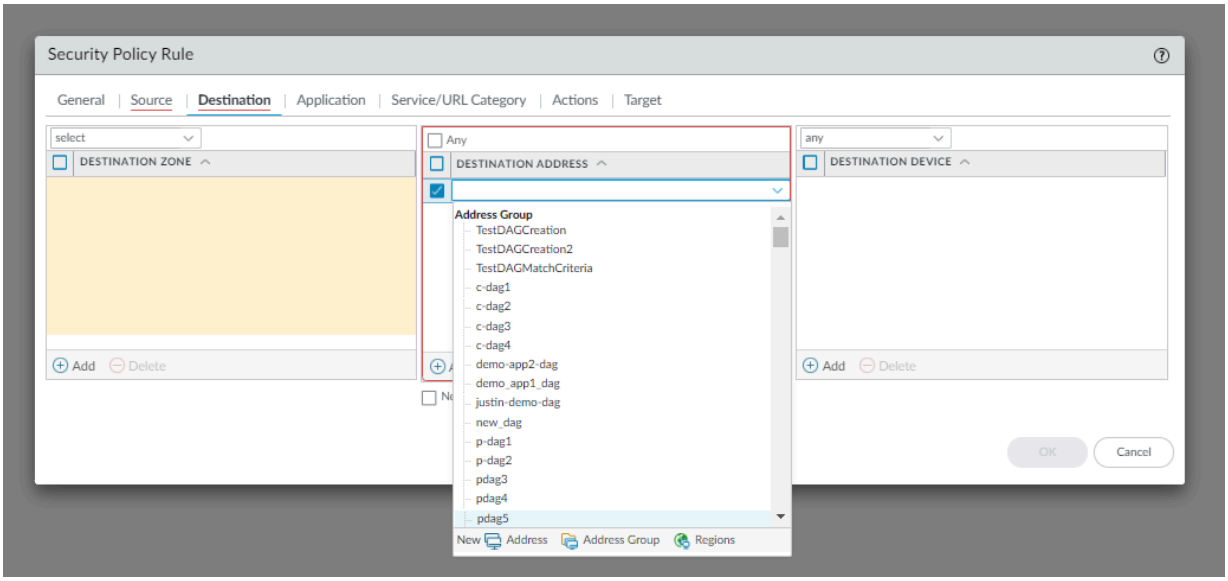

 

**STEP 10 |** Wählen Sie auf der Registerkarte **Source (Quelle)** die dynamische Adressgruppe für das Feld **Source Address (Quelladresse)** aus und klicken Sie auf **Add (Hinzufügen)**.



**STEP 11 |** Wählen Sie auf der Registerkarte **Destination (Ziel)** die dynamische Adressgruppe für das Feld **Destination Address (Zieladresse)** aus und klicken Sie auf **Add (Hinzufügen)**.




**STEP 12 |** Klicken Sie auf **OK**.

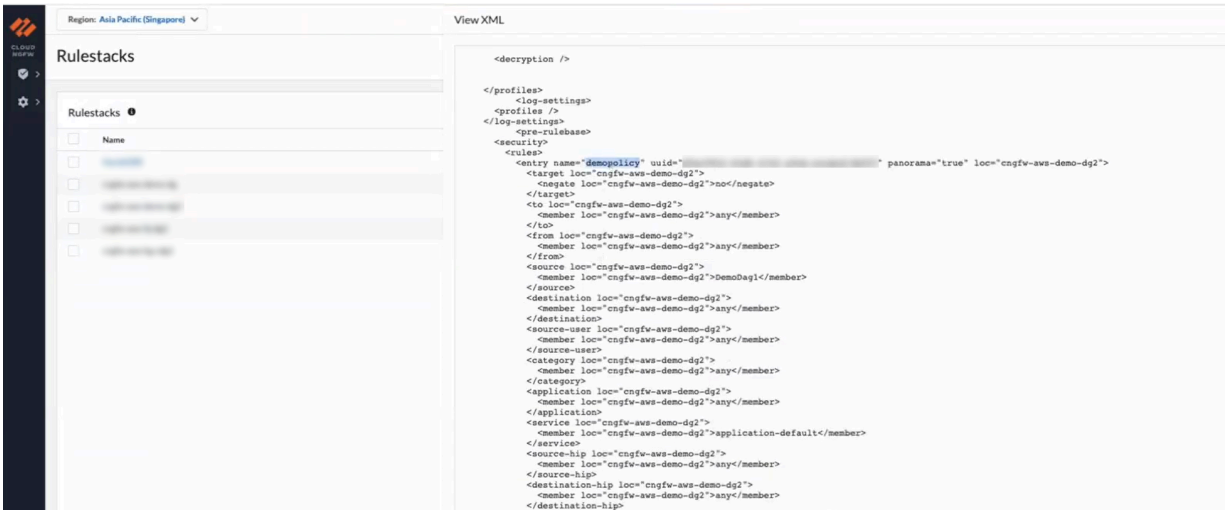
**STEP 13 |** Führen Sie einen **Commit** aus und übertragen Sie Ihre Änderungen per **Push** an die Cloud NGFW-Gerätegruppe.

Weitere Informationen zum Ausführen eines **Commits** und Übertragen von Konfigurationsänderungen per **Push** an die Firewalls finden Sie unter Vorschau, Validierung oder Übernehmen von Konfigurationsänderungen.

Kehren Sie zur **Cloud NGFW**-Konsole zurück, um eine XML-Datei mit Richtlinienregeln für dynamische Adressen zu überprüfen, die von Panorama an die jeweilige Cloud-Gerätegruppe gesendet wurden. Klicken

Wechseln Sie zu **View XML (XML anzeigen)**, um Informationen zu Richtlinienregeln für dynamische Adressen anzuzeigen, die neu zur Cloud-Gerätegruppe hinzugefügt wurden.



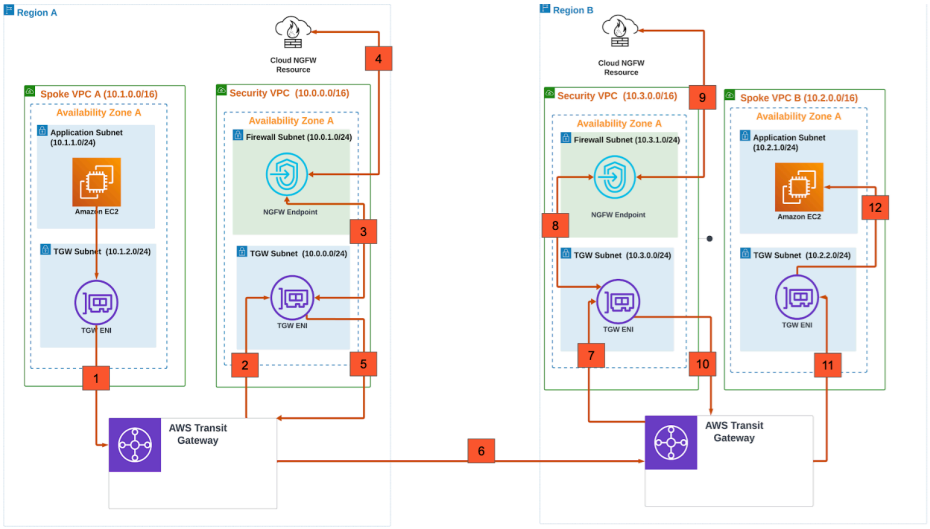

Fügen Sie dem Client-Konto ein neues Subnetz hinzu. Weitere Informationen finden Sie unter Subnetz in der AWS-Konsole erstellen.

Tagbasierte Richtlinien für mehrere Regionen

Sie können Ihren Cloud-Gerätegruppen Tags aus zwei verschiedenen Regionen hinzufügen.



Beispiel:

Region X und Region Y sind Ihre gewünschten Regionen, um die Erkennung von AWS-Ressourcentags zu ermöglichen. Wenn in Region X eine CNGFW-Ressource vorhanden ist, die die Tags aus Region Y erlernen und diese dann für die Cloud-Gerätegruppe in Region X verwenden soll, gehen Sie wie folgt vor:

**STEP 1 |** Fügen Sie dem Cloud NGFW-Mandanten AWS-Konten hinzu und sammeln Sie Tags daraus.

**STEP 2 |** Verwenden Sie das Panorama-Plug-in, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen.

**STEP 3 |** Konfigurieren Sie DAG-Objekte mit Tags in Gerätegruppen.

*Sie werden nur die Tags der Region X sehen können, die zum Konfigurieren Ihrer DAG-Objekte verfügbar sind.*

**STEP 4 |** Erstellen Sie in Region Y die Cloud-Gerätegruppe mit demselben Namen wie in Region X. Führen Sie einen Commit aus und übertragen Sie Ihre Änderungen per Push an Panorama. Erstellen Sie bei Bedarf eine VPC-Gruppe und weisen Sie entsprechende VPCs zu oder verwenden Sie die Standard-VPC-Gruppe in Region Y.

**STEP 5 |** Erstellen Sie eine Überwachungsdefinition in Region Y und wählen Sie dann die VPC-Gruppe und die Benachrichtigungsgruppe aus (sofern die Cloud-Gerätegruppe bereits zugeordnet ist).

**STEP 6 |** Konfigurieren Sie DAG-Objekte mit Tags in Gerätegruppen. Sie können jetzt sehen, dass sowohl Tags aus der Region X als auch aus der Region Y zum Konfigurieren Ihrer DAG-Objekte verfügbar sind.

**STEP 7 |** Führen Sie einen **Commit** für die Konfiguration in Panorama aus.

In der Cloud-Gerätegruppe werden Ihnen nun die zu konfigurierenden Tags aus Region Y angezeigt, und Sie können eine dynamische Adressgruppe erstellen.

## Zonenbasierte Richtlinienregeln konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Durch die Segmentierung des Netzwerks in funktionale und organisatorische Zonen wird die Angriffsfläche verringert – also der Teil, der potenziellen Angreifern ausgesetzt ist. Sicherheitszonen schützen Ihr Netzwerk, indem sie es in kleinere, einfacher zu verwaltende Bereiche unterteilen und den Zugriff auf diese Bereiche kontrollieren.

Bei selbstverwalteten Palo Alto Networks Firewalls (wie der VM-Series) umfasst eine Sicherheitszone eine oder mehrere physische oder virtuelle Firewallschnittstellen und die Netzwerksegmente, die mit den

Schnittstellen der Zone verbunden sind. Zuerst definieren Sie Zonen und verknüpfen dann die physischen und virtuellen Schnittstellen mit diesen Zonen. Schließlich verwenden Sie diese Zonen in den von Ihnen erstellten Sicherheitsrichtlinienregeln.

Cloud NGFW richtet die Netzwerkkonstrukte jedoch automatisch für Sie ein. Sie müssen sich nicht mehr darum kümmern, Schnittstellen zu konfigurieren und diese mit den von Ihnen erstellten Zonen zu verknüpfen. Sie können zonenbasierte Richtlinienregeln in Panorama erstellen und sie in Cloud NGFW durchsetzen.

**Cloud NGFW-Zonen**

Mit Cloud NGFW können Sie Ihren VPC-Verkehr mithilfe von **privaten** und **öffentlichen** Zonen klassifizieren, um die Durchsetzung von Richtlinien zu vereinfachen.

- Die **private Zone** umfasst Ihr Hybrid-Cloud-Netzwerk, das durch Präfixe für privaten Datenverkehrsbereich definiert ist. Dieses Netzwerk umfasst Ihre VPCs auf AWS und Ihr lokales Netzwerk (verbunden über Direct Connect oder VPN).
- Die **öffentliche Zone** umfasst alle Präfixe außerhalb Ihres Hybrid-Cloud-Netzwerks (das öffentliche Internet).

Steuern Sie diese Klassifizierung, indem Sie die Präfixe für den privaten Datenverkehrsbereich für den Endpunkt, auf dem der Datenverkehr in die Cloud NGFW-Ressource gelangt, entsprechend angeben.

**Quell- und Zielzonen**

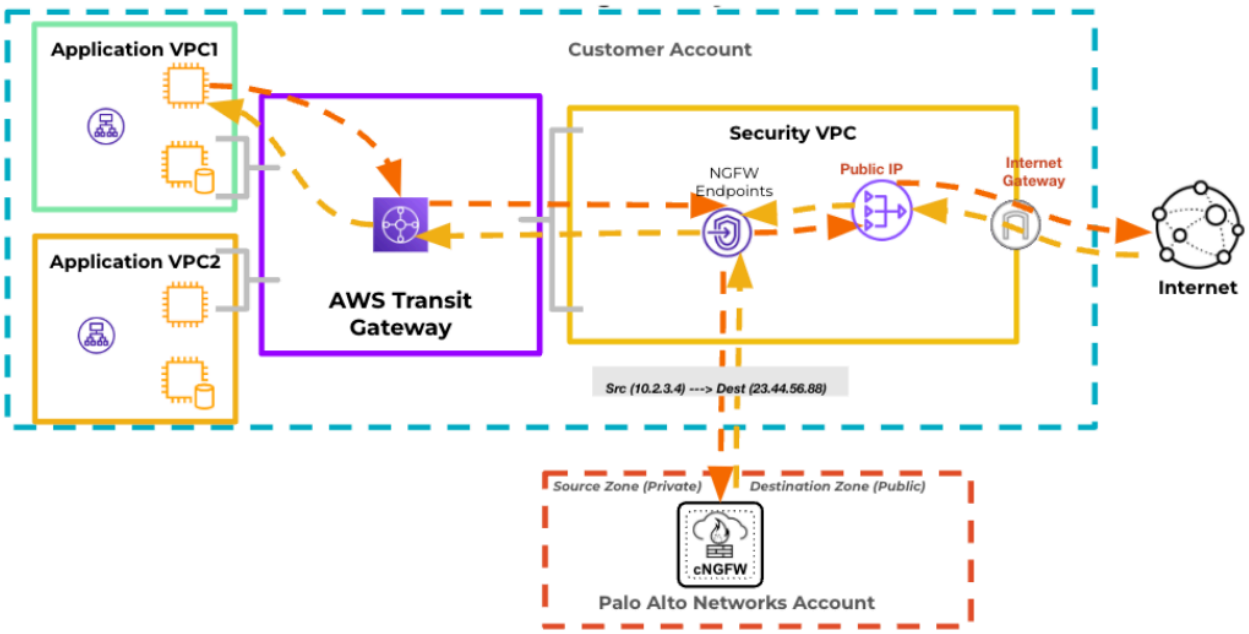
Cloud NGFW weist die **Quellzone** automatisch als **privat** zu, wenn die Datenverkehrssitzung eine Quell-IP-Adresse innerhalb der Präfixe für privaten Datenverkehrsbereich hat, die für den Endpunkt definiert sind, auf dem der Datenverkehr in die Cloud NGFW-Ressource gelangt. Andernfalls weist Cloud NGFW die Quellzone als **öffentlich** zu.

In ähnlicher Weise weist Cloud NGFW die **Zielzone** automatisch als **privat** zu, wenn die Datenverkehrssitzung eine Ziel-IP-Adresse innerhalb der Präfixe für privaten Datenverkehrsbereich hat, die für den Endpunkt definiert sind, auf dem der Verkehr in die Cloud NGFW-Ressource gelangt. Andernfalls weist Cloud NGFW die Zielzone als **öffentlich** zu.

Für eine Sitzung mit der Quell-IP-Adresse 10.2.3.4 und der Ziel-IP-Adresse 23.44.55.66 weist Cloud NGFW beispielsweise die Quellzone (Eingangszone) als privat und die Zielzone als öffentlich zu.

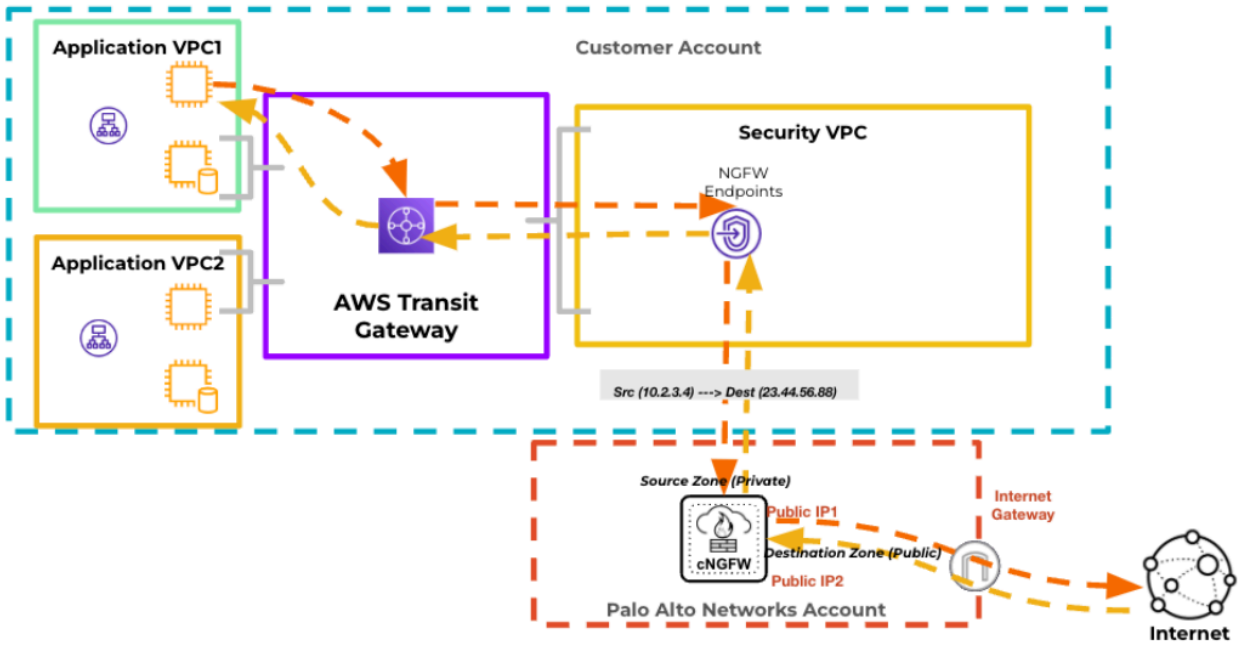
In der folgenden Abbildung sind die Quell- und Zielzonen für den Datenverkehr über einen Endpunkt mit deaktiviertem Ausgangs-NAT dargestellt:




In der folgenden Abbildung sind die Quell- und Zielzonen für den Datenverkehr über einen Endpunkt mit aktiviertem Ausgangs-NAT dargestellt:




## Zonenschutz

Eine effektive Abwehr von DoS-Angriffen erfordert einen mehrschichtigen Ansatz. Die erste Verteidigungsschicht sollte ein dedizierter, hochvolumiger DDoS-Schutzdienst wie AWS Shield sein, um volumetrische Angriffe abzuwehren, für die die sitzungsbasierten Firewalls nicht ausgelegt sind. Cloud NGFW verwendet das Zonenschutzprofil jedoch, um detailliertere Ebenen der DoS-Angriffsabwehr hinzuzufügen und Einblicke in den Anwendungsverkehr bereitzustellen, den dedizierte DDoS-Dienste nicht bieten.

Nachdem der Datenverkehr den dedizierten DDoS-Dienst (wie AWS Shield) durchlaufen und Ihre VPC erreicht hat, wendet Cloud NGFW das Zonenschutzprofil an, falls eines an die Eingangszone (Quellzone) angehängt ist. Cloud NGFW bestimmt die Eingangszone (Quellzone) anhand der Quell-IP-Adresse des Pakets. Zonenschutzprofile bieten einen umfassenden Schutz vor DoS-Angriffen, die auf dem Gesamtdatenverkehr basieren, der die Zone betritt. Wenn das Paket vom Zonenschutzprofil abgelehnt wird, verwirft Cloud NGFW das Paket und überspringt die Sicherheitsrichtliniensuche. Cloud NGFW wendet Zonenschutzprofile nur auf neue Sitzungen an (Pakete, die keiner vorhandenen Sitzung entsprechen). Sobald die Sitzung eingerichtet ist, umgeht die Cloud NGFW-Paketverarbeitungs-Engine die Suche nach dem Zonenschutzprofil für nachfolgende Pakete in dieser Sitzung.

Sie können mithilfe der Panorama Cloud-Gerätegruppenvorlage ein Zonenschutzprofil an die privaten und öffentlichen Zonen anhängen. Ein Zonenschutzprofil schützt die Eingangszone (oder Quellzone) vor den häufigsten Flood-, Reconnaissance- und paketbasierten Angriffen.

- Flood-Schutz. Ein Zonenschutzprofil mit konfiguriertem Flood-Schutz schützt eine ganze Eingangszone vor SYN-, ICMP-, ICMPv6-, UDP- und anderen IP-Flood-Angriffen.
- Reconnaissance-Schutz. Ähnlich wie bei der militärischen Definition von Reconnaissance entspricht die Netzwerksicherheitsdefinition von Reconnaissance dem Versuch von Angreifern, Informationen über die Sicherheitslücken Ihres Netzwerks zu erhalten, indem sie das Netzwerk heimlich nach Sicherheitslücken durchsuchen. Reconnaissance-Aktivitäten sind oft der Auftakt zu einem Netzwerkangriff. *Aktivieren Sie Reconnaissance-Schutz sowohl in privaten als auch in öffentlichen Zonen*, um sich vor Port-Scans und Host-Sweep zu schützen.

- Schutz vor paketbasierten Angriffen. Paketbasierte Angriffe können die unterschiedlichsten Formen annehmen. Zonenschutzprofile überprüfen IP-, TCP-, ICMP-, IPv6- und ICMPv6-Paket-Header und schützen eine Zone, indem sie Pakete mit unerwünschten Eigenschaften verwerfen oder unerwünschte Optionen von Paketen entfernen, bevor sie zur Zone zugelassen werden.

**Zuordnung von Cloud NGFW-Zonen**

Zonen sind mit Schnittstellen auf selbstverwalteten Firewalls wie der VM-Series verknüpft. In Cloud NGFW wird die Netzwerkinfrastruktur jedoch automatisch für Sie eingerichtet. Das bedeutet, dass Sie sich keine Gedanken mehr über die Konfiguration von Schnittstellen und deren Verknüpfung mit den von Ihnen erstellten Zonen machen müssen (und in Panorama Cloud NGFW-Vorlagenstacks und -Vorlagen wird die Weboberfläche zum Konfigurieren von Schnittstellen aus Panorama entfernt – alle unnötigen Panorama-Weboberflächenelemente werden in von Panorama verwalteten Cloud-Gerätegruppen entfernt).

Um eine konsistente Durchsetzung der Sicherheitsrichtlinien zu ermöglichen, müssen Sie jedoch Zonenzuordnungen in Ihren Cloud-Gerätegruppen erstellen, damit Cloud NGFW weiß, ob die Sicherheitszonen, die in Ihrem Panorama vorhanden sind, mit der privaten (internen) oder öffentlichen (externen) Zone von Cloud NGFW verknüpft werden müssen. Diese Zuordnungen ermöglichen es Cloud NGFW, Ihre Sicherheitsrichtlinienregeln ordnungsgemäß durchzusetzen.

*In einigen Fällen kann die Zonenzuordnung fehlschlagen, wenn Sie nicht die neueste Version des AWS-Plug-ins (Version 5.3.0) verwenden. Palo Alto Networks empfiehlt, dass Sie keine zonenbasierten Richtlinien für bestehende Firewalls aktivieren, die nicht mithilfe der AWS-Plug-in-Version 5.3.0 oder höher auf das neue Ausgangs-NAT-AMI aktualisiert wurden.*

## Zonenzuordnung in Panorama Cloud-Gerätegruppen konfigurieren

Die folgenden Mindestsystemanforderungen sind für zonenbasierte Richtlinienregeln erforderlich:

- AWS-Plug-in-Version 5.3.0 oder höher
- PAN-OS-Version 10.2.8 oder höher
- Cloud Connector-Plug-in-Version 2.0.1 oder höher

So konfigurieren Sie die Zonenzuordnung mit der Panorama-Konsole:

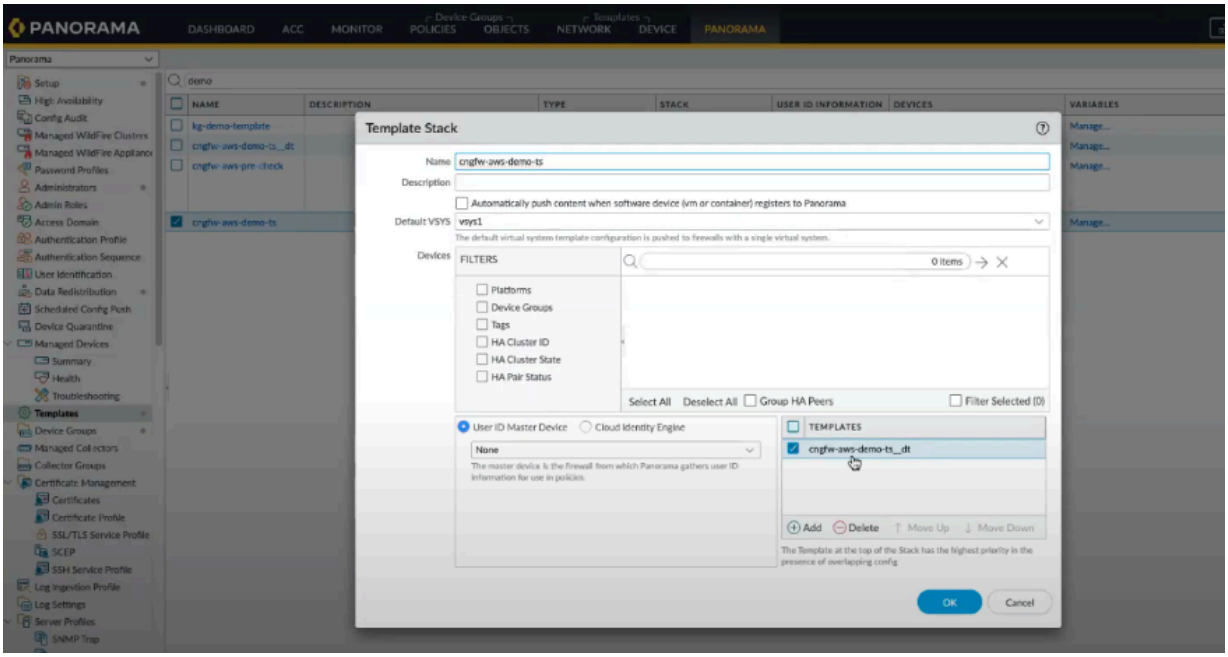
**STEP 1 |** Fügen Sie mithilfe der Panorama-Konsole eine Cloud-Gerätegruppe hinzu.

**STEP 2 |** **Panorama > Templates (Panorama > Vorlagen)** und wählen Sie Ihren **Vorlagenstack** aus

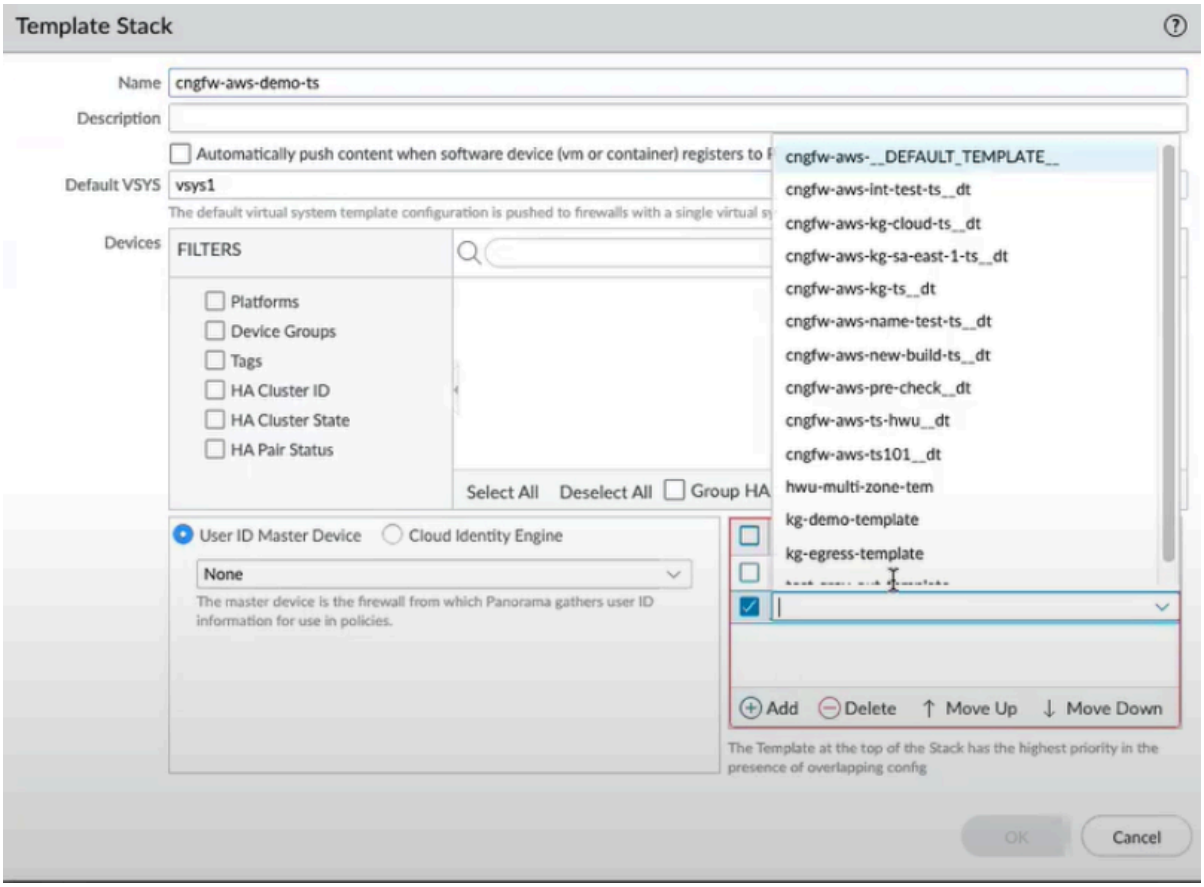
Das AWS-Plug-in verknüpft den Vorlagenstack mit Ihrer Cloud-Gerätegruppe. Das AWS-Plug-in erstellt eine Standardvorlage und fügt dieser Vorlage standardmäßig die Zonen **Public (Öffentlich)** und **Private (Private)** hinzu.

Im Abschnitt **Templates (Vorlagen)** sehen Sie die vom AWS-Plug-in erstellte Standardvorlage, die denselben Namen wie Ihr Vorlagenstack hat, wobei an ihren Namen das Suffix `__dt` angehängt ist.



**STEP 3 |** Sie können Ihre anderen Panorama-Vorlagen auch auf die Vorlagenstackliste verweisen, auf **Add (Hinzufügen)** klicken und dann die Vorlage auswählen.




**STEP 4 |** Erstellen Sie ein Zonenschutzprofil und verknüpfen Sie es mit Ihren **privaten** und **öffentlichen** Standardzonen Ihrer Standardvorlage. So erstellen Sie das Zonenschutzprofil:

1. Gehen Sie in der Panorama-Konsole zu **Network (Netzwerk)** > **Zone Protection (Zonenschutz)**.
2. Klicken Sie auf **Add (Hinzufügen)**.
3. Geben Sie einen **Namen** und eine **Beschreibung** für Ihr Zonenschutzprofil ein.
4. Wählen Sie die Zonenschutzdienste aus.
5. Klicken Sie auf **OK**.

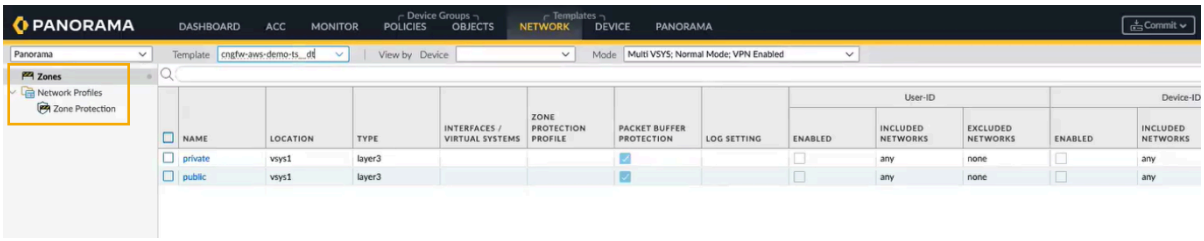
Nachdem Sie die Zonenschutzprofile erstellt haben, führen Sie die folgenden Schritte aus, um die **privaten** und **öffentlichen** Zonen Ihrer Standardvorlage zu verknüpfen:

**STEP 5 |** Wählen Sie in der Panorama-Konsole die Registerkarte **Networks (Netzwerke)** aus.

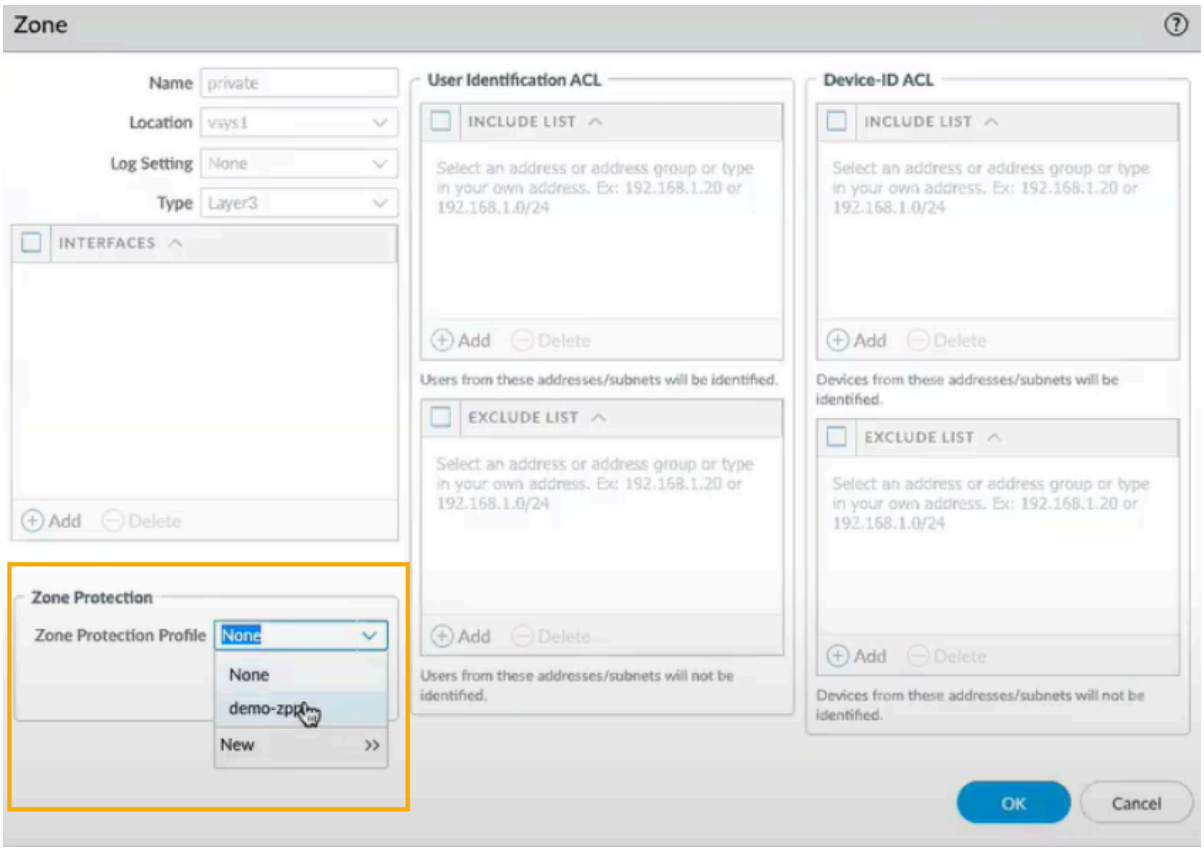
**STEP 6 |** Wählen Sie Ihre **Vorlage** aus.

**STEP 7 |** Gehen Sie zu **Zones (Zonen)**.



**STEP 8 |** Klicken Sie auf **Private (Privat)** und wählen Sie das **Zonenschutzprofil** für Ihre **private Zone** aus.

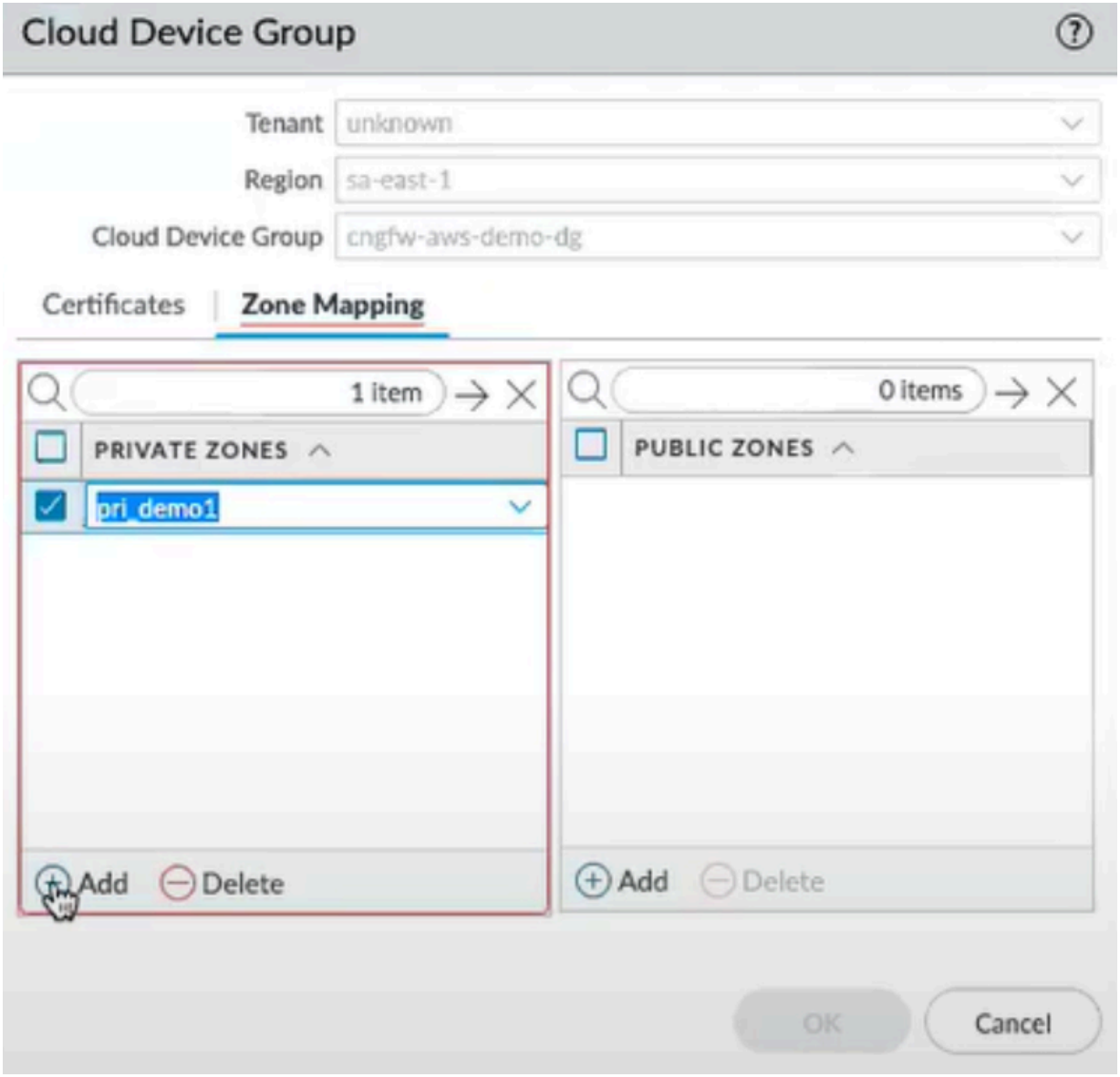



**STEP 9 |** Klicken Sie auf **Public (Öffentlich)** und wählen Sie das **Zonenschutzprofil** für Ihre **öffentliche Zone** aus.

**STEP 10 |** Navigieren Sie zurück zu Ihrer Cloud-Gerätegruppe. Gehen Sie zur Registerkarte **Zone Mapping (Zonenzuordnung)**.

Es wird die Liste der Panorama-Vorlagen angezeigt, auf die Sie in der Vorlagenstackliste verwiesen haben. Sie können die Panorama-Zonen den **privaten** und **öffentlichen** Standardzonen zuordnen, die vom AWS-Plug-in erstellt werden.




**STEP 11 |** Konfigurieren Sie Sicherheitsrichtlinienregeln für Cloud-Gerätegruppen in Panorama. Sie können dann die oben zugewiesenen Panorama-Sicherheitszonen, **private** oder **öffentliche** Standardzonen in

Ihren Sicherheitsrichtlinien als Quell- oder Zielzonen verwenden. Weitere Informationen finden Sie im Abschnitt Richtlinie anwenden.

*„Private-to-Public“ (Privat-zu-Öffentlich), „Public-to-Private“ (Öffentlich-zu-Privat), „Private-to-Private“ (Privat-zu-Privat), „Any-to-Any“ (Beliebig-zu-Beliebig) und „Private-to-Any“ (Privat-zu-Beliebig) sind die zulässigen zonenbasierten Richtlinienregeln in den Panorama Cloud-Gerätegruppen. Jede andere Kombination aus Quell- und Zielsicherheitszonen wird in Ihren Sicherheitsregeln nicht unterstützt.*

**STEP 12 |** Führen Sie einen **Commit** aus und übertragen Sie Ihre Änderungen per **Push** an Panorama.

**STEP 13 |** Melden Sie sich bei Ihrer Cloud NGFW-Konsole an, um Ihre XML-Datei zu überprüfen, die Zuordnungen **privater** und **öffentlicher** Zonen enthält, die von Panorama an die jeweilige Cloud-Gerätegruppe übertragen wurden.

**STEP 14 |** Gehen Sie zu **Rulestacks (Regelstapel)**, wählen Sie Ihre Cloud-Gerätegruppe aus und klicken Sie auf **View XML (XML anzeigen)**, um Informationen zu neu hinzugefügten **privaten** und **öffentlichen** Zonen von Panorama zur Cloud-Gerätegruppe anzuzeigen.

*Mithilfe der im obigen Verfahren beschriebenen Schritte können Sie auch zonenbasierte Richtlinienregeln für Ihre vorhandenen Cloud-Gerätegruppen konfigurieren, indem Sie die vorhandenen Vorlagen aus dem Vorlagenstack hinzufügen und dann Sicherheitsrichtlinienregeln für diese Cloud-Gerätegruppen in Panorama konfigurieren.*

# Strata Cloud Manager für die Richtlinienverwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Sie können Ihre Cloud NGFW-Ressource mit Strata Cloud Manager (SCM) für die Richtlinienverwaltung verknüpfen. Strata Cloud Manager bietet eine einheitliche Verwaltungslösung für Ihre gesamte Netzwerksicherheitsbereitstellung, sodass Sie Ihre Palo Alto Networks Sicherheitsinfrastruktur einfach von einer einzigen optimierten Weboberfläche aus verwalten können. Mit dieser Oberfläche erhalten Sie einen umfassenden Überblick über Benutzer, Zweigstellen, Anwendungen und Bedrohungen an allen Punkten zur Durchsetzung der Netzwerksicherheit. Diese Funktion bietet umsetzbare Erkenntnisse, höhere Sicherheit sowie einfache Fehlerbehebung und Problemlösung.

Beachten Sie bei der Verwendung von SCM für die Richtlinienverwaltung in Cloud NGFW Folgendes:

- Wenn Sie zum ersten Mal eine Verbindung zu SCM herstellen, werden Cloud NGFW-Ressourcen (z. B. die Ressourcen-ID) möglicherweise nicht angezeigt. Diese Ressourcen werden nach wenigen Augenblicken angezeigt, wenn keine zugrunde liegenden Verbindungsprobleme vorliegen.
- Die Best Practices für die SCM-Richtlinienverwaltung der Cloud NGFW unterscheiden sich von denen, die die Panorama-Richtlinienverwaltung mit Ihrer Cloud NGFW-Ressource verwenden. Beispielsweise kann ein Teil des Passthrough-Datenverkehrs in einer von Panorama verwalteten Umgebung in einer von SCM verwalteten Cloud NGFW-Ressource verloren gehen.
- X-Forwarded-Funktionen werden in einer SCM-Richtlinienverwaltung für Ihre Cloud NGFW-Ressource nicht unterstützt.
- Das Cloud-Zertifikat wird nicht unterstützt.
- DLP wird nicht unterstützt.
- Wenn Sie Sicherheitsregeln für Ihre SCM-verwaltete Cloud NGFW-Ressource konfigurieren, müssen Sie für die Sicherheitsregel **ANY (BELIEBIG)** angeben. Die Zone **from/to (von/bis)** wird jedoch im Strata-Protokollierungsdienst als **Datenzone** angezeigt.

## Ihre Cloud NGFW-Ressource mit Strata Cloud Manager für die Richtlinienverwaltung verknüpfen

So integrieren Sie Ihre Cloud NGFW-Ressource in Strata Cloud Manager für die Richtlinienverwaltung:

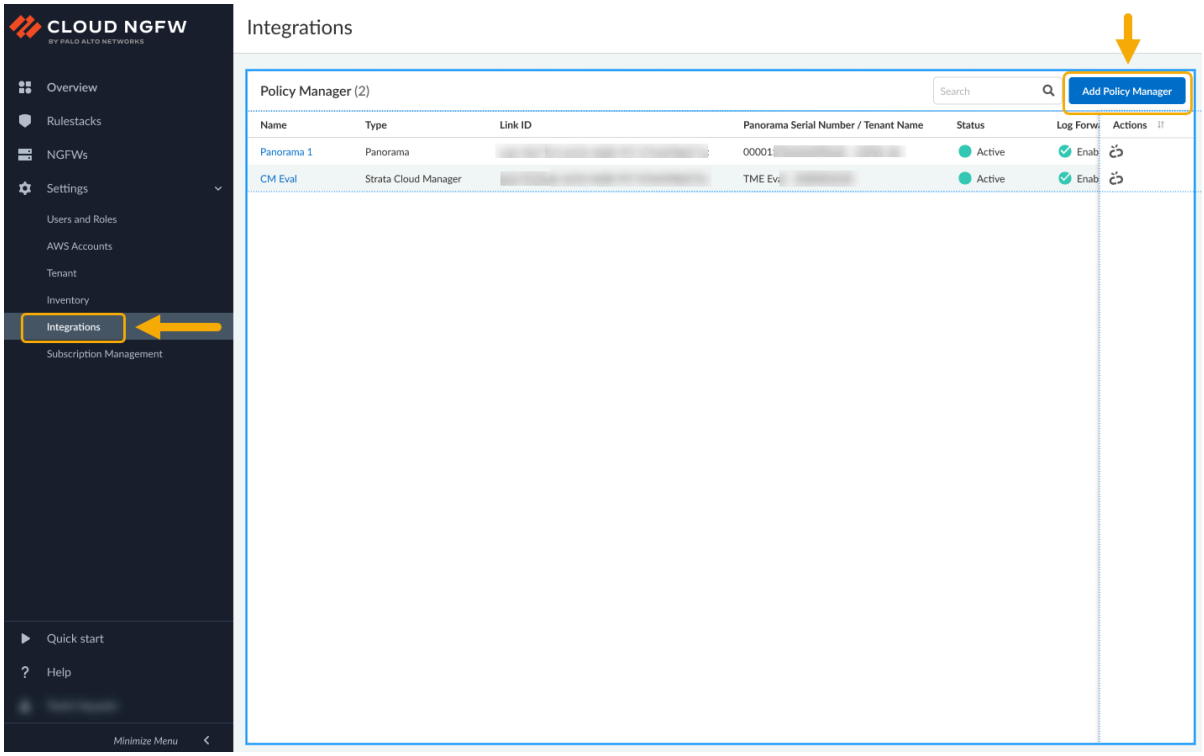
**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Wählen Sie **Integrations (Integrationen)** aus.

**STEP 3 |** Klicken Sie im Fenster **Policy Manager (Richtlinien-Manager)** auf **Add Policy Manager (Richtlinien-Manager hinzufügen)**.

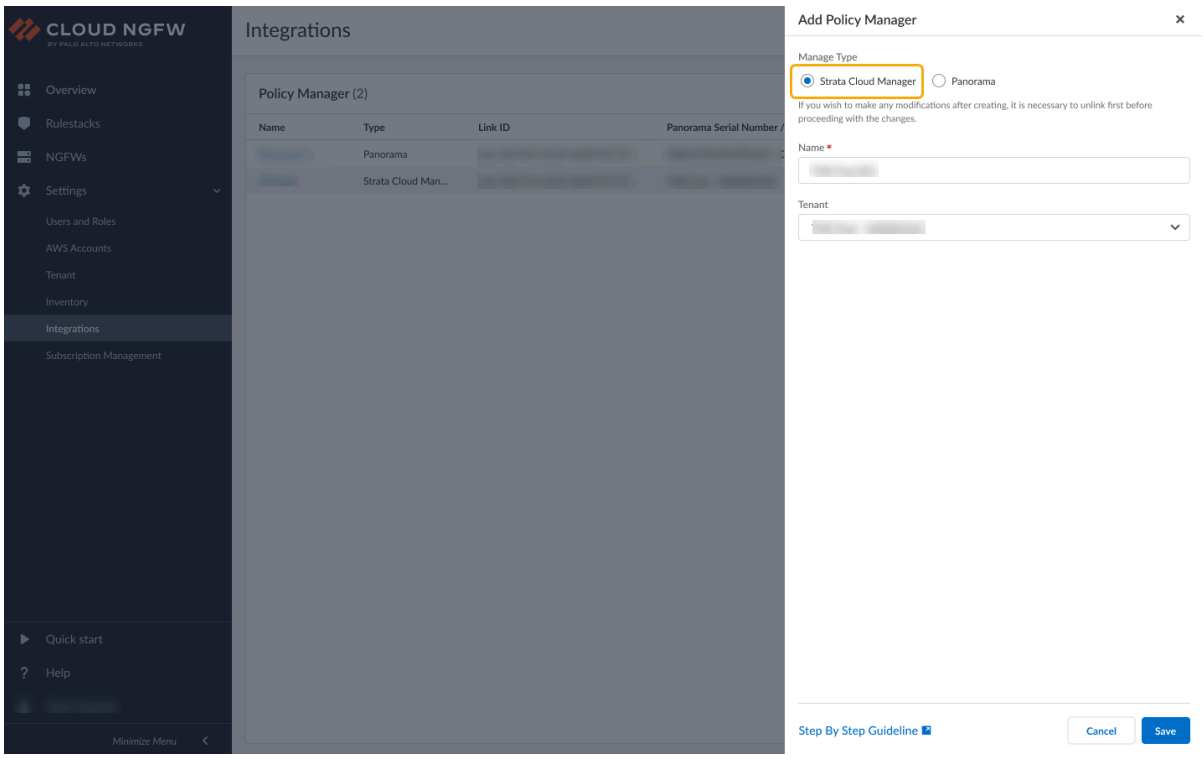
 



**STEP 4 |** Wählen Sie im Abschnitt **Add Policy Manager (Richtlinien-Manager hinzufügen)** unter **Manage Type (Verwaltungstyp)** die Option **Strata Cloud Manager** aus.



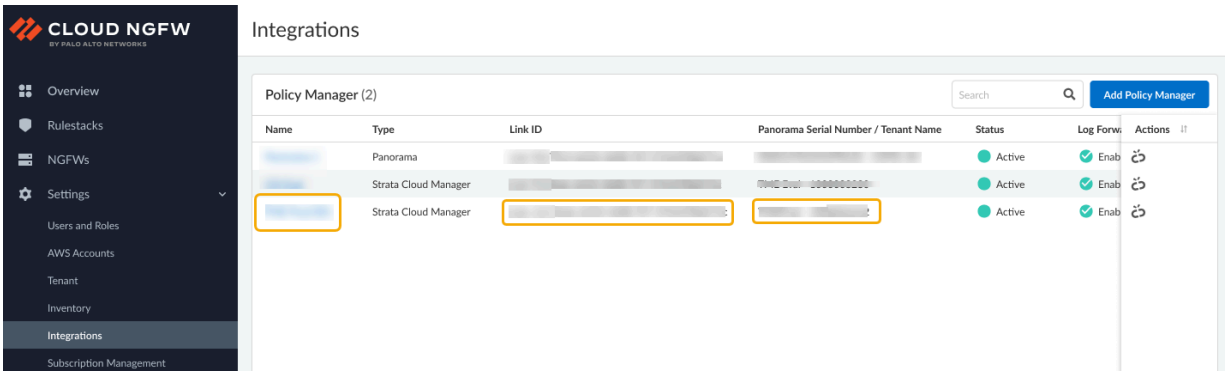
**STEP 5 |** Geben Sie einen beschreibenden Namen ein.

**STEP 6 |** Verwenden Sie das Dropdown-Menü, um den SCM-**Mandanten** auszuwählen, den Sie der Ressource zuordnen möchten.

*Für SCM und CNGFW muss dasselbe Customer-Support-Portal(CSP)-Konto verwendet werden.*

**STEP 7 |** Klicken Sie auf **Save (Speichern)**. Dadurch wird Ihre Cloud NGFW-Ressource effektiv mit dem SCM-Mandanten verknüpft.

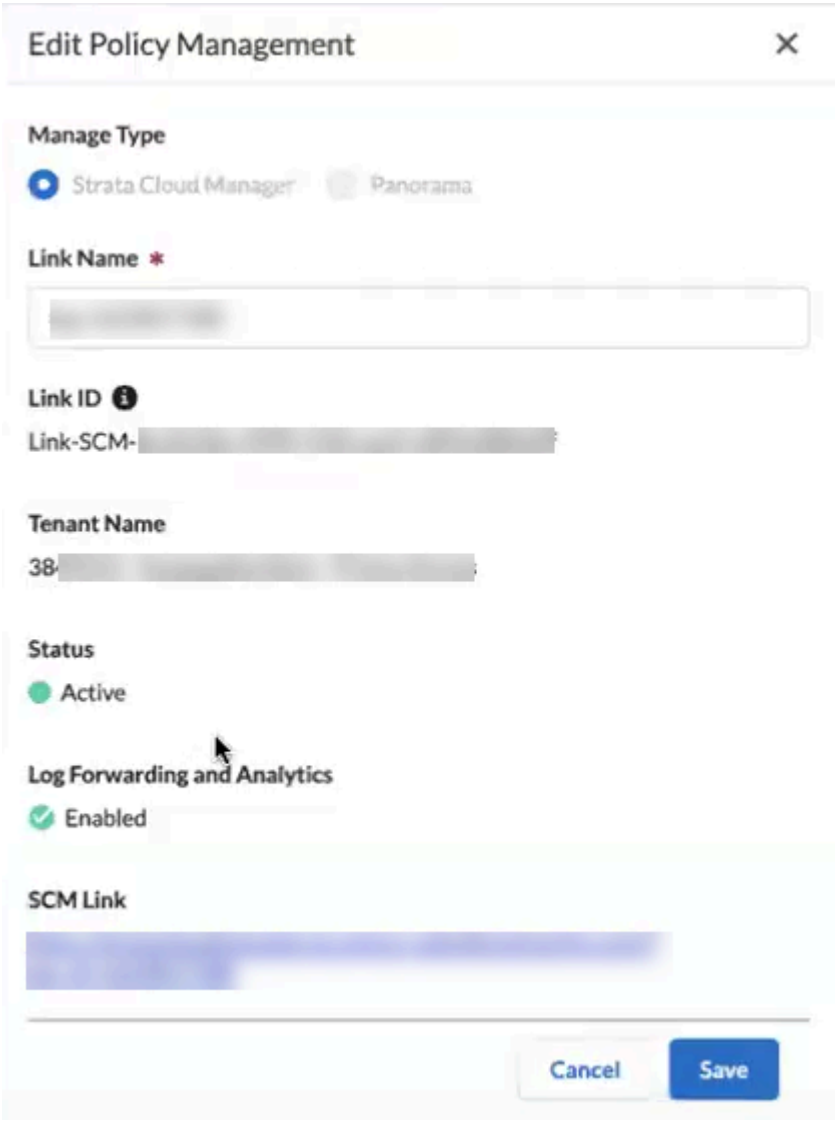
Nach dem Speichern der Konfiguration wird die Seite **Integrations (Integrationen)** aktualisiert, um das neue Richtlinienverwaltungsparadigma zusammen mit der zugeordneten Verknüpfungs-ID sowie der SCM-Seriennummer und dem Mandantennamen widerzuspiegeln:




Um Informationen über einen einzelnen verknüpften SCM-Mandanten anzuzeigen, klicken Sie im Fenster **Policy Manager (Richtlinien-Manager)** auf die **Verknüpfungs-ID**. Sie können im Bildschirm

**Edit Policy Management (Richtlinienverwaltung bearbeiten)** den **Verknüpfungsnamen** ändern und Informationen anzeigen:




## Firewall zur Richtlinienverwaltung des Strata Cloud Managers zuordnen

Nachdem Sie eine Verbindung zur Strata Cloud-Richtlinienverwaltung hergestellt haben, können Sie dem verknüpften SCM-Mandanten eine neue Firewall zuordnen:

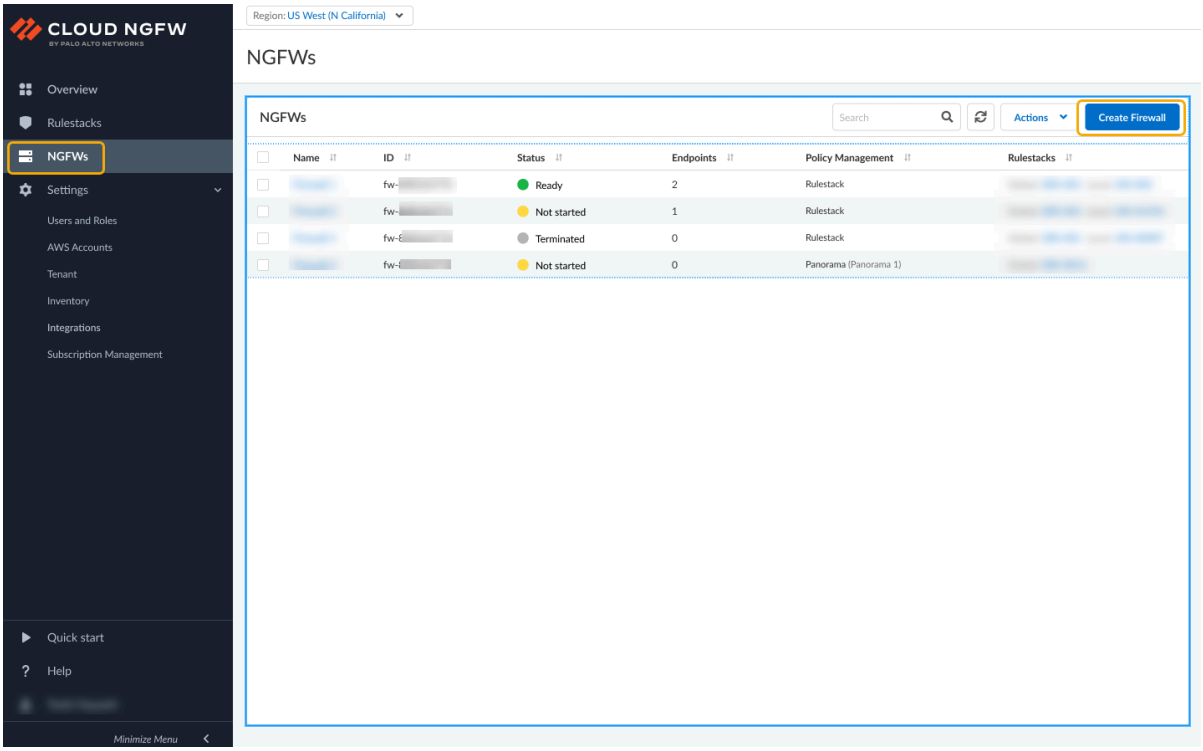
**STEP 1 |** Melden Sie sich bei der Cloud NGFW-Konsole an.

**STEP 2 |** Wählen Sie **NGFWs** aus.

**STEP 3 |** Klicken Sie auf **Create Firewall (Firewall erstellen)**.



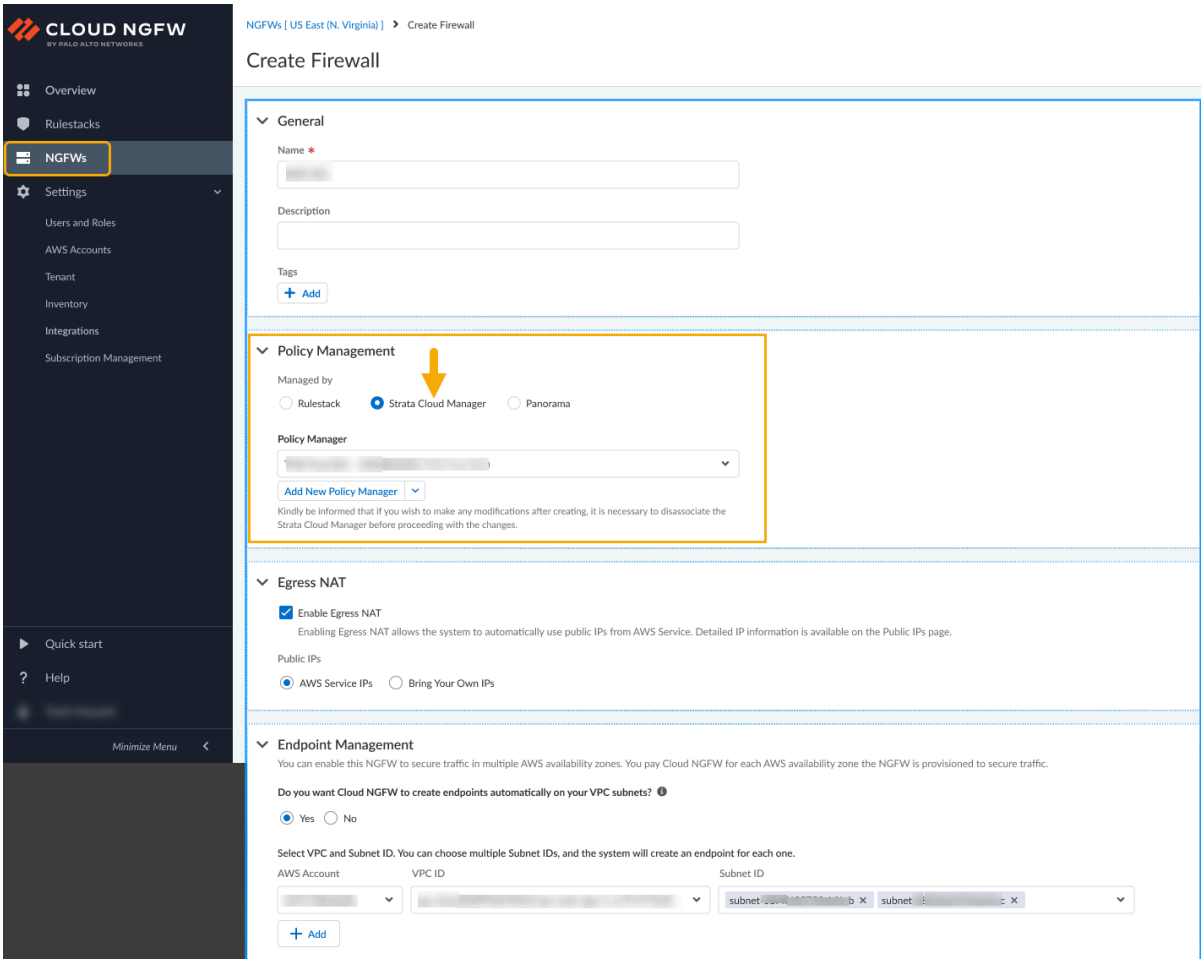
**STEP 4 |** Geben Sie im Bildschirm **Create Firewall (Firewall erstellen)** einen Namen für die Firewall ein.

**STEP 5 |** Fügen Sie optional eine Beschreibung hinzu.

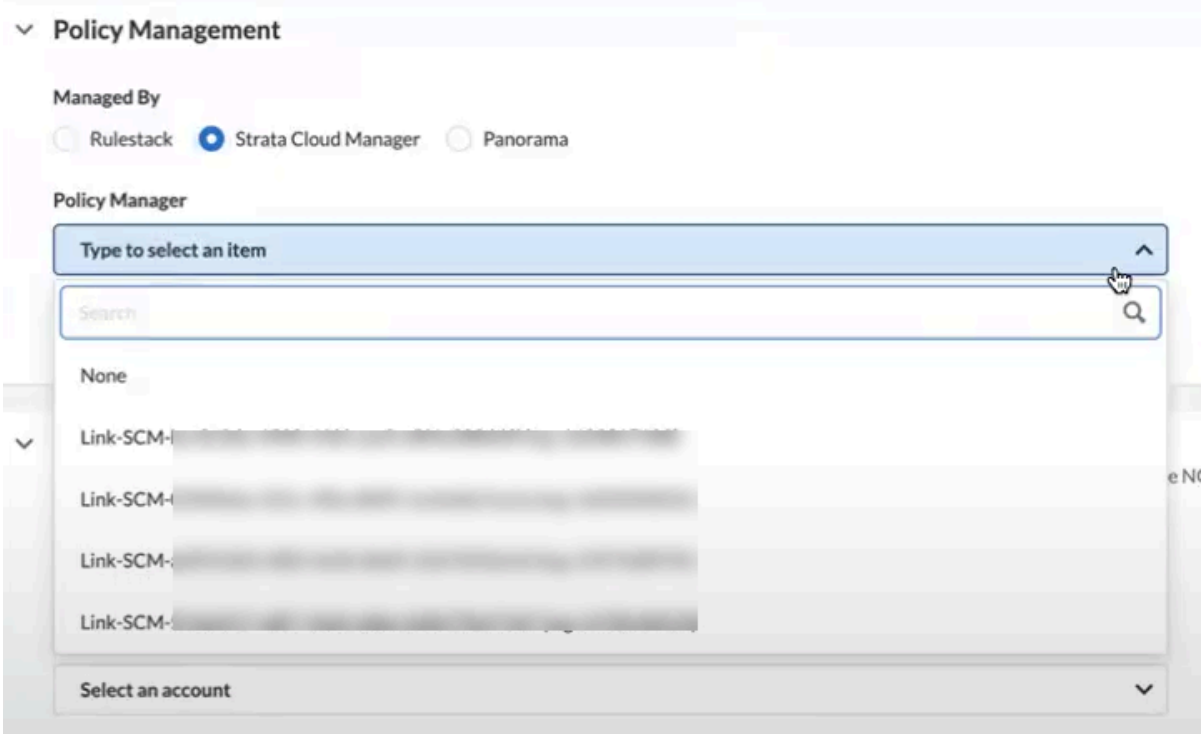
**STEP 6 |** Wählen Sie im Abschnitt **Policy Management (Richtlinienverwaltung)** die Option **Strata Cloud Manager** aus.



**STEP 7 |** Wählen Sie im Dropdown-Menü **Policy Manager (Richtlinien-Manager)** den verknüpften SCM-Mandanten aus, den Sie der Firewall zuordnen möchten.



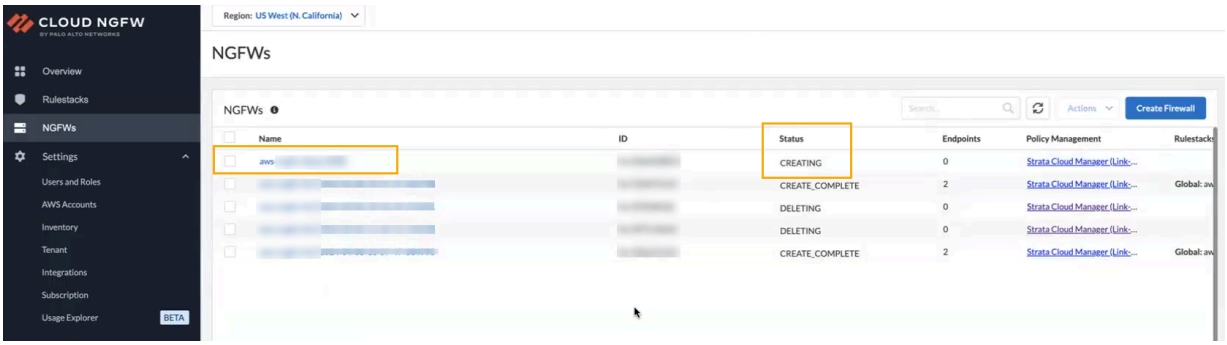
**STEP 8 |** Konfigurieren Sie **Endpunktverwaltung**, um den Datenverkehr in mehreren AWS-Verfügbarkeitszonen abzusichern.

1. Legen Sie fest, ob Cloud NGFW in Ihren VPC-Subnetzen Endpunkte automatisch erstellen soll. Wählen Sie **Yes (Ja)** aus, wenn die *Endpunkte durch den Dienst verwaltet werden sollen*.

   *Standardmäßig erstellt die Cloud NGFW-Ressource diese Endpunkte nicht automatisch; das Optionsfeld ist auf **No (Nein)** gesetzt.*

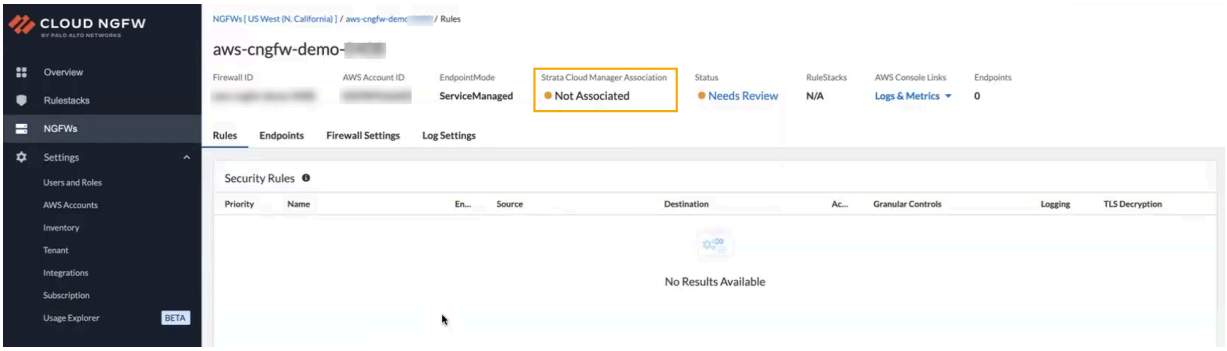
2. Wählen Sie aus der Dropdown-Liste die **AWS-Konto-ID** aus.
3. Wählen Sie aus der Dropdown-Liste die **VPC** aus.
4. Wählen Sie im Feld **Subnet (Subnetz)** ein verfügbares Subnetz aus.
5. Klicken Sie auf **Save (Speichern)**.

Der NGFW-Bildschirm ändert sich und spiegelt die neu erstellte Firewall wider. Das Erstellen einer neuen Firewall dauert ungefähr 6–10 Minuten. In der Spalte **Status** wird **CREATING (WIRD ERSTELLT)** angezeigt:




Klicken Sie auf den **NGFW-Namen**, um detaillierte Informationen zur Firewall anzuzeigen. Beim Erstellen der Firewall werden nur begrenzte Informationen angezeigt:




# Firewall in Strata Cloud Manager anzeigen

Nachdem Sie Ihre Cloud NGFW-Ressource mit einem SCM-Mandanten verknüpft und eine Firewall erstellt haben, können Sie SCM für die Richtlinienverwaltung verwenden.

*Wenn Sie sich bei Strata Cloud Manager anmelden, zeigt das Dashboard die Anzahl der Cloud NGFWs unter **NGFW > Software** nicht an.*

**STEP 1 |** Melden Sie sich über den Palo Alto Networks Hub direkt bei der Strata Cloud Manager-App unter stratacloudmanager.paloaltonetworks.com an.

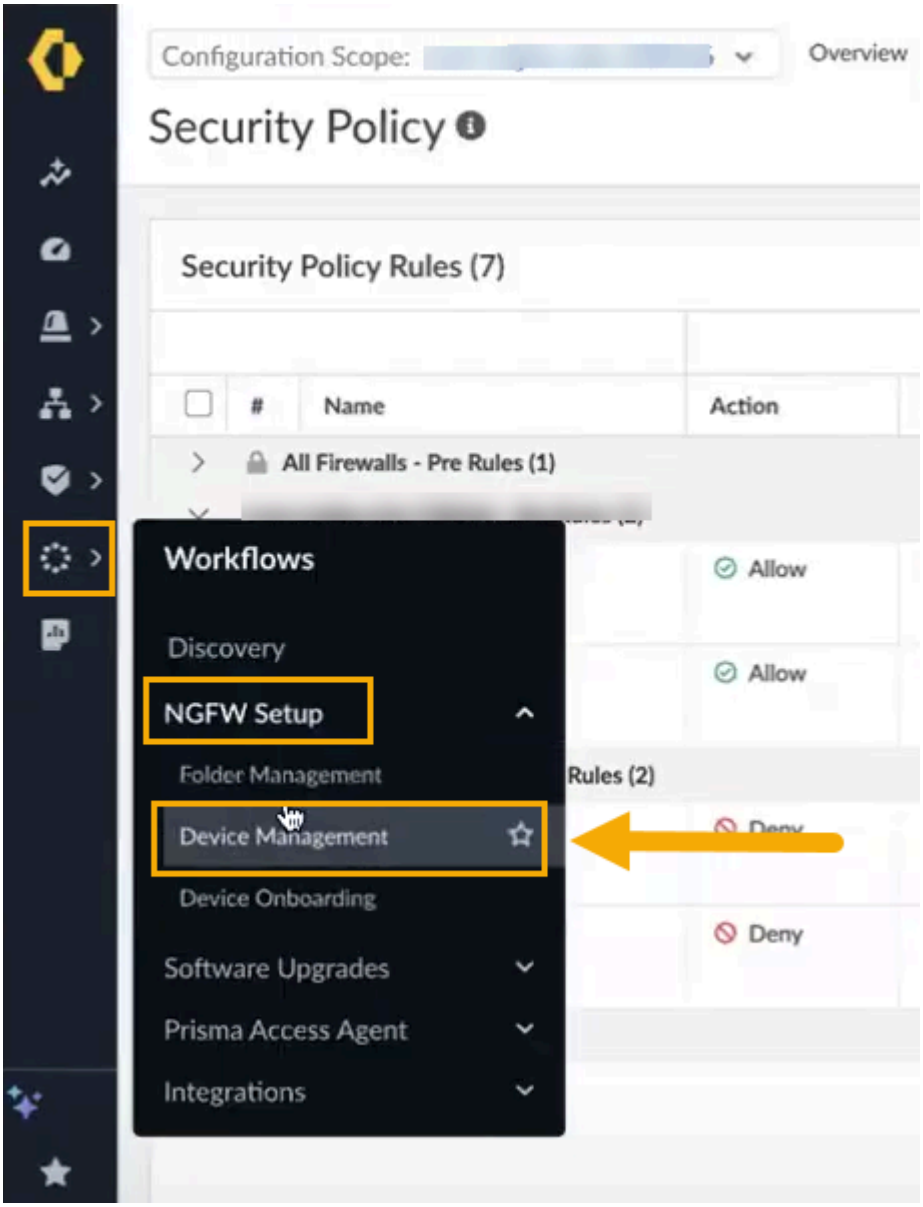
 

**STEP 2 |** Suchen Sie in der Strata Cloud Manager-Oberfläche Ihren Cloud NGFW-Mandanten mithilfe der linken Navigationsoption:

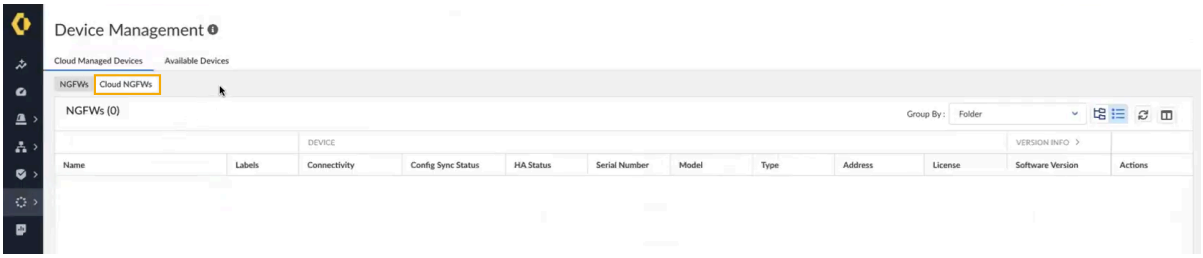
Dadurch werden die verfügbaren Mandanten angezeigt, die mit Ihrer Cloud NGFW-Ressource verknüpft sind. Sie können alternativ mithilfe des *Mandantennamens* oder der *Mandanten-ID* nach dem Mandanten suchen.

**STEP 3 |** Wählen Sie **Workflows > NGFW Setup > Device Management (Workflows > NGFW-Setup > Geräteverwaltung)** aus:

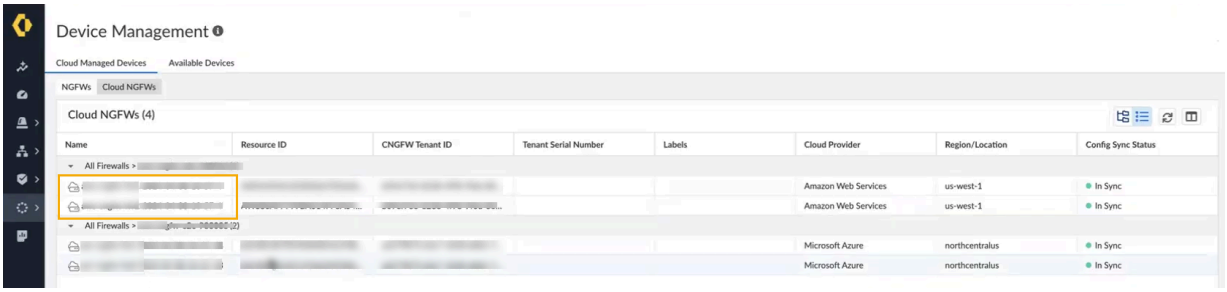


**STEP 4 |** Im Bildschirm „Device Management“ (Geräteverwaltung) werden die **NGFWs** und **Cloud NGFWs** angezeigt. Klicken Sie auf **Cloud NGFWs**, um die dem SCM-Mandanten zugeordneten Firewalls anzuzeigen:




Im Bildschirm **Device Management (Geräteverwaltung)** werden die Cloud NGFW-Ressourcen angezeigt, die derzeit von SCM verwaltet werden:



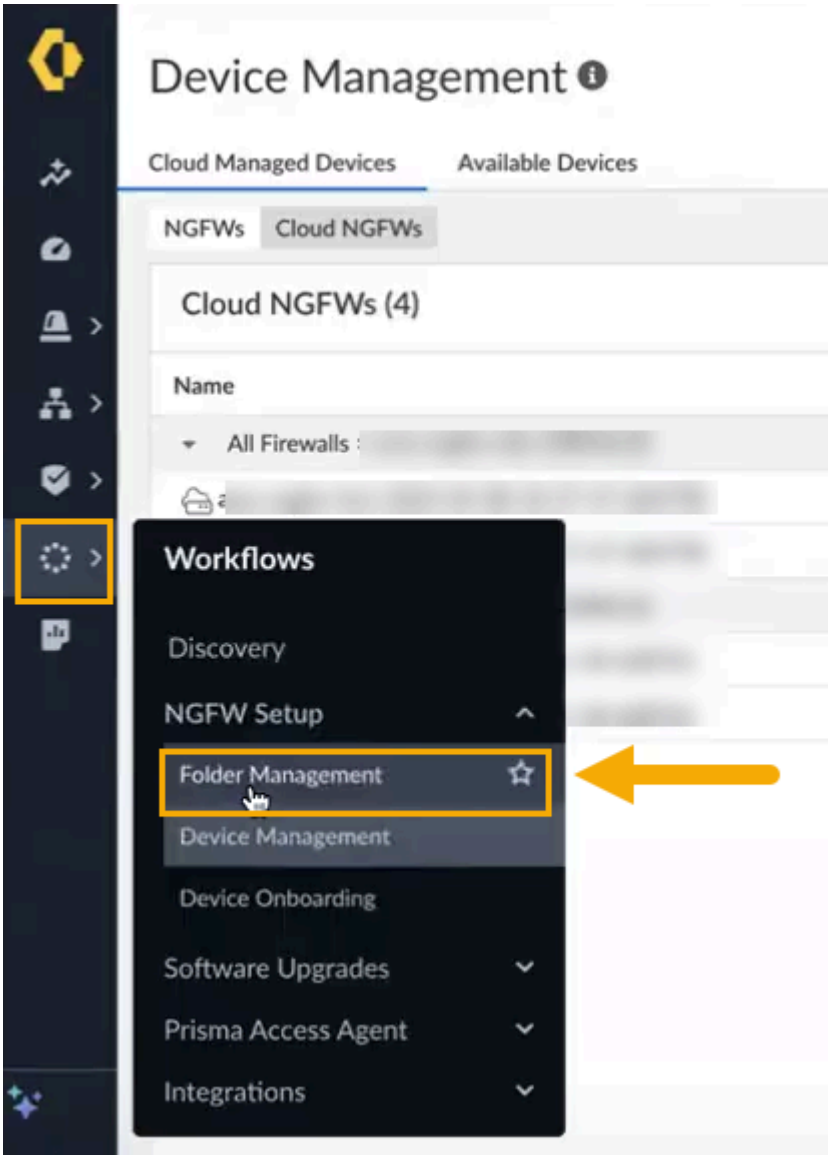

Im Bildschirm „Device Management“ (Geräteverwaltung) werden die folgenden Felder angezeigt:

- Name. Gibt den Namen der Cloud NGFW-Ressource an.
- Resource ID (Ressourcen-ID). Gibt die Ressourcen-ID an, die der NGFW-Ressource zugeordnet ist.
- CNGFW Tenant ID (CNGFW-Mandanten-ID). Die ID, die dem Cloud NGFW-Mandanten zugeordnet ist, der mit SCM verknüpft ist.
- CNGFW Tenant Serial Number (Seriennummer des CNGFW-Mandanten). Die dem Cloud NGFW-Mandanten zugeordnete Seriennummer.
- Labels (Bezeichnungen). Eine beliebige Bezeichnung, die der Cloud NGFW zugewiesen wurde.
- Cloud Provider (Cloud-Anbieter). Gibt den Cloud-Anbieter an, der der Cloud NGFW-Ressource zugeordnet ist.
- Region und Standort. Die Region, in der sich die Cloud NGFW-Ressource befindet.
- Status der Konfigurationssynchronisierung. Der Status der Cloud NGFW-Ressource.

**STEP 5 |** Im Bildschirm **Device Management (Geräteverwaltung)** sind Ihre Cloud NGFW-Ressourcen in *Ordnern* gruppiert. Zum Anzeigen der Struktur dieser Ordner wählen Sie **Workflows > Folder Management (Workflows > Ordnerverwaltung)** aus:




Im Bildschirm **Folder Management (Ordnerverwaltung)** werden die Cloud NGFW-Ressourcen angezeigt, die dem SCM-Mandanten zugeordnet sind:

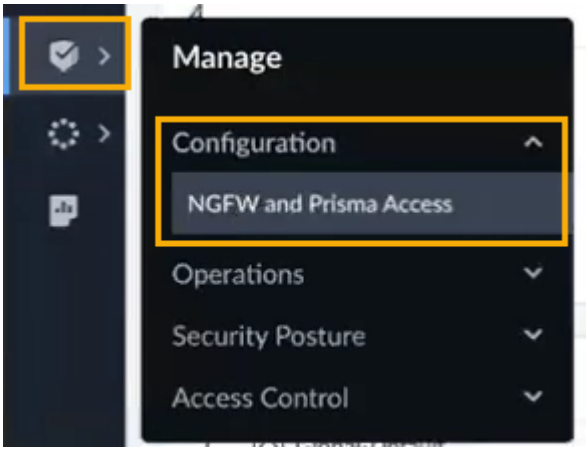

*Informationen zum Erstellen von Ordnern finden Sie unter* Ordner für Ihre Cloud NGFW-Ressource mithilfe von Strata Cloud Manager erstellen.

## Strata Cloud Manager für die Richtlinienverwaltung in Cloud NGFW verwenden

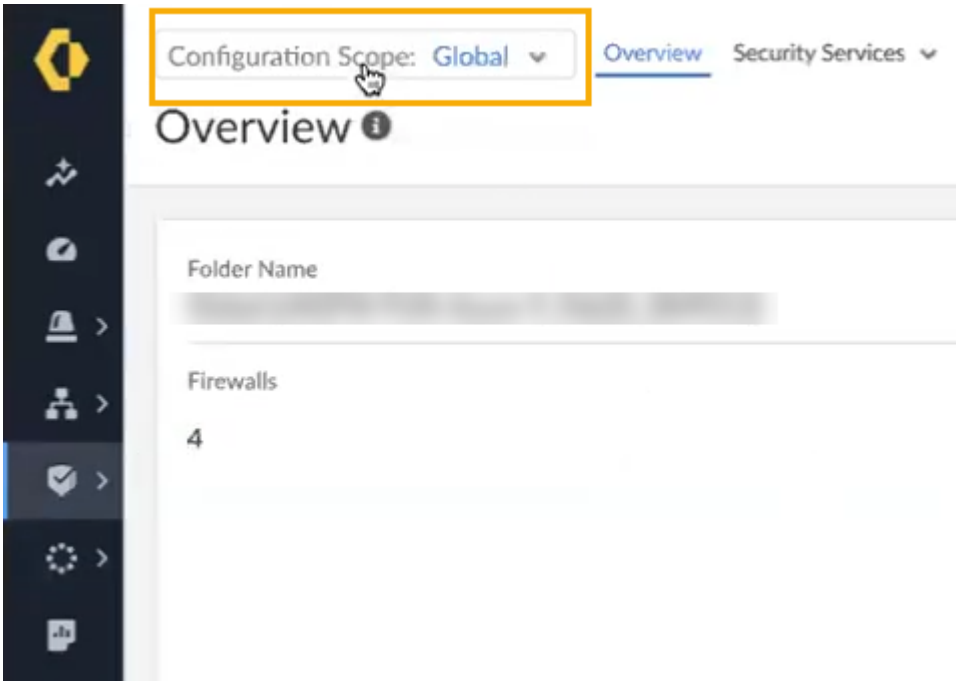
Sie können Strata Cloud Manager verwenden, um Sicherheitsrichtlinienregeln global auf die Cloud NGFW-Ressourcen anzuwenden, die in einem Ordner enthalten sind.

**STEP 1 |** Wählen Sie in Strata Cloud Manager die Optionen **Manage > Configuration > NGFW and Prisma Access (Verwalten > Konfiguration > NGFW und Prisma Access)** aus.

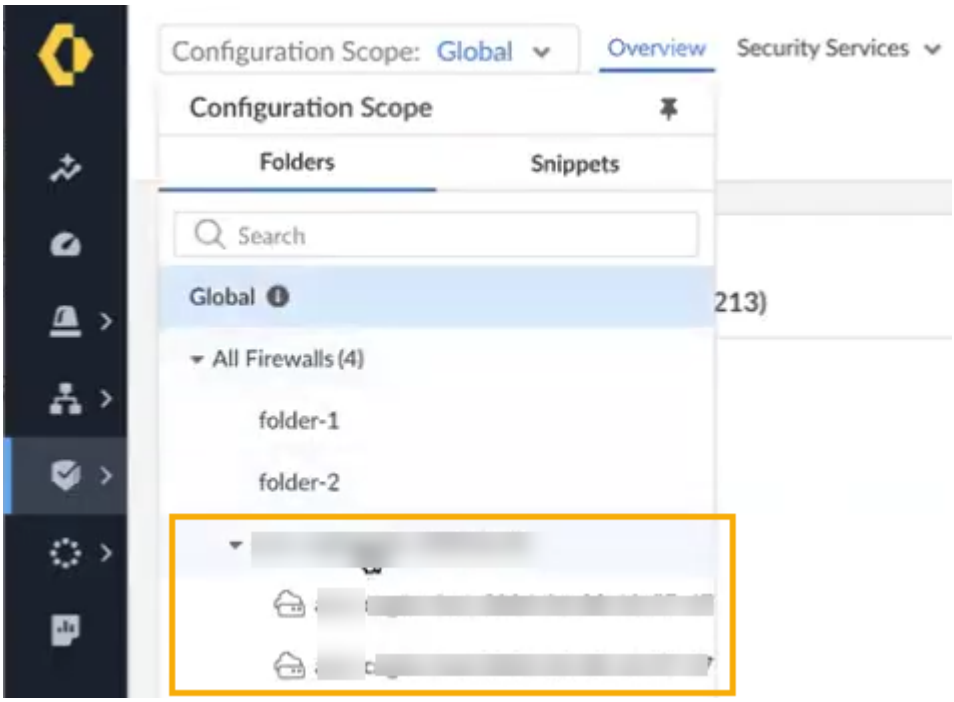



**STEP 2 |** Wählen Sie **Configuration Scope (Konfigurationsumfang)** aus.



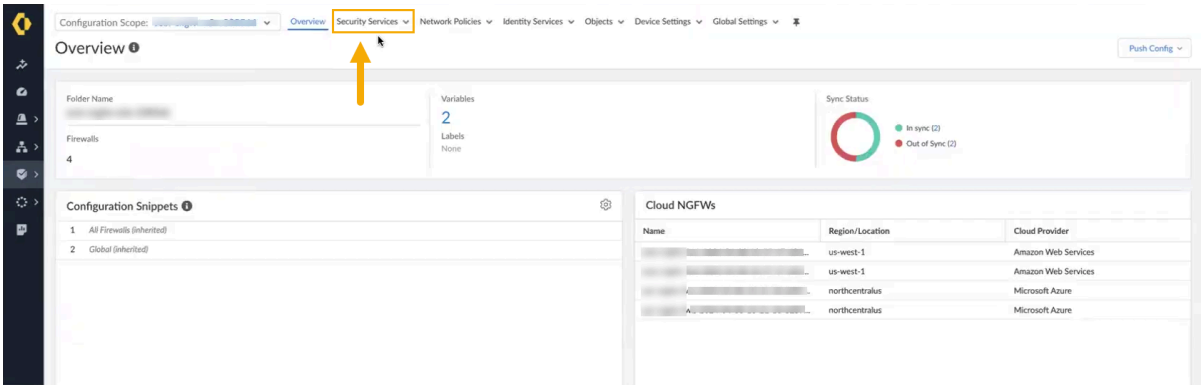

 

**STEP 3 |** Suchen Sie in der Dropdown-Liste den Ordner, der die **Cloud NGFW AWS-Ressourcen** enthält:



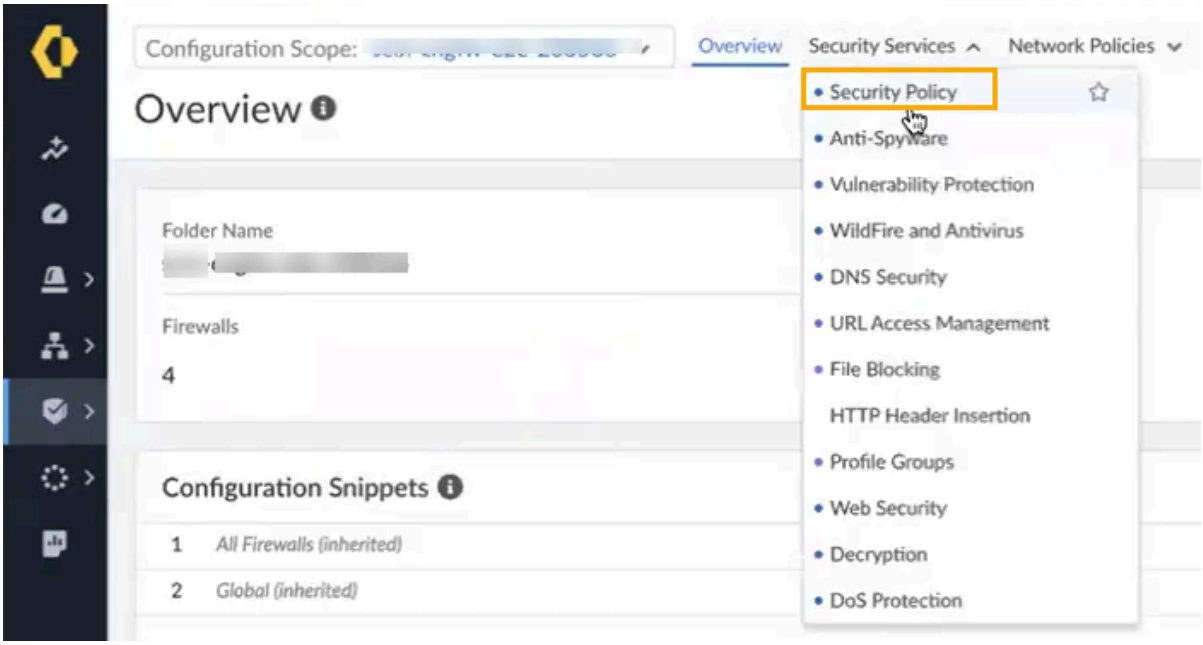

 

**STEP 4 |** Wählen Sie auf der Seite **Overview (Übersicht)** die Option **Security Services (Sicherheitsdienste)** aus:



**STEP 5 |** Wählen Sie in der Dropdown-Liste **Security Services (Sicherheitsdienste)** die Option **Security Policy (Sicherheitsrichtlinie)** aus:




Weitere Informationen zur Konfiguration der Sicherheitsrichtlinie mit Strata Cloud Manager finden Sie unter Verwalten: Sicherheitsrichtlinie.

## Ordner für Ihre Cloud NGFW-Ressource mithilfe von Strata Cloud Manager erstellen

Nachdem Sie das entsprechende Abonnement für die Nutzung des Strata Cloud Manager-Dienstes für Ihre Cloud NGFW-Ressource konfiguriert haben, erstellen Sie einen Ordner, in dem Sie die Ihrer Firewall zugeordneten Daten anzeigen können. Ordner werden verwendet, um Ihre Firewalls oder Bereitstellungstypen (z. B. eine Dienstverbindung für Ihre Cloud NGFW-Ressource) logisch zu gruppieren und so die Konfigurationsverwaltung zu vereinfachen. Sie können einen Ordner erstellen, der mehrere verschachtelte Ordner enthält, um Firewalls und Bereitstellungen zu gruppieren, die ähnliche Konfigurationen erfordern. Bereits verschachtelte Ordner können auch mehrere verschachtelte Ordner enthalten.

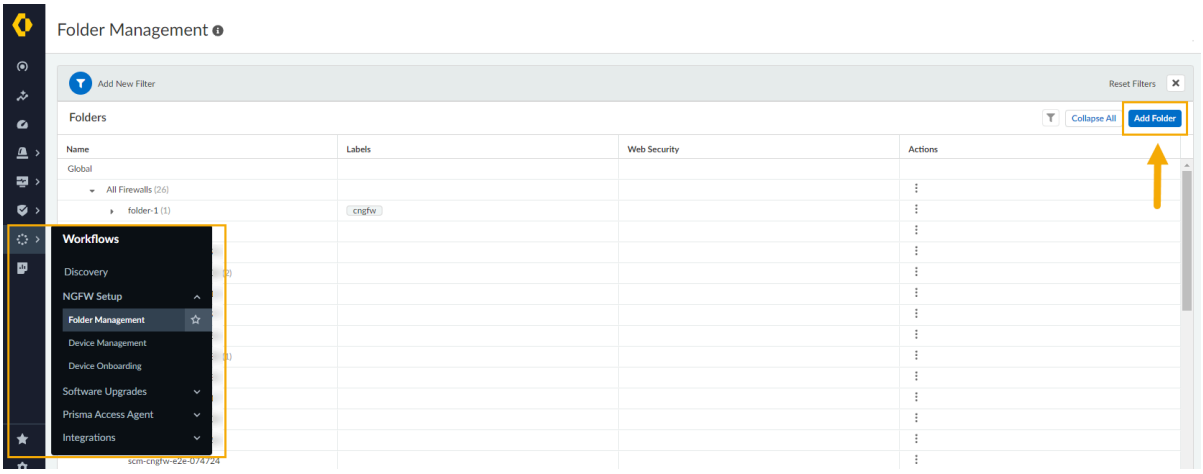
*Ordner für andere Palo Alto Networks Anwendungen wie Prisma Access und Ihre NGFWs werden getrennt verwaltet, d. h. Sie können NGFWs nicht in einem Ordner mit Prisma Access-Bereitstellungen gruppieren. Sie können jedoch freigegebene Einstellungen problemlos global auf alle Ordner anwenden oder mithilfe von Manage: Snippets (Verwalten: Snippets) Standardeinstellungen und Richtlinienanforderungen auf mehrere Ordner anwenden.*

So erstellen Sie einen Ordner für Ihre Cloud NGFW-Ressource:

**STEP 1 |** Melden Sie sich über den Palo Alto Networks Hub direkt bei der Strata Cloud Manager-App unter stratacloudmanager.paloaltonetworks.com an.

**STEP 2 |** Wählen Sie in der Strata Cloud Manager-Oberfläche die Optionen **Workflows > NGFW Setup > Folder Management (Workflows > NGFW-Setup > Ordnerverwaltung)** aus und klicken Sie auf **Add Folder (Ordner hinzufügen)**.




**STEP 3 |** Gehen Sie im Bildschirm **Create Folder (Ordner erstellen)** wie folgt vor:

1. Geben Sie einen beschreibenden Namen für den Ordner ein.
2. Optional können Sie eine Beschreibung für den Ordner angeben.
3. Weisen Sie optional eine oder mehrere Bezeichnungen zu. Sie können eine vorhandene Bezeichnung auswählen oder eine neue Bezeichnung erstellen, indem Sie die Bezeichnung

eingeben, die Sie erstellen möchten. Wählen Sie beispielsweise aus der Dropdown-Liste **Labels (Bezeichnungen)** die Option **cngfw** aus.

4. Geben Sie mithilfe des Dropdown-Menüs an, wo der Ordner erstellt werden soll. Sie können **All Firewalls (Alle Firewalls)** auswählen oder alternativ einen vorhandenen Ordner auswählen, um den Ordner darunter zu verschachteln. Dies ist ein erforderliches Feld.
5. Klicken Sie auf **Create (Erstellen)**.

Geben Sie einen beschreibenden Namen für den Ordner ein.

## Überwachung und Fehlerbehebung mit Strata Cloud Manager

Sie können Strata Cloud Manager verwenden, um sich über den Status Ihrer Cloud NGFW-Ressource zu informieren. Verwenden Sie die Funktion **Monitor (Überwachen)** von SCM und erfahren Sie mehr über:

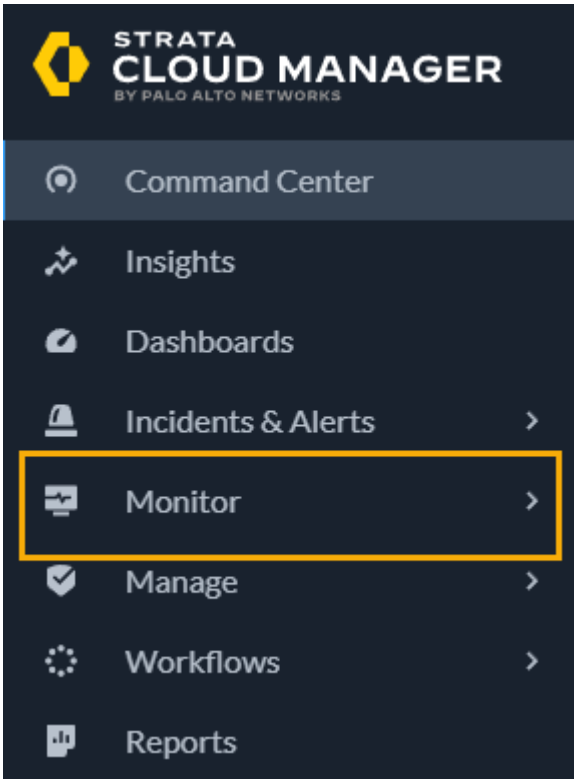
- Produkte und Abonnements, die Sie mit Strata Cloud Manager verwalten.
- Den Zustand und den Konnektivitätsstatus Ihrer Cloud NGFW-Geräte.

Weitere Informationen finden Sie unter Überwachung in Strata Cloud Manager.

So verwenden Sie Strata Cloud Manager zur Überwachung Ihrer Cloud NGFW-Ressource:

**STEP 1 |** Melden Sie sich über den Palo Alto Networks Hub direkt bei der Strata Cloud Manager-App unter stratacloudmanager.paloaltonetworks.com an.

**STEP 2 |** Wählen Sie in der Benutzeroberfläche **Monitor (Überwachen)** aus:



# Überwachen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Verschaffen Sie sich einen umfassenden Überblick über Ihren Netzwerkverkehr sowie die Produkte und Abonnements, die Sie mit Strata Cloud Manager verwalten. In Prisma Access können Sie den Zustand und den Konnektivitätsstatus Ihrer Remote-Netzwerke, Anwendungen, NGFW-Geräte und mobilen Benutzer schützend überwachen. Strata Cloud Manager bietet auch Funktionen zur Überwachung der Leistung gängiger Netzwerkdienste sowie der Verbrauchsdetails Ihrer Abonnementlizenzen und zur Verwaltung des Tools für die Analyse von Konnektivitätsproblemen.

Um potenziellen Problemen vorzubeugen und bei Bedarf die Reaktion auf Vorfälle zu beschleunigen, bietet die Firewall mithilfe anpassbarer und informativer Berichte Informationen über Datenverkehr und Benutzermuster. Über das Dashboard, das Application Command Center (ACC), Berichte und Protokolle in der Firewall können Sie die Aktivitäten in Ihrem Netzwerk überwachen. Sie können die Protokolle überwachen und die Informationen filtern, um Berichte mit vordefinierten oder benutzerdefinierten Ansichten zu erstellen. Sie können beispielsweise die vordefinierten Vorlagen verwenden, um Berichte über Benutzeraktivitäten zu erstellen, oder die Berichte und Protokolle analysieren, um ungewöhnliches Verhalten in Ihrem Netzwerk zu interpretieren und einen benutzerdefinierten Bericht über das Datenverkehrsmuster zu erstellen. Für eine visuell ansprechende Darstellung der Netzwerkaktivität enthalten das Dashboard und das ACC Widgets, Diagramme und Tabellen, mit denen Sie interagieren können, um die Informationen zu finden, die Ihnen wichtig sind. Darüber hinaus können Sie die Firewall so konfigurieren, dass überwachte Informationen wie E-Mail-Benachrichtigungen, Syslog-Meldungen, SNMP-Traps und NetFlow-Datensätze an externe Dienste weitergeleitet werden.

# Protokolle nativ in AWS anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Ein Protokoll ist eine automatisch generierte Datei mit Zeitstempel, die einen Prüfpfad für Systemereignisse auf der Firewall oder Netzwerkverkehrsereignisse bereitstellt, die von der Firewall überwacht werden. Protokolleinträge enthalten Artefakte, bei denen es sich um Eigenschaften, Aktivitäten oder Verhaltensweisen im Zusammenhang mit dem protokollierten Ereignis handelt, z. B. Anwendungstyp oder IP-Adresse eines Angreifers. Jeder Protokolltyp zeichnet Informationen für einen separaten Ereignistyp auf. Beispielsweise generiert die Firewall ein Bedrohungsprotokoll, um Datenverkehr aufzuzeichnen, der mit der Signatur einer Spyware, Sicherheitslücke oder Malware übereinstimmt, oder einen DoS-Angriff, der mit den Schwellenwerten übereinstimmt, die für eine Port-Scan- oder Host-Sweep-Aktivität auf der Firewall konfiguriert wurden.

Die Cloud NGFW kann Datenverkehrs-, Bedrohungs- und Entschlüsselungsprotokolle an einen S3-Bucket, eine CloudWatch-Protokollgruppe oder Kinesis Data Firehose senden. Die Namen dieser Protokollziele müssen in der CloudFormation-Vorlage (CloudFormation Template, CFT) der Cloud NGFW enthalten sein, die gestartet wird, wenn Sie Ihr Tenet Admin-AWS-Konto zur Cloud NGFW hinzufügen. Die CloudWatch-Protokollgruppe und Kinesis Data Firehose haben den Standardwert **PaloAltoCloudNGFW** in der CFT. Der S3-Bucket hat keinen Standardwert. Die Cloud NGFW erstellt diese Ressourcen nicht in Ihrer AWS-Umgebung. Die CFT erteilt der Cloud NGFW die Berechtigungen, die Protokolle an das Ziel zu schreiben. Ein Ziel mit dem Namen, den Sie in der CFT angegeben haben, muss in Ihrer Bereitstellung vorhanden sein, um NGFW-Protokolle erfolgreich zu erfassen.

*CloudWatch-Protokollgruppe, S3-Bucket, CloudWatch-Namespace und Kinesis-Stream sollten in der CloudFormation-Vorlage (CFT) vorab erstellt werden.*

## Protokolltypen

Cloud NGFW kann drei Arten von Protokollen erfassen und speichern.

- **Datenverkehr**: Datenverkehrsprotokolle enthalten einen Eintrag für den Beginn und das Ende jeder Sitzung. Weitere Informationen finden Sie unter Datenverkehrsprotokollfelder in Cloud NGFW für AWS.
- **Bedrohung**: Bedrohungsprotokolle enthalten Einträge, wenn der Datenverkehr mit einem der Sicherheitsprofile übereinstimmt, die einer Sicherheitsregel auf der Firewall zugeordnet sind. Jeder Eintrag enthält die folgenden Informationen: Datum und Uhrzeit, Art der Bedrohung (z. B. Malware

oder Spyware), Bedrohungsbeschreibung oder URL (Spalte „Name“), Alarmaktion (z. B. Zulassen oder Blockieren) und Schweregrad.

Weitere Informationen finden Sie unter Bedrohungsprotokollfelder in Cloud NGFW für AWS.

| Severity (Schweregrad) | Beschreibung |
|---|---|
| Kritisch | Schwerwiegende Bedrohungen, wie z. B. solche, die Standardinstallationen weit verbreiteter Software betreffen, führen zu einer Root-Kompromittierung von Servern, und der ausgenutzte Code ist für Angreifer weit verbreitet. Der Angreifer benötigt normalerweise keine speziellen Authentifizierungsdaten oder Kenntnisse über die einzelnen Opfer, und das Ziel muss nicht dazu manipuliert werden, spezielle Funktionen auszuführen. |
| Hoch | Bedrohungen, die kritisch werden können, aber abmildernde Faktoren haben. Beispielsweise können sie schwierig auszunutzen sein, nicht zu erhöhten Rechten führen oder nur einen kleinen Opferpool haben. |
| Mittel | Kleinere Bedrohungen, bei denen die Auswirkungen minimal sind, wie z. B. DoS-Angriffe, die das Ziel nicht gefährden, oder Exploits, die erfordern, dass sich ein Angreifer im selben LAN wie das Opfer befindet. Sie betreffen nur nicht standardmäßige Konfigurationen, verschleiern Anwendungen oder bieten sehr eingeschränkten Zugriff. |
| Niedrig | Bedrohungen der Stufe „Warnung“, die nur sehr geringe Auswirkungen auf die Infrastruktur einer Organisation haben. Sie erfordern normalerweise einen lokalen oder physischen Systemzugriff und können häufig zu Datenschutz- oder DoS-Problemen des Opfers und Informationslecks führen. |
| Informativ | Verdächtige Ereignisse, die keine unmittelbare Bedrohung darstellen, die aber gemeldet werden, um die Aufmerksamkeit auf tiefgreifendere Probleme zu lenken, die möglicherweise existieren könnten. Protokolleinträge für die URL-Filterung werden als informativ protokolliert. Protokolleinträge mit einem beliebigen Urteil und einer Aktion, die auf Blockieren eingestellt ist, werden als informativ protokolliert. |

- **Entschlüsselung**: Entschlüsselungsprotokolle enthalten standardmäßig Einträge für nicht erfolgreiche TLS-Handshakes und können Einträge für erfolgreiche TLS-Handshakes enthalten, wenn Sie sie in der Entschlüsselungsrichtlinie aktivieren. Wenn Sie Einträge für erfolgreiche Handshakes aktivieren, stellen Sie sicher, dass Sie über die Systemressourcen (Protokollspeicherplatz) für die Protokolle verfügen. Weitere Informationen finden Sie unter Entschlüsselungsprotokollfelder in Cloud NGFW für AWS.

# Protokollziel

Sie haben drei Auswahlmöglichkeiten für das Ziel Ihrer Cloud NGFW-Protokolle. Diese Ziele befinden sich alle außerhalb des Cloud NGFW-Diensts, aber innerhalb Ihres AWS-Kontos: S3-Bucket, Cloudwatch-Protokollgruppe oder Kinesis Data Firehose. Jede Protokolldatei wird als JSON-Datei generiert.

Wenn Sie Cloud NGFW für AWS abonnieren, werden Sie aufgefordert, Ihren AWS CloudFormation-Vorlagenstack einzurichten. Im Stapel sind die Protokollierungsziele für die CloudWatch-Protokollgruppe und den Kinesis Data Firehose-Bereitstellungsstream mit dem Ziel **PaloAltoCloudNGFW** vorab ausgefüllt. Das Feld „S3 Bucket“ (S3-Bucket) ist nicht vorab ausgefüllt. Wenn Sie die Protokolle an ein anderes Ziel senden möchten, müssen Sie dieses Ziel erstellen und den Standardwert ersetzen, bevor Sie die Erstellung des Stapels abschließen.

Jede NGFW-Ressource (angezeigt als NGFW-Name im Protokollstreamnamen) gibt ihre Protokolle in mehreren Streams aus (gekennzeichnet durch den String zufälliger Zeichen im Protokollstreamnamen). Daher können Protokolle für eine bestimmte Cloud NGFW-Ressource auf mehrere Streams verteilt sein.

Wenn Sie die Protokolle an eine CloudWatch-Protokollgruppe senden, können Sie die Protokolleinträge direkt in der AWS CloudWatch-Konsole anzeigen. In der CloudWatch-Protokollgruppe, die Sie beim Konfigurieren der Protokollierung angeben, sehen Sie eine Liste der Protokollstreams. Der Name des Protokollstreams wird wie folgt angezeigt:

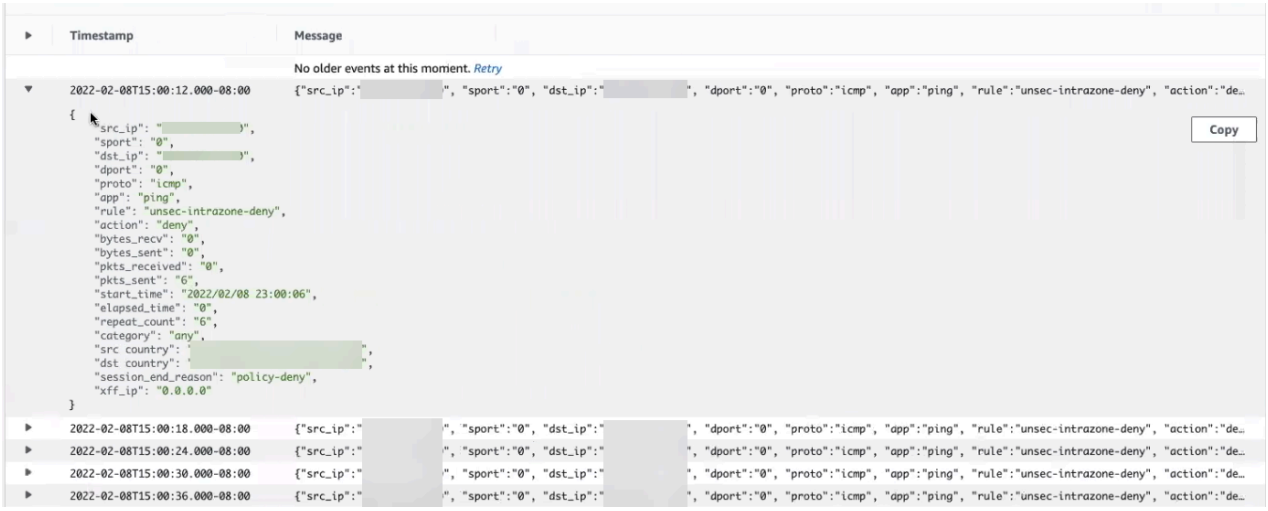
```
/<aws-account-id>/<region>/<NGFW-name>/<random-string>/<log-type>.<year>.<month>.<day>.<hour>
```

Beispielsweise /account123/us-west-1/firewall-1/qadd232312345dea/TRAFFIC.2022.02.10.Twenty-three

*Dabei bezieht sich <random string> auf die jeweilige NGFW-Ressource, die das Protokoll generiert hat.*

Sie können auf den Namen des Streams klicken, um die Protokolleinträge anzuzeigen, die wie im folgenden Beispiel dargestellt angezeigt werden.




Wenn Sie die Protokolle an einen S3-Bucket senden, werden die Protokolldateien als JSON-Datei gespeichert. Die NGFW sendet eine neue Protokolldatei, wenn eines der folgenden Kriterien erfüllt ist: Die Firewall hat 256 MB an Protokollen generiert oder es sind 10 Minuten vergangen, seit die letzte Protokolldatei generiert wurde. Um die Dateien in dem von Ihnen angegebenen S3-Bucket zu finden, greifen Sie auf die S3-Konsole in AWS zu und suchen Sie den angegebenen Bucket. Wählen Sie dann ***AWS-account-id (AWS-Konto-ID)*** > ***region (Region)*** > ***NGFW-name (NGFW-Name)*** > ***log-type (Protokolltyp)*** > ***year (Jahr)*** > ***month (Monat)*** > ***day (Tag)*** > ***hour (Stunde)*** aus. Die Namen der S3-Bucket-Protokolldateien haben das folgende Format:

```
<aws-account-id>-<region>-<NGFW-name>-<log-type>-<year>-<month>-<day>-<hour>-<random-string>
```

*Dabei bezieht sich <random string> auf die jeweilige NGFW-Ressource, die das Protokoll generiert hat.*

Anschließend können Sie die Datei herunterladen und einen JSON-Reader verwenden, um die Protokolle in einem besser lesbaren Format anzuzeigen. Zusätzlich zu den Protokollinformationen enthält jeder Protokolleintrag auch einen Header, der Datum, Priorität, Uhrzeit, Firewall-Hostname, Protokolltyp, Jahr, Monat, Tag, Stunde, Minute und Sekunde aufzeichnet.


Wenn Sie Protokolldateien an Kinesis Firehose senden, werden Protokolle an den von Ihnen angegebenen Streamnamen und dann an das endgültige Ziel gesendet, z. B. einen S3-Bucket, Datadog oder Splunk. Die Quelle für Kinesis Firehose muss **Direct PUT oder eine andere Quelle** sein. Zusätzlich zu den Protokollinformationen enthält jeder Protokolleintrag auch einen Header, der Datum, Priorität, Uhrzeit, Firewall-Hostname, Protokolltyp, Jahr, Monat, Tag, Stunde, Minute, Sekunde, Region, Firewall-Name und AWS-Konto-ID aufzeichnet. Die NGFW fügt den Protokollen die Region, den Firewall-Namen und die AWS-Konto-ID hinzu, um zu kennzeichnen, wo das Protokoll generiert wurde, da diese Informationen nicht im Namen der Protokolldatei enthalten sind. Anschließend können Sie die JSON-Datei herunterladen, um sie anzuzeigen.

*Die in Protokolleinträgen und Protokolldateinamen aufgezeichneten Zeiten und Daten werden in UTC-Zeit angezeigt. Die Protokolldaten in der AWS-Konsole werden jedoch mit Ihrer Ortszeit und Ihrem Ortsdatum angezeigt.*

**STEP 1 |** Wählen Sie in der Cloud NGFW-Konsole **NGFWs** und die Firewall aus, für die die Protokollierung konfiguriert werden soll.

**STEP 2 |** Wählen Sie **Log Settings (Protokolleinstellungen)** aus.

**STEP 3 |** Wählen Sie unter **Log Type (Protokolltyp)** einen oder mehrere zu erfassende Protokolltypen aus.

*Sie haben die Option, alle Protokolle an dasselbe Ziel zu senden oder für jeden Protokolltyp ein anderes Ziel auszuwählen.*

**STEP 4 |** Wählen Sie **Log Destination (Protokollziel)** aus. Wenn Sie mehr als einen Protokolltyp auswählen, müssen Sie das Ziel für jeden Protokolltyp einzeln auswählen.

**STEP 5 |** Geben Sie den Namen von **Log Destination (Protokollziel)** ein. Der Name des Protokollziels muss

**STEP 6 |** Klicken Sie auf **Save (Speichern)**.

# Datenverkehrsprotokollfelder in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

In der folgenden Tabelle werden die Datenverkehrsprotokollfelder in Cloud NGFW für AWS beschrieben:

| Feldname | Beschreibung |
|---|---|
| Generierte Zeit (time_generated oder cef-formatted-time_generated) | Uhrzeit, zu der das Protokoll auf der Datenebene generiert wurde. |
| Quelladresse (src_ip) | Ursprüngliche IP-Adresse der Sitzungsquelle. |
| Quellport (sport) | Quellport, der von der Sitzung verwendet wird. |
| Sitzungs-ID (sessionid) | Eine interne numerische Kennung, die auf jede Sitzung angewendet wird. |
| Zieladresse (dst_ip) | Ursprüngliche IP-Adresse des Sitzungsziels. |
| Zielport (dport) | Zielport, der von der Sitzung verwendet wird. |
| IP-Protokoll (proto) | IP-Protokoll, das der Sitzung zugeordnet ist. |
| Anwendung (app) | Anwendung, die der Sitzung zugeordnet ist. |
| Regelname (rule) | Name der Regel, die der Sitzung entspricht. |
| Aktion (action) | Für die Sitzung ergriffene Aktion; mögliche Werte sind:<br>• allow: Sitzung wurde von der Richtlinie zugelassen<br>• deny: Sitzung wurde von der Richtlinie abgelehnt<br>• reset both: Sitzung wurde beendet und ein TCP-Reset wird an beide Seiten der Verbindung gesendet<br>• reset client: Sitzung wurde beendet und ein TCP-Reset wird an den Client gesendet<br>• reset server: Sitzung wurde beendet und ein TCP-Reset wird an den Server gesendet |

| Feldname | Beschreibung |
|---|---|
| Empfangene Bytes (bytes_recv) | Anzahl der Bytes in Server-zu-Client-Richtung der Sitzung. |
| Gesendete Bytes (bytes_sent) | Anzahl der Bytes in Client-zu-Server-Richtung der Sitzung. |
| Empfangene Pakete (pkts_received) | Anzahl der Server-zu-Client-Pakete für die Sitzung. |
| Gesendete Pakete (pkts_sent) | Anzahl der Client-zu-Server-Pakete für die Sitzung. |
| Startzeit (start_time) | Zeitpunkt des Sitzungsstarts und der Datenträgernutzung. |
| Verstrichene Zeit (elapsed_time) | Verstrichene Zeit der Sitzung. |
| Anzahl der Wiederholungen (repeat_count) | Anzahl der Sitzungen mit derselben Quell-IP, Ziel-IP, Anwendung und demselben Untertyp innerhalb von 5 Sekunden. |
| Kategorie (category) | Mit der Sitzung verknüpfte URL-Kategorie (falls zutreffend). |
| Quellland (src country) | Quellland oder interne Region für private Adressen. Die maximale Länge beträgt 32 Byte. |
| Zielland (dst country) | Zielland oder interne Region für private Adressen. Die maximale Länge beträgt 32 Byte. |
| Grund für Sitzungsende (session_end_reason) | Der Grund, warum eine Sitzung beendet wurde. Wenn der Abbruch mehrere Gründe hatte, zeigt dieses Feld nur den Grund mit der höchsten Priorität an. Die möglichen Gründe für ein Sitzungsende lauten wie folgt in der Reihenfolge der Priorität (wobei der erste am höchsten ist):<br>• threat: Die Firewall hat eine Bedrohung erkannt, die mit einer Aktion zum Zurücksetzen, Löschen oder Blockieren (einer IP-Adresse) verbunden ist.<br>• policy-deny: Die Sitzung stimmte mit einer Sicherheitsregel mit einer deny- oder drop-Aktion überein.<br>• decrypt-cert-validation: Die Sitzung wurde beendet, weil Sie die Firewall so konfiguriert haben, dass sie blockiert, wenn die Sitzung Client-Authentifizierung verwendet oder wenn die Sitzung ein Serverzertifikat mit einer der folgenden Bedingungen verwendet: „abgelaufen“, „nicht vertrauenswürdiger Aussteller“, „unbekannter Status“ oder „Timeout der Statusüberprüfung“. Dieser Grund für das Sitzungsende wird auch angezeigt, wenn das Serverzertifikat eine schwerwiegende Fehlerwarnung des Typs „bad_certificate“, „unsupported_certificate“, „certificate_revoked“, „access_denied“ oder „no_certificate_RESERVED“ (nur SSLv3) erzeugt. |

| Feldname | Beschreibung |
| --- | --- |
| | • decrypt-unsupport-param: Die Sitzung wurde beendet, weil Sie die Firewall so konfiguriert haben, dass sie die SSL-Forward-Proxy-Entschlüsselung oder die eingehende SSL-Inspektion blockiert, wenn die Sitzung eine nicht unterstützte Protokollversion, Verschlüsselung oder einen SSH-Algorithmus verwendet. Dieser Grund für das Sitzungsende wird angezeigt, wenn die Sitzung eine schwerwiegende Fehlerwarnung des Typs „unsupported_extension“, „unexpected_message“ oder „handshake_failure“ erzeugt.<br>• decrypt-error: Die Sitzung wurde beendet, weil Sie die Firewall so konfiguriert haben, dass sie die SSL-Forward-Proxy-Entschlüsselung oder die eingehende SSL-Inspektion blockiert, wenn Firewall-Ressourcen nicht verfügbar waren. Dieser Grund für das Sitzungsende wird auch angezeigt, wenn Sie die Firewall so konfiguriert haben, dass SSL-Datenverkehr blockiert wird, der SSL-Fehler aufweist oder der eine andere schwerwiegende Fehlerwarnung als die für die Beendigungsgründe „decrypt-cert-validation“ und „decrypt-unsupport-param“ aufgeführten Warnungen ausgegeben hat.<br>• tcp-rst-from-client: Der Client hat ein TCP-Reset an den Server gesendet.<br>• tcp-rst-from-server: Der Server hat ein TCP-Reset an den Client gesendet.<br>• resources-unavailable: Die Sitzung wurde aufgrund einer Beschränkung der Systemressourcen abgebrochen. Beispielsweise könnte die Sitzung die Anzahl der pro Ablauf zulässigen Pakete außerhalb der Reihenfolge oder die globale Warteschlange für Pakete außerhalb der Reihenfolge überschritten haben.<br>• tcp-fin: Beide Hosts in der Verbindung haben eine TCP-FIN-Nachricht gesendet, um die Sitzung zu schließen.<br>• tcp-reuse: Eine Sitzung wird wiederverwendet und die Firewall schließt die vorherige Sitzung.<br>• decoder: Der Decoder erkennt eine neue Verbindung innerhalb des Protokolls (z. B. HTTP-Proxy) und beendet die vorherige Verbindung.<br>• aged-out: Die Sitzung ist abgelaufen.<br>• n/a: Dieser Wert gilt, wenn der Datenverkehrsprotokolltyp nicht **end** ist. |
| XFF-Adresse (xff_ip) | Die IP-Adresse des Benutzers, der die Webseite angefordert hat, oder die IP-Adresse des vorletzten Geräts, über das die Anforderung geleitet wurde. Wenn die Anforderung durch einen |

| Feldname | Beschreibung |
| --- | --- |
| | oder mehrere Proxys, Load Balancer oder andere Upstream-Geräte geleitet wird, zeigt die Firewall die IP-Adresse des neuesten Geräts an. |

## Bedrohungsprotokollfelder in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

| Feldname | Beschreibung |
| --- | --- |
| Generierte Zeit (time_generated oder cef-formatted-time_generated) | Uhrzeit, zu der das Protokoll auf der Datenebene generiert wurde. |
| Quelladresse (src_ip) | Ursprüngliche IP-Adresse der Sitzungsquelle. |
| Quellport (sport) | Quellport, der von der Sitzung verwendet wird. |
| Sitzungs-ID (sessionid) | Eine interne numerische Kennung, die auf jede Sitzung angewendet wird. |
| Zieladresse (dst_ip) | Ursprüngliche IP-Adresse des Sitzungsziels. |
| Zielport (dport) | Zielport, der von der Sitzung verwendet wird. |
| IP-Protokoll (proto) | IP-Protokoll, das der Sitzung zugeordnet ist. |
| Anwendung (app) | Anwendung, die der Sitzung zugeordnet ist. |
| Regelname (rule) | Name der Regel, die der Sitzung entspricht. |
| Aktion (action) | Für die Sitzung ergriffene Aktionen; Werte sind alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url.<br>• alert: Bedrohung oder URL erkannt, aber nicht blockiert<br>• allow: Flood-Erkennungswarnung |

| Feldname | Beschreibung |
|---|---|
| | • deny: Mechanismus zur Flood-Erkennung aktiviert und Datenverkehr basierend auf der Konfiguration ablehnen<br>• drop: Bedrohung erkannt und die zugehörige Sitzung wurde gelöscht<br>• reset-client: Bedrohung erkannt und ein TCP-RST wird an den Client gesendet<br>• reset-server: Bedrohung erkannt und ein TCP-RST wird an den Server gesendet<br>• reset-both: Bedrohung erkannt und ein TCP-RST wird sowohl an den Client als auch an den Server gesendet<br>• block-url: URL-Anforderung wurde blockiert, da sie mit einer URL-Kategorie übereinstimmte, die als blockiert festgelegt war<br>• block-ip: Bedrohung erkannt und Client-IP wird blockiert<br>• random-drop: Flood erkannt und das Paket wurde nach dem Zufallsprinzip verworfen<br>• sinkhole: DNS-Sinkhole aktiviert<br>• syncookie-sent: syncookie-Warnung<br>• block-continue (nur URL-Untertyp): eine HTTP-Anforderung wird blockiert und auf eine Continue-Seite mit einer Schaltfläche zur Bestätigung zum Fortfahren umgeleitet<br>• continue (nur URL-Untertyp): Antwort auf eine continue-Seite der block-continue-URL, die angibt, dass eine block-continue-Anforderung fortgesetzt werden durfte<br>• block-override (nur URL-Untertyp): eine HTTP-Anforderung wird blockiert und an eine Admin-Überschreibungsseite umgeleitet, für die ein Passcode vom Firewall-Administrator erforderlich ist, um fortzufahren<br>• override-lockout (nur URL-Untertyp): zu viele fehlgeschlagene Admin-Überschreibungs-Passcodeversuche von der Quell-IP. IP ist jetzt von der block-override-Weiterleitungsseite blockiert<br>• override (nur URL-Untertyp): Antwort auf eine block-override-Seite, auf der ein korrekter Passcode angegeben wird und die Anforderung zulässig ist<br>• block (nur WildFire®): Datei wurde von der Firewall blockiert und in WildFire® hochgeladen |
| Bedrohungskategorie (threat_category) | Beschreibt Bedrohungskategorien, mit denen verschiedene Arten von Bedrohungssignaturen eingestuft werden. |
| Bedrohungs-/Inhaltstyp (threat_content_type) | Untertyp des Bedrohungsprotokolls. Folgende Werte sind möglich:<br>• data: Datenmuster, das einem Datenfilterungsprofil entspricht.<br>• file: Dateityp, der einem Dateiblockadeprofil entspricht. |

| Feldname | Beschreibung |
|---|---|
| | • flood: Flood, die über ein Zonen-Sicherheitsprofil erkannt wird.<br>• packet: Paketbasierter Angriffsschutz, der durch ein Zonen-Sicherheitsprofil ausgelöst wird.<br>• scan: Scan, der über ein Zonen-Sicherheitsprofil erkannt wird.<br>• spyware: Spyware, die über ein Anti-Spyware-Profil erkannt wird.<br>• url: URL-Filterungs-Protokoll.<br>• ml-malware: Malware, die von WildFire Inline ML über ein Antivirenprofil erkannt wird.<br>• Malware: Malware, die über ein Antivirenprofil erkannt wird.<br>• vulnerability: Sicherheitslücken-Exploit, der über ein Sicherheitslücken-Sicherheitsprofil erkannt wird.<br>• wildfire: WildFire-Urteil, das generiert wird, wenn die Firewall eine Datei per WildFire-Analyseprofil an WildFire sendet und ein Urteil (Malware, Phishing, Grayware oder gutartig, je nachdem, was Sie protokollieren) im WildFire-Übermittlungsprotokoll protokolliert wird.<br>• wildFire®malware: Malware, die über ein Antivirenprofil erkannt wird. |
| Bedrohungs-/Inhaltsname (threat_content_name) | Palo Alto Networks Kennung für bekannte und benutzerdefinierte Bedrohungen. Es handelt sich um eine Beschreibungszeichenfolge, gefolgt von einer numerischen 64-Bit-Kennung in Klammern für einige Untertypen:<br>• 8000-8099: Scan-Erkennung<br>• 8500-8599: Flood-Erkennung<br>• 9999: URL-Filterungs-Protokoll<br>• 10000-19999: Erkennung von Spyware-Telefonen<br>• 20000-29999: Erkennung von Spyware-Downloads<br>• 30000-44999: Erkennung von Sicherheitslücken-Exploits<br>• 52000-52999: Erkennung von Dateitypen<br>• 60000-69999: Erkennung von Datenfilterung<br><br>*Bedrohungs-ID-Bereiche für Malware-Erkennung, WildFire-Signaturfeed und DNS-C2-Signaturen, die in früheren Versionen verwendet wurden, wurden durch permanente, global eindeutige IDs ersetzt. Über die Feldnamen „Bedrohungs-/Inhaltstyp (subtype)“ und „Bedrohungskategorie (thr_category)“ können Sie aktualisierte Berichte erstellen sowie Bedrohungsprotokolle und ACC-Aktivitäten filtern.* |

| Feldname | Beschreibung |
|---|---|
| Schweregrad (severity) | Schweregrad der Bedrohung; Werte sind „informational“, „low“, „medium“, „high“, „critical“. |
| Richtung (direction) | Gibt die Richtung des Angriffs an, Client-zu-Server oder Server-zu-Client:<br>• 0: Richtung der Bedrohung ist Client-zu-Server<br>• 1: Richtung der Bedrohung ist Server-zu-Client |
| Wiederholungsanzahl (repeatcnt) | Anzahl der Sitzungen mit derselben Quell-IP, Ziel-IP, Anwendung und demselben Inhalts- und Bedrohungstyp innerhalb von 5 Sekunden. |
| Grund (data_filter_reason) | Grund für die Datenfilterungsaktion. |
| XFF-Adresse (xff_ip) | Die IP-Adresse des Benutzers, der die Webseite angefordert hat, oder die IP-Adresse des vorletzten Geräts, über das die Anforderung geleitet wurde. Wenn die Anforderung durch einen oder mehrere Proxys, Load Balancer oder andere Upstream-Geräte geleitet wird, zeigt die Firewall die IP-Adresse des neuesten Geräts an. |
| Inhaltsversion (contentver) | Anwendungs- und Bedrohungsversion auf Ihrer Firewall, als das Protokoll generiert wurde. |

## Entschlüsselungsprotokollfelder in Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Die folgende Tabelle enthält Informationen zu den Entschlüsselungsprotokollfeldern:

| Feldname | Beschreibung |
|---|---|
| Generierte Zeit (time_generated oder cef-formatted-time_generated) | Uhrzeit, zu der das Protokoll auf der Datenebene generiert wurde. |

| Feldname | Beschreibung |
|---|---|
| Quell-IP-Adresse (src_ip) | Ursprüngliche IP-Adresse der Sitzungsquelle. |
| Quellport (sport) | Quellport, der von der Sitzung verwendet wird. |
| Sitzungs-ID (sessionid) | Eine interne numerische Kennung, die auf jede Sitzung angewendet wird. |
| Zieladresse (dst_ip) | Ursprüngliche IP-Adresse des Sitzungsziels. |
| Zielport (dport) | Zielport, der von der Sitzung verwendet wird. |
| IP-Protokoll (proto) | IP-Protokoll, das der Sitzung zugeordnet ist. |
| Anwendung (app) | Anwendung, die der Sitzung zugeordnet ist. |
| Regel (rule) | Sicherheitsrichtlinienregel, die den Sitzungsdatenverkehr steuert. |
| Aktion (action) | Für die Sitzung ergriffene Aktion; mögliche Werte sind:<br>• allow: Sitzung wurde von der Richtlinie zugelassen<br>• deny: Sitzung wurde von der Richtlinie abgelehnt<br>• reset both: Sitzung wurde beendet und ein TCP-Reset wird an beide Seiten der Verbindung gesendet<br>• reset client: Sitzung wurde beendet und ein TCP-Reset wird an den Client gesendet<br>• reset server: Sitzung wurde beendet und ein TCP-Reset wird an den Server gesendet |
| TLS-Version (tls_version) | Die Version des TLS-Protokolls, die für die Sitzung verwendet wird. |
| Schlüsselaustauschalgorithmus (key_exchange_algorithm) | Schlüsselaustauschalgorithmus, der für die Sitzung verwendet wird. |
| Verschlüsselungsalgorithmus (tls_enc) | Der Algorithmus, der zum Verschlüsseln der Sitzungsdaten verwendet wird, z. B. AES-128-CBC, AES-256-GCM. |
| Hash-Algorithmus (hash_algorithm) | Authentifizierungsalgorithmus, der für die Sitzung verwendet wird, z. B. SHA, SHA256, SHA384. |
| Elliptische Kurve (elliptic_curve) | Die elliptische Kryptografiekurve, die Client und Server aushandeln und für Verbindungen verwenden, die ECDHE-Verschlüsselungssammlungen nutzen. |

| Feldname | Beschreibung |
|---|---|
| Angabe des Servernamens (server_name_indication) | Die Angabe des Servernamens. |
| Länge von der Angabe des Servernamens (server_name_indication_length) | Die Länge von der Angabe des Servernamens (hostname). |
| Proxytyp (proxy_type) | Der Entschlüsselungsproxytyp, z. B. **„Forward“ für Forward-Proxy**, **„Inbound“ für eingehende Prüfung**, **„No Decrypt“** für unverschlüsselten Datenverkehr, „GlobalProtect“.<br><br>*Wenn Sie **Keine Entschlüsselung** statt **Keine** auswählen, wird der Datenverkehr verringert.* |
| Kettenstatus (chain_status) | Legt fest, ob der Kette vertraut wird. Werte sind:<br>• Nicht geprüft<br>• Nicht vertrauenswürdig<br>• Vertrauenswürdig<br>• Unvollständig |

# Protokolle und Aktivitäten zu Datenverkehr und Bedrohungen in Panorama anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

## Cloud NGFW-Protokolle in Panorama anzeigen

Wenn Ihre Cloud NGFW-Ressourcen in Panorama und im Strata-Protokollierungsdienst integriert sind, werden Protokolle und Aktivitäten erfasst und in Panorama auf den Registerkarten „Monitor“ (Überwachung) und „ACC“ (Application Command Center) angezeigt. Panorama sammelt Protokolle, die von der Cloud NGFW generiert wurden, und zeigt sie auf der Registerkarte **Monitor (Überwachen)** an. Sie können aus den Datenverkehrs-, Bedrohungs-, URL-Filter- und Entschlüsselungsprotokollen auswählen und diese nach ID oder Name filtern. Beschreibungen der Protokollfelder finden Sie unter Dokumentation zur Cloud NGFW-Protokollierung.

**STEP 1 |** Melden Sie sich bei Panorama an.

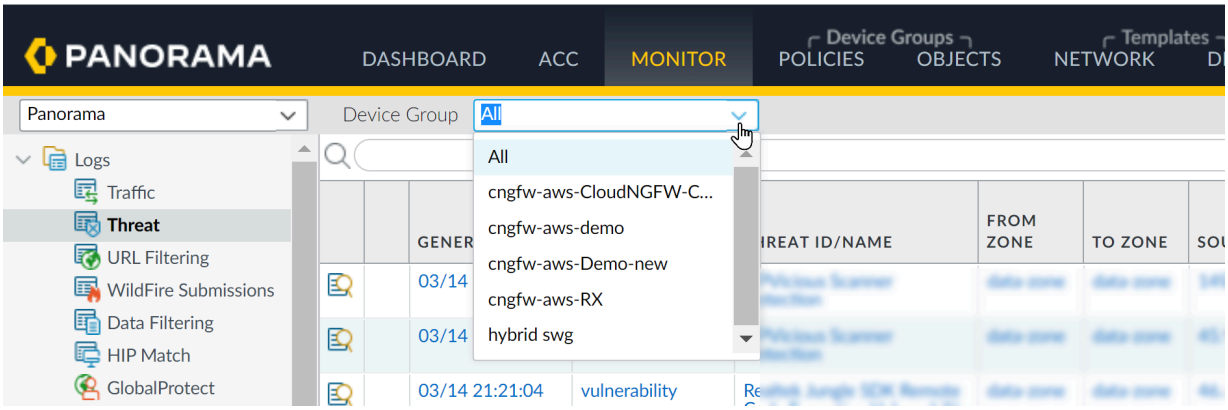
**STEP 2 |** Wählen Sie **Monitor** aus.

**STEP 3 |** Wählen Sie aus der Drop-down-Liste **Device Group** die **Cloud Device Group** aus, um die Aktivität anzuzeigen.

**STEP 4 |** Sie können einen Panorama-Filter verwenden, um das Protokoll einer einzelnen Cloud-Gerätegruppe anzuzeigen. Suchen Sie die Schaltfläche **Device Name**. Klicken Sie im oberen rechten Bereich der Panorama-Benutzeroberfläche auf das Symbol **+**, um einen neuen Filter hinzuzufügen. Geben Sie den Namen für den Filter ein und klicken Sie dann auf **Save**. Klicken Sie auf das Symbol **Load Filter**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

**STEP 5 |** Im Menü **Logs** auf der linken Seite der Panorama-Konsole können Sie einen bestimmten Protokolltyp auswählen, der angezeigt werden soll.




# Cloud NGFW-Aktivität im ACC anzeigen

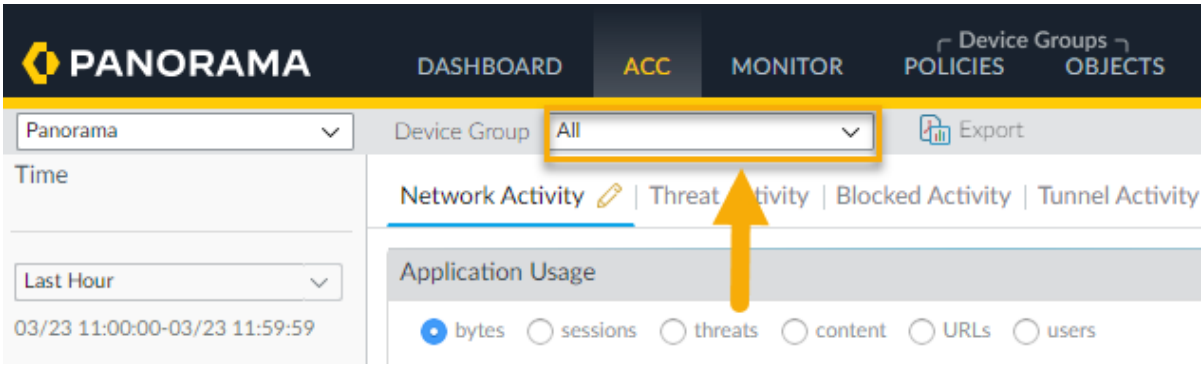
Das ACC ist ein Analysetool, das verwertbare Informationen über die Aktivitäten in Ihrem Netzwerk liefert. Das ACC verwendet die Cloud NGFW-Protokolle, um die Datenverkehrstrends in Ihrem Netzwerk grafisch darzustellen. Die grafische Darstellung ermöglicht es Ihnen, mit den Daten zu interagieren und die Beziehungen zwischen Ereignissen im Netzwerk zu visualisieren, einschließlich Netzwerknutzungsmustern, Datenverkehrsmustern sowie verdächtigen Aktivitäten und Anomalien.

In Panorama können Sie ACC-Inhalte basierend auf der Cloud-Gerätegruppe filtern. Weitere Informationen zum Filtern und Anzeigen bestimmter Informationen zu Aktivitäten in Ihren Cloud NGFW-Ressourcen finden Sie in der ACC-Dokumentation für PAN-OS.

**STEP 1 |** Melden Sie sich bei Panorama an.

**STEP 2 |** Wählen Sie **ACC** aus.

**STEP 3 |** Wählen Sie aus der Drop-down-Liste **Device Group** die **Cloud Device Group** aus, um die Aktivität anzuzeigen.




**STEP 4 |** Sie können einen Panorama-Filter verwenden, um das Protokoll einer einzelnen Cloud-Gerätegruppe anzuzeigen. Suchen Sie die Schaltfläche **Device Name**. Klicken Sie im oberen rechten Bereich der Panorama-Benutzeroberfläche auf das Symbol +, um einen neuen Filter hinzuzufügen. Geben Sie den

Namen für den Filter ein und klicken Sie dann auf **Save**. Klicken Sie auf das Symbol **Load Filter**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

# Datenverkehrs- und Bedrohungsprotokolle im Strata-Protokollierungsdienst anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Wenn Sie Cloud NGFW in Panorama und im Strata-Protokollierungsdienst integrieren, können Sie Protokolle weiterleiten, die von Ihren Cloud NGFW-Ressourcen erstellt wurden, und sie im Strata-Protokollierungsdienst anzeigen. In der Weboberfläche des Strata-Protokollierungsdienstes können Sie die Datenverkehrs-, Bedrohungs- und Entschlüsselungsprotokolle anzeigen, die von Ihren Cloud NGFW-Ressourcen generiert wurden.

*Wenn Sie Panorama verwenden und den Strata-Protokollierungsdienst nicht für die Protokollerfassung verwenden, können Sie Protokolle an eine andere Entität weiterleiten, müssen jedoch den Strata-Protokollierungsdienst in Ihrem Protokollierungsprofil aktivieren.*

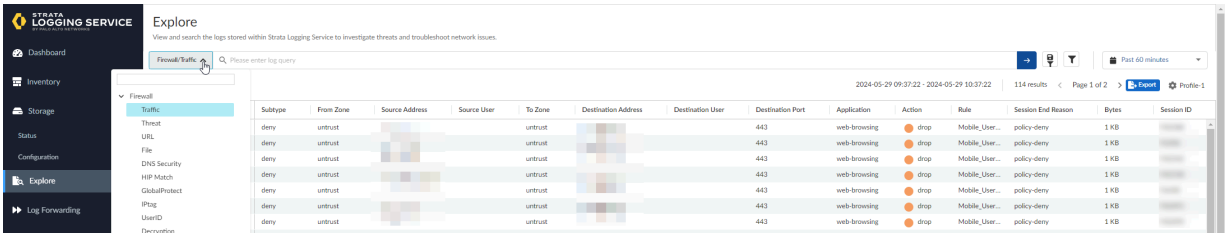
Weitere Informationen zu den Protokollfeldern finden Sie in der Schema-Referenz für den Strata-Protokollierungsdienst: Datenverkehr, Bedrohung und Entschlüsselung.

**STEP 1 |** Melden Sie sich bei Ihrer Instanz des Strata-Protokollierungsdienstes an.

**STEP 2 |** Wählen Sie **Explore (Erkunden)** aus.

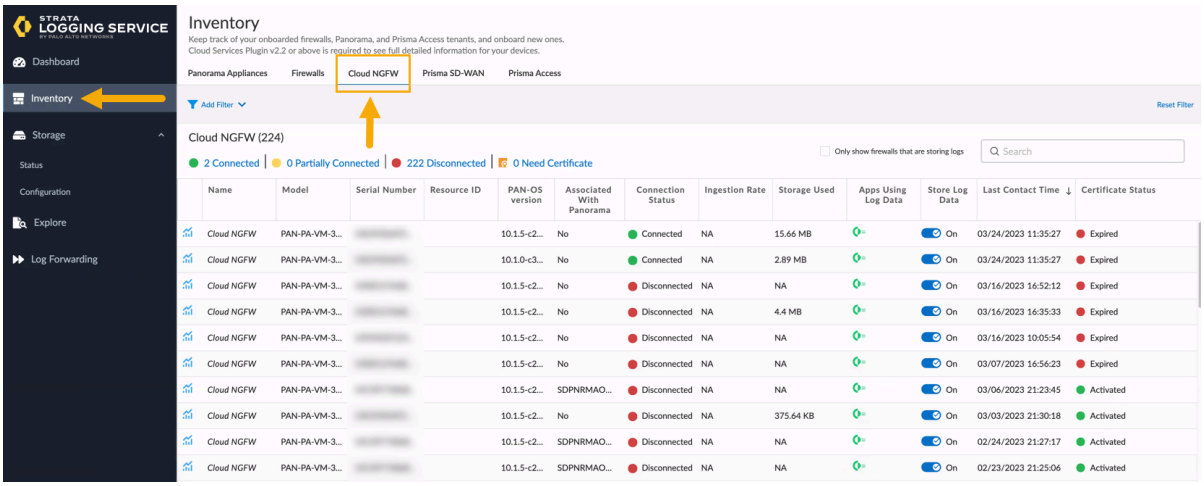
**STEP 3 |** In der Dropdown-Liste der Abfrage können Sie den Protokolltyp auswählen. Auf jeder Seite werden 100 Protokolle angezeigt. Sie können jedoch die Abfragen des Strata-Protokollierungsdienstes verwenden, um die angezeigten Informationen zu präzisieren.




**STEP 4 |** Wählen Sie **Inventory (Inventar)** aus, um Informationen zu eingebundenen Firewalls anzuzeigen.

**STEP 5 |** Wählen Sie auf der Seite **Inventory (Inventar)** die Option **Cloud NGFW** aus.




# Protokolle an den Strata-Protokollierungsdienst weiterleiten

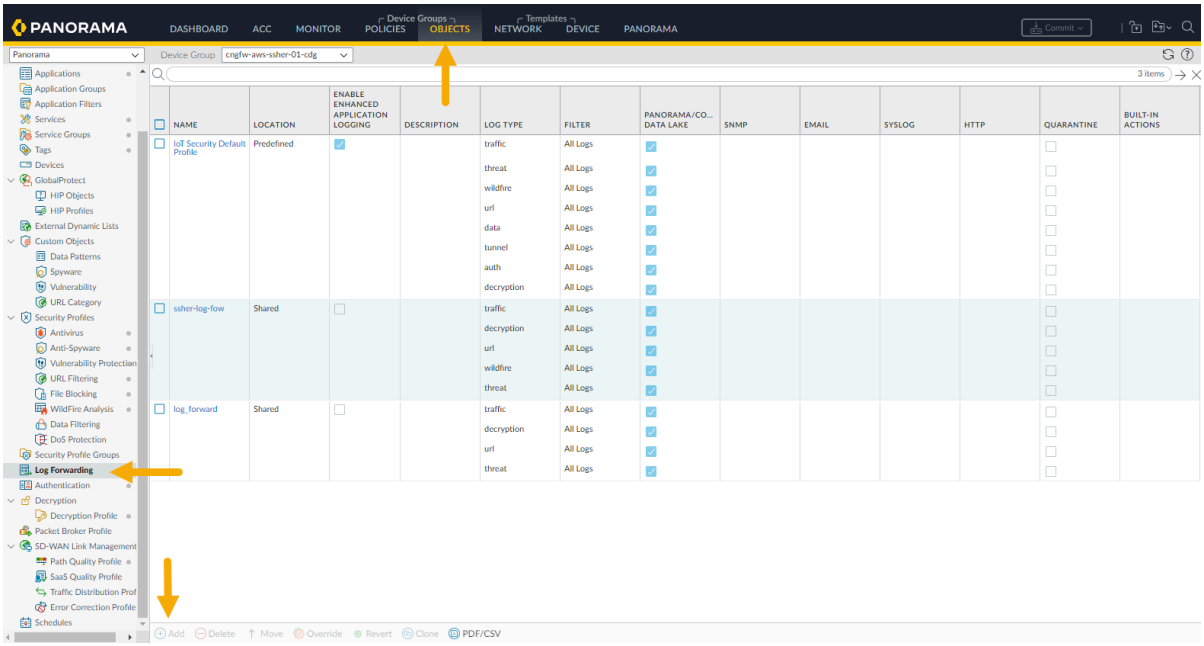
So leiten Sie Protokolle an den Strata-Protokollierungsdienst weiter:

**STEP 1 |** Wählen Sie in der Panorama-Konsole die Option **Objects (Objekte)** unter **Device Groups (Gerätegruppen)** aus.

**STEP 2 |** Wählen Sie **Log Forwarding (Protokollweiterleitung)** aus.

**STEP 3 |** Klicken Sie auf **Add (Hinzufügen)**, um ein neues Profil für die Übereinstimmungsliste zur Protokollweiterleitung zu erstellen.

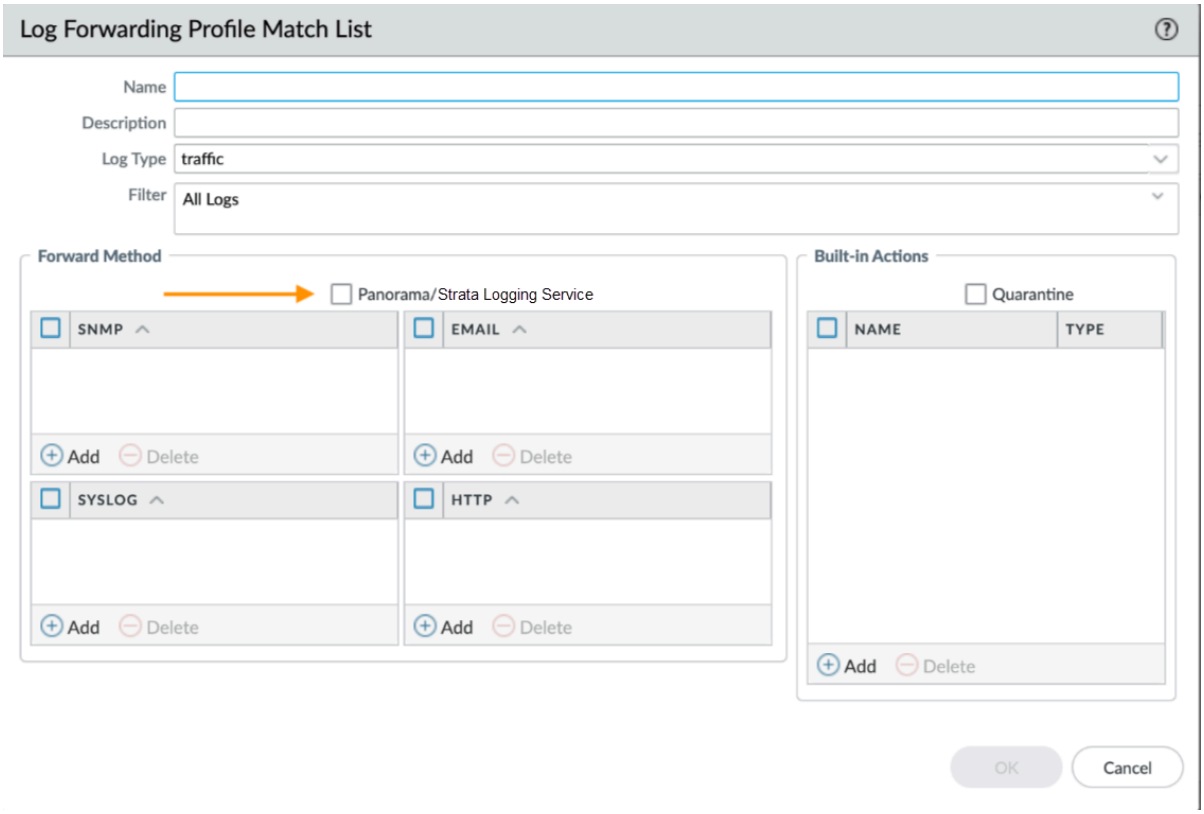


**STEP 4 |** Geben Sie im Bildschirm **Log Forwarding Profile Match List (Übereinstimmungsliste für Protokollweiterleitungsprofil)** einen Namen für das Protokoll an.

**STEP 5 |** Wählen Sie aus der Dropdown-Liste die Option **Log Type (Protokolltyp)** aus.

**STEP 6 |** Wählen Sie **Panorama/Strata Logging Service (Panorama/Strata-Protokollierungsdienst)** als **Weiterleitungsmethode** aus.



**STEP 7 |** Klicken Sie auf **OK**.

**STEP 8 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

## Protokolle ohne den Strata-Protokollierungsdienst weiterleiten

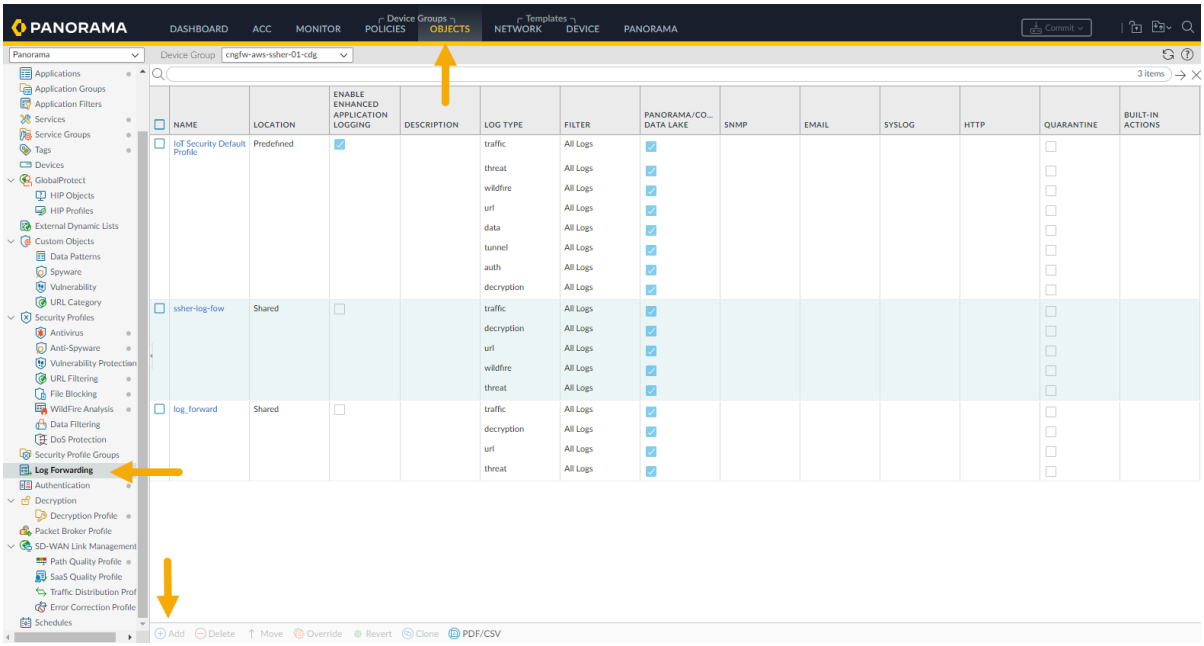
Wenn Sie Panorama verwenden, jedoch nicht den Strata-Protokollierungsdienst für die Protokollerfassung nutzen, können Sie Protokolle an eine andere Entität weiterleiten, z. B. AWS CloudWatch, Amazon S3 oder Amazon Kinesis.

**STEP 1 |** Wählen Sie in der Panorama-Konsole die Option **Objects (Objekte)** unter **Device Groups (Gerätegruppen)** aus.

**STEP 2 |** Wählen Sie **Log Forwarding (Protokollweiterleitung)** aus.

**STEP 3 |** Klicken Sie auf **Add (Hinzufügen)**, um ein neues Profil für die Übereinstimmungsliste zur Protokollweiterleitung zu erstellen.



**STEP 4 |** Geben Sie im Bildschirm **Log Forwarding Profile Match List (Übereinstimmungsliste für Protokollweiterleitungsprofil)** einen Namen für das Protokoll an.

**STEP 5 |** Wählen Sie aus der Dropdown-Liste die Option **Log Type (Protokolltyp)** aus.

Wenn Panorama nicht mit dem Strata-Protokollierungsdienst verknüpft ist, werden die Protokolle nicht an die Panorama-Konsole weitergeleitet, sondern können in einer anderen Anwendung wie CloudWatch, S3 oder Kinesis angezeigt werden. Verwenden Sie die Cloud NGFW-Konsole, um diese anderen Protokollierungsmethoden zu konfigurieren.

*Aktivieren Sie den Strata-Protokollierungsdienst in Ihrem Protokollierungsprofil auch dann, wenn Sie nicht beabsichtigen, Protokolle direkt an den Dienst zu senden.*

**STEP 6 |** Klicken Sie auf **OK**.

**STEP 7 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

# Überwachungsprotokolle in Cloud NGFW für AWS anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Verfolgen Sie Administratoraktivitäten in Cloud NGFW für AWS, um Echtzeitberichte über Aktivitäten in der gesamten Bereitstellung zu erhalten. Wenn Sie Grund zu der Annahme haben, dass ein Administratorkonto kompromittiert wurde, liefert Ihnen das Überwachungsprotokoll den vollständigen Verlauf der Navigation eines Administrators im Cloud NGFW-Mandanten und seiner Konfigurationsänderungen, sodass Sie alle Aktionen des kompromittierten Kontos detailliert analysieren und darauf reagieren können.

Wenn Sie Cloud NGFW für AWS bereits bereitgestellt haben, müssen Sie möglicherweise Ihre CFT aktualisieren, falls die aktuelle CFT nicht das Feld „Audit Log“ (Überwachungsprotokoll) enthält.

*Die Protokollgruppe muss in der AWS-Konsole in derselben Region erstellt werden, in der auch die Cloud NGFW-CFT bereitgestellt wurde.*

Wenn ein Ereignis eintritt, wird ein Überwachungsprotokoll generiert und an die von Ihnen angegebene CloudWatch-Protokollgruppe weitergeleitet.

**STEP 1 |** Aktualisieren Sie bei Bedarf Ihre CFT, um Berechtigungen hinzuzufügen, die zum Schreiben in die CloudWatch-Protokollgruppe des Überwachungsprotokolls erforderlich sind.

1. Melden Sie sich bei der Cloud NGFW-Konsole an.
2. Wählen Sie **AWS Accounts (AWS-Konten)** > **Download CFT (CFT herunterladen)** aus, um die CFT als YAML-Datei herunterzuladen.
3. Laden Sie Ihre CFT hoch, bearbeiten Sie sie und wenden Sie sie auf die AWS-Konsole an.
   1. Melden Sie sich bei der AWS-Konsole an und wählen Sie **CloudFormation** > **Stacks (Stapel)** aus.
   2. Suchen Sie den Cloud NGFW-Stapel **PaloAltoNetworksCrossAccountRoleSetup**.
   3. Wählen Sie **Update (Aktualisieren)** aus.
   4. Wählen Sie die Vorlage **Replace current (Aktuelle ersetzen)** und **Upload a template file (Vorlagendatei hochladen)** aus.
   5. Wählen Sie die YAML-Datei für Ihre CFT aus und klicken Sie auf **Next (Weiter)**.
   6. Überprüfen Sie die Einstellung für den CFT-Stapel und klicken Sie auf **Next (Weiter)**.
   7. Überprüfen Sie die Optionen für den CFT-Stapel und klicken Sie auf **Next (Weiter)**.
   8. Überprüfen Sie den CFT-Stapel und klicken Sie auf **Update (Aktualisieren)**.

**STEP 2 |** Melden Sie sich bei der Cloud NGFW-Mandantenkonsole an.

**STEP 3 |** Wählen Sie **Tenant (Mandant)** aus.

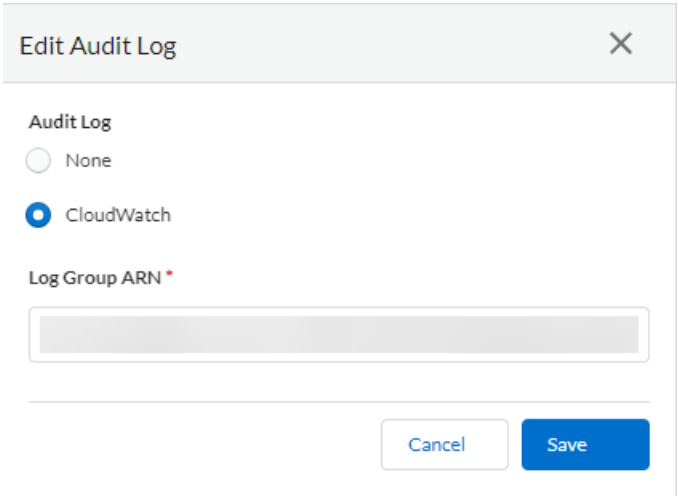
**STEP 4 |** Klicken Sie auf das Bearbeitungssymbol Edit für **Audit Log Settings (Überwachungsprotokolleinstellungen)**.

**STEP 5 |** Wählen Sie das Optionsfeld „CloudWatch“ aus.

**STEP 6 |** Geben Sie den Amazon Resource Name (Amazon-Ressourcennamen, ARN) Ihrer CloudWatch-Zielprotokollgruppe ein.

Stellen Sie sicher, dass der hier eingegebene ARN mit der CloudWatch-Protokollgruppe übereinstimmt, die Sie in Ihrem CFT-Stapel angegeben haben.

**STEP 7 |** Klicken Sie auf **Save (Speichern)**.



# Benutzerdefinierte Metriken in AWS CloudWatch veröffentlichen und anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW für AWS veröffentlicht benutzerdefinierte Metriken in AWS CloudWatch, um Sie bei der Überwachung des Zustands, der Leistung und der Nutzungsmuster Ihrer Cloud NGFW zu unterstützen. Mit diesen zusätzlichen Metriken können Sie den Gesamtzustand Ihrer Cloud NGFW-Ressourcen bewerten, Leistungsengpässe identifizieren und Anomalien erkennen. Bei diesen Metriken handelt es sich um numerische Werte, die Aspekte einer Cloud NGFW zu einem bestimmten Zeitpunkt beschreiben. Metriken, die alle fünf Minuten erfasst werden, sind aufgrund ihrer häufigen Stichprobenerstellung nützlich für Warnungen.

*Die CloudWatch-Protokollgruppe, der S3-Bucket, der CloudWatch-Namespace und der Kinesis-Stream sollten in der CloudFormation-Vorlage (CloudFormation Template, CFT) vorab erstellt werden.*

*Metriken werden alle fünf Minuten erfasst. Alle Metriken werden in einem Namespace veröffentlicht. CloudWatch speichert Ihre Metriken, sodass Sie auf historische Informationen zugreifen können, um die Leistung Ihrer Cloud NGFW-Ressourcen besser zu beurteilen. Sie können auch Alarme festlegen, die bestimmte Schwellenwerte überwachen und Benachrichtigungen senden oder Maßnahmen ergreifen, wenn diese Schwellenwerte erreicht werden. Weitere Informationen finden Sie in der* Amazon CloudWatch-Dokumentation.

Die folgenden CloudWatch-Metriken werden von der Cloud NGFW-Ressource unterstützt:

| Feldname | Beschreibung |
|---|---|
| Dataplane CPU Utilization (%) (CPU-Auslastung auf Datenebene (%)) | Überwacht die CPU-Auslastung auf Datenebene und misst die Datenverkehrsmenge auf der Cloud NGFW-Ressource. |
| Dataplane Packet Buffer Utilization (%) (Auslastung des Paketpuffers auf Datenebene (%)) | Überwacht die Nutzung des Puffers auf Datenebene und misst die Pufferauslastung. Wenn ein plötzlicher Anstieg des Datenverkehrs zu verzeichnen ist, können Sie durch die Überwachung der Pufferauslastung sicherstellen, dass die |

| Feldname | Beschreibung |
|---|---|
| | Firewall den Puffer auf der Datenebene nicht erschöpft, was zu verworfenen Paketen führt. |
| Connection per Second (Verbindung pro Sekunde) | Stellt die Gesamtzahl der gleichzeitigen TCP-Verbindungen dar. |
| Session Throughput Kbps (Sitzungsdurchsatz in kbit/s) | Der Sitzungsdurchsatz, gemessen in kbit/s. |
| Session Throughput Pps (Sitzungsdurchsatz in Paketen/s) | Der Sitzungsdurchsatz, gemessen in Paketen/s. |
| Sessions Active (Aktive Sitzungen) | Überwacht die Gesamtzahl der Sitzungen, die auf der Cloud NGFW-Ressource aktiv sind. Eine aktive Sitzung ist eine Sitzung, die sich in der Flow-Lookup-Tabelle befindet und für die Pakete überprüft und weitergeleitet werden, wie von der Richtlinie gefordert. |
| Session Utilization (%) (Sitzungsauslastung (%)) | Überwacht die derzeit aktiven TCP-, UDP-, ICMP- und SSL-Sitzungen sowie die Paketrate, die Rate des Aufbaus neuer Verbindungen und den Firewalldurchsatz, um die Sitzungsauslastung zu bestimmen. |
| BytesIn (Eingehende Bytes) | Anzahl der Bytes in Server-zu-Client-Richtung der Sitzung. |
| BytesOut (Ausgehende Bytes) | Anzahl der Bytes in Client-zu-Server-Richtung der Sitzung. |
| PktsIn (Eingehende Pakete) | Anzahl der Server-zu-Client-Pakete für die Sitzung. |
| PktsOut (Ausgehende Pakete) | Anzahl der Client-zu-Server-Pakete für die Sitzung. |

So veröffentlichen Sie CloudWatch-Metriken:

**STEP 1 |** Melden Sie sich bei Ihrer Cloud NGFW-Ressource an.

**STEP 2 |** Wählen Sie **NG Firewalls (NG-Firewalls)** aus.

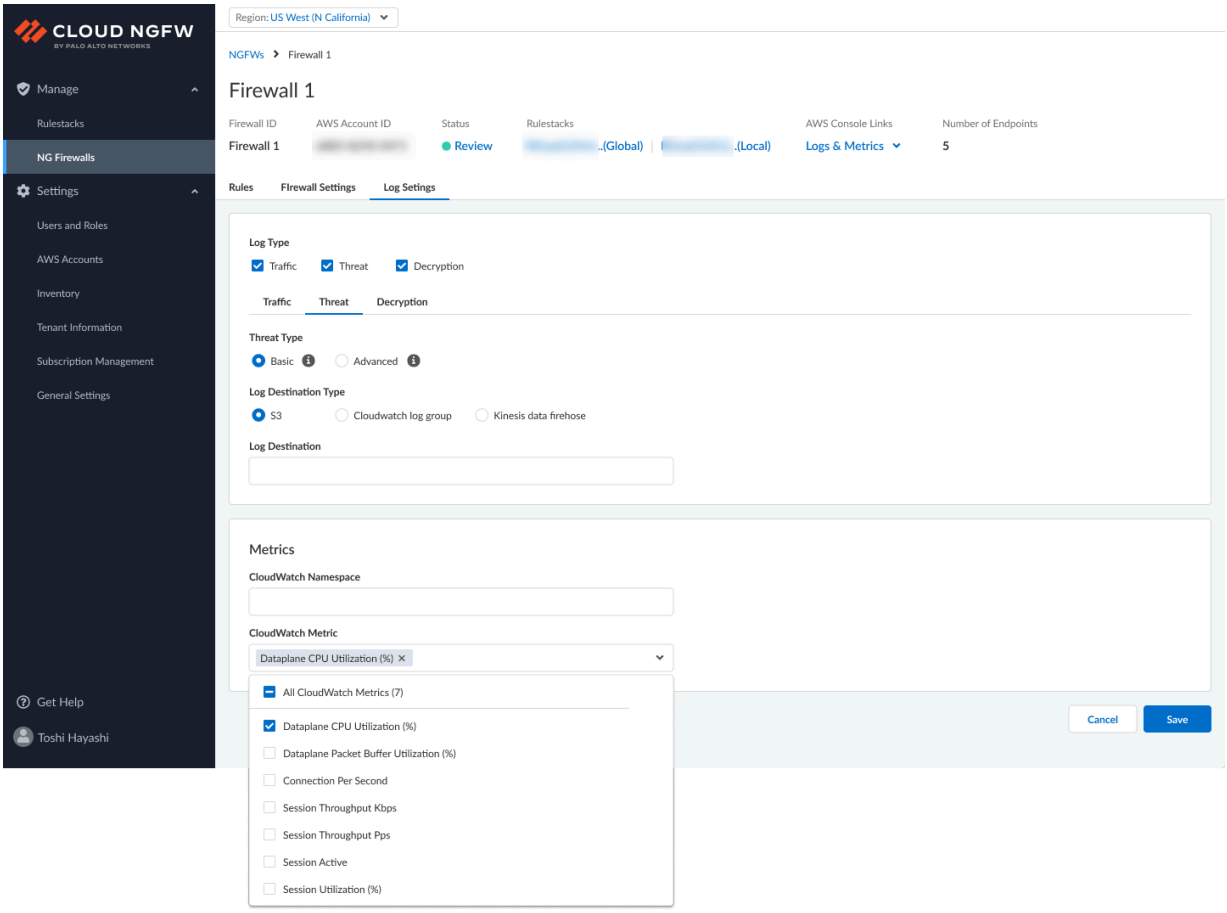
**STEP 3 |** Wählen Sie **Log Settings (Protokolleinstellungen)** aus.

**STEP 4 |** Geben Sie unter **Metrics (Metriken)** Folgendes an:

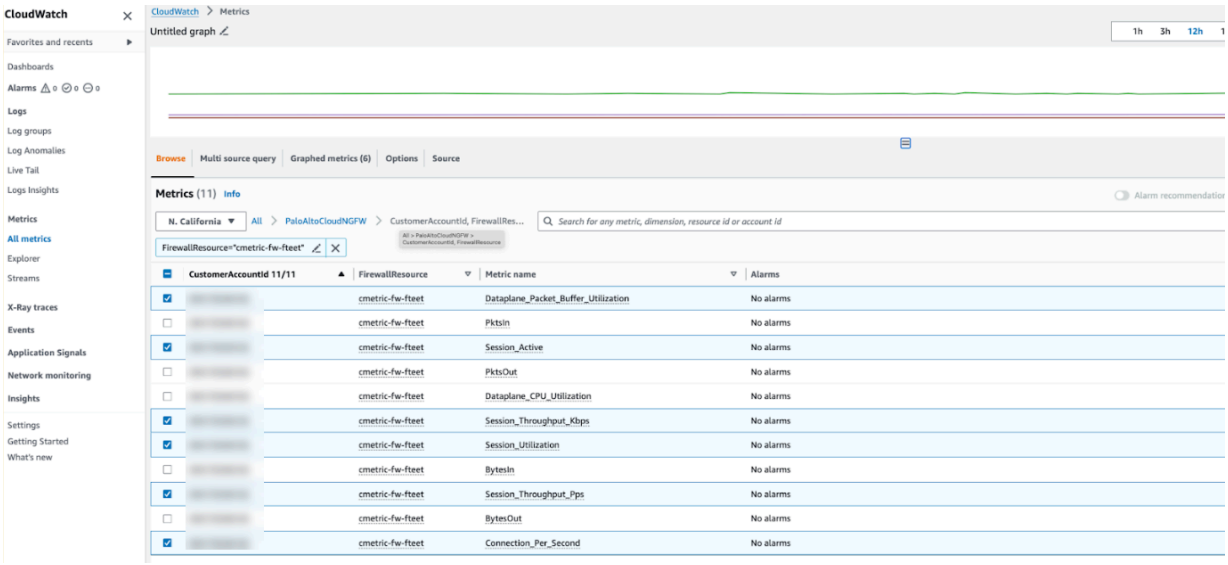
1. **CloudWatch Namespace**. Dieses Feld stellt den Speicherort in AWS dar, an dem die Metriken erfasst werden.
2. **CloudWatch Metric**. Wählen Sie die zu überwachenden Metriken aus. In der obigen Tabelle finden Sie die unterstützten Metriken.

**STEP 5 |** Klicken Sie auf **Save (Speichern)**.




Eine Beispielausgabe von Metriken, die in einem Konto angezeigt werden, sieht wie folgt aus:



# Firewall-as-Code

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Die Cloud NGFW für AWS unterstützt Firewall-as-Code. Dazu gehört die Unterstützung für Terraform, ein Open-Source-Tool, mit dem Sie Infrastrukturressourcen mithilfe von Konfigurationsdateien definieren, verwalten und versionieren können. Als Infrastructure-as-Code-Tool ermöglicht Ihnen Terraform die Automatisierung von Cloud- und lokalen Ressourcen, indem Sie Ressourcen in Konfigurationsdateien definieren, die Sie wiederverwenden, teilen und versionieren können, um Folgendes zu erreichen:

- Senkung der Kosten durch Minimierung redundanter Arbeitsabläufe.
- Verringerung des Risikos durch Standardisierung der Art und Weise, wie Infrastruktur kodifiziert und wiederverwendet wird.
- Verwendung von Automatisierung, um die Zeit zu verkürzen, die für die Bereitstellung Ihrer Cloud NGFW-Ressource benötigt wird.
- Verbesserung der Zuverlässigkeit, indem sichergestellt wird, dass Ihre Cloud NGFW-Ressourcen wie in den Terraform-Konfigurationsdateien deklariert bereitgestellt und konfiguriert werden.

Zusätzlich zur Terraform-Unterstützung unterstützt Ihre Cloud NGFW-Ressource auch AWS CloudFormation. CloudFormation ist ein Service von AWS, der Sie bei der Modellierung und Konfiguration Ihrer AWS-Ressourcen unterstützt, indem eine Vorlage erstellt wird, die alle von Ihnen verwendeten AWS-Ressourcen beschreibt (z. B. eine Amazon EC2-Instanz). Mit der CloudFormation-Vorlage müssen Sie Ihre AWS-Ressourcen nicht einzeln erstellen und konfigurieren. Die Vorlage erleichtert Ihnen die Arbeit. Insbesondere übernimmt sie folgende Aufgaben:

- Vereinfachung der Infrastrukturverwaltung, indem eine Vorlage verwendet wird, um alle Ressourcen (z. B. eine Gruppe für automatische Skalierung oder einen elastischen Load Balancer) und deren Eigenschaften zu beschreiben.
- Replikation Ihrer Infrastruktur, sodass Sie Ihre CloudFormation-Vorlage auf konsistente und wiederholbare Weise wiederverwenden können. Beschreiben Sie Ihre Ressourcen einmal anhand der Vorlage und stellen Sie dann dieselben Ressourcen immer wieder in mehreren Regionen bereit.
- Steuerung und Verfolgung von Änderungen an Ihren Bereitstellungen, indem Situationen wie beispielsweise inkrementelle Upgrades unterstützt werden. So kann möglicherweise ein Upgrade zu unvorhergesehenen Leistungsproblemen geführt haben. Ein manuelles Zurücksetzen Ihrer Infrastruktur auf die ursprünglichen Einstellungen würde voraussetzen, dass Sie mit den geänderten Ressourcen und den ursprünglichen Einstellungen vertraut sind. Die CloudFormation-Vorlage, die als leicht lesbare Textdatei geschrieben ist, hilft Ihnen dabei, Änderungen an Ihrer Infrastruktur zu bestimmen, indem

Revisionen eindeutig gekennzeichnet werden. Und in Verbindung mit einem Versionskontrollsystem wissen Sie genau, wann, wo und von wem Änderungen vorgenommen wurden.

# Programmgesteuerten Zugriff aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Der programmgesteuerte Zugriff in Cloud NGFW ermöglicht Ihnen das Erstellen und Verwalten von NGFWs und Regelstapeln mithilfe von REST-APIs. Mit diesen APIs können Sie Aktionen für Cloud NGFW-Ressourcen (NGFW und Regelstapel) über eine Anwendung oder ein Drittanbieter-Tool aufrufen. Diese APIs ermöglichen Ihnen außerdem die Verwendung von Infrastructure-as-Code(IAC)-Tools wie CloudFormation-Vorlagen (CloudFormation Templates, CFT) und Terraform-Vorlagen. Sie können diese IAC-Tools in Workloads innerhalb oder außerhalb der AWS-Umgebung installieren und ausführen.

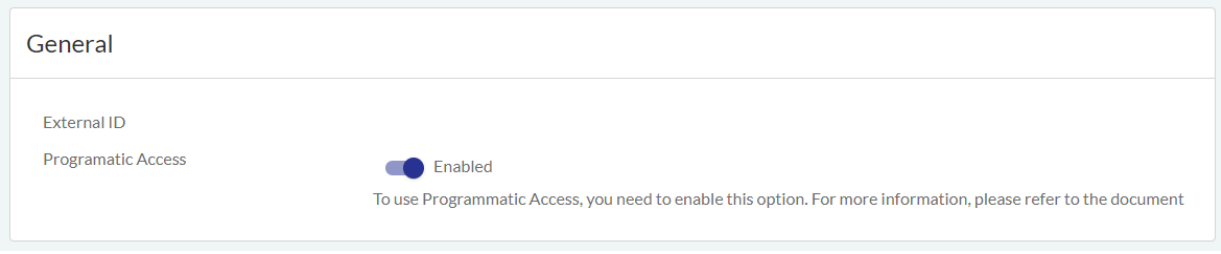
Da der programmgesteuerte Zugriff sehr effektiv ist, stellt Cloud NGFW keinen weiteren Zugriffsschlüssel oder geheimen Schlüssel zum Signieren von Autorisierungsanforderungen bereit. Stattdessen können Sie die IAM-Rolle in Ihrem AWS-Konto verwenden, um auf die Cloud NGFW-APIs zuzugreifen, und dann konfigurieren, welche IAM-Ressourcen diese Rolle übernehmen können. Dieser Ansatz verbessert den allgemeinen Sicherheitsstatus, da temporäre Anmeldeinformationen verwendet und automatisch gewechselt werden.

Der programmgesteuerte Zugriff in Cloud NGFW ist standardmäßig deaktiviert.

Informationen zu den API-Referenzmaterialien finden Sie in der Dokumentation zur Cloud NGFW-API.

**STEP 1 |** Programmgesteuerten Zugriff aktivieren

- Wählen Sie in der **Cloud NGFW Tenant (Cloud NGFW-Mandanten)**-Konsole die Option **Tenant (Mandant)** aus.
- Klicken Sie unter **General (Allgemein)** auf den Schieberegler **Programmatic Access (Programmgesteuerter Zugriff)**.
- Klicken Sie zur Bestätigung auf **Enable (Aktivieren)**.



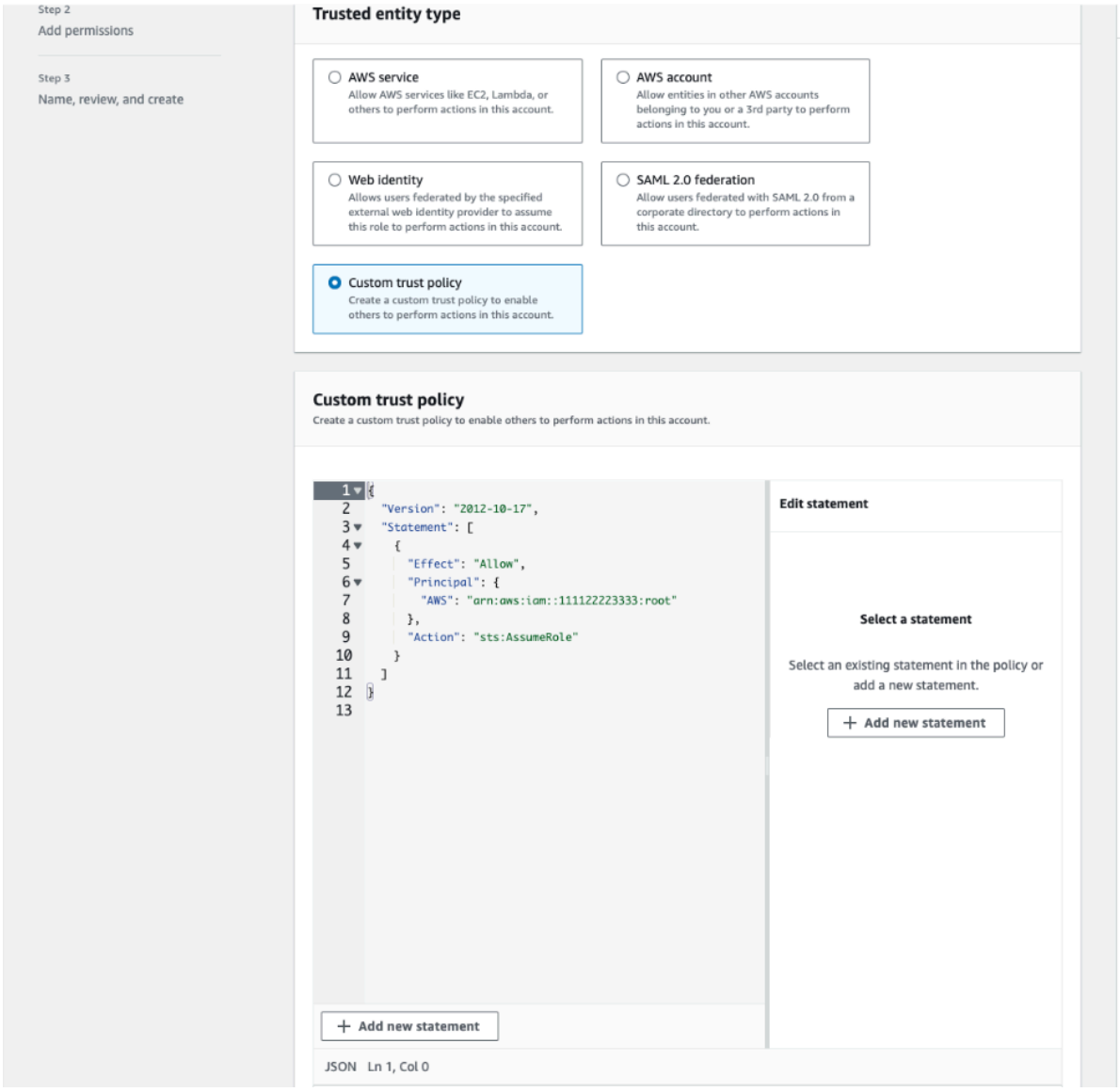

 

**STEP 2 |** Erstellen Sie eine neue Rolle mit einer *benutzerdefinierten Vertrauensrichtlinie*.

Im Folgenden ist ein Beispiel für eine benutzerdefinierte Vertrauensrichtlinie aufgeführt:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
 "Action": "sts:AssumeRole" } ] }
```

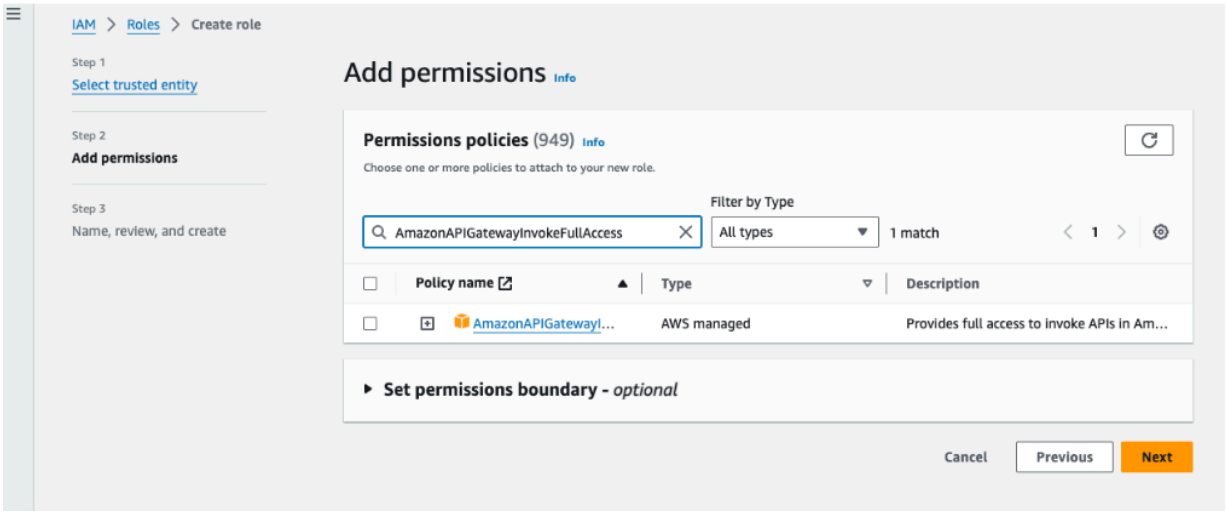
 



*Das oben erwähnte Beispiel für eine Vertrauensbeziehung mit dem Principal „root“ könnte den Zugriff auf mehr Principals ermöglichen als beabsichtigt. Die Elemente „Principal“ und „Condition“ können verwendet werden, um den Zugriff auf die Rolle für bestimmte Principals einzuschränken. Weitere Informationen finden Sie unter How to use trust policies with IAM roles. Sie können diese Rolle auch in einem AWS-Konto erstellen und bestimmte Berechtigungen mithilfe des kontoübergreifenden Zugriffs an ein anderes Konto delegieren. Informationen zur Definition einer Vertrauensrichtlinie mit kontoübergreifendem Zugriff finden Sie in den hier aufgeführten Beispielen.*

**STEP 3 |** Fügen Sie die Amazon-Berechtigungsrichtlinie **ApiGatewayInvokeFullAccess** hinzu, um APIs aufzurufen. Klicken Sie hier, um mehr zu erfahren.

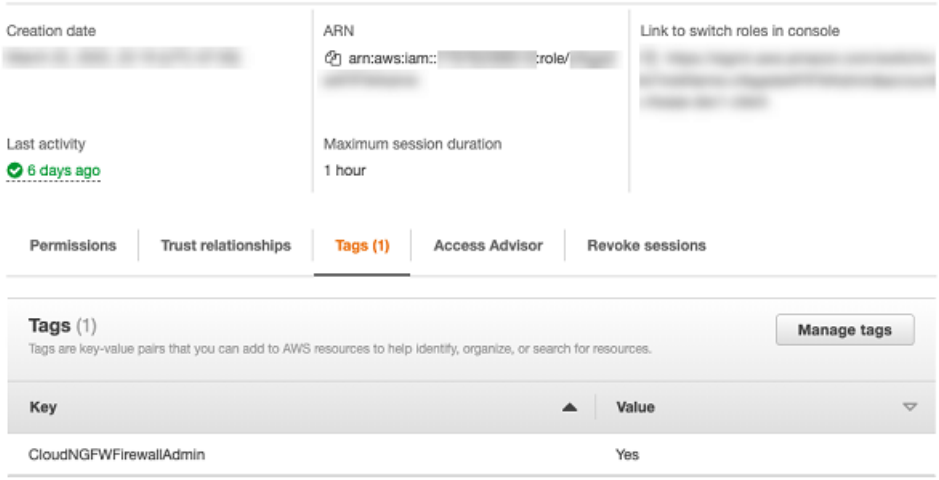



**STEP 4 |** Fügen Sie der IAM-Rolle die folgenden Tags (bestehend aus einem Schlüssel und einem Wert) hinzu, um nach Bedarf Berechtigungsrichtlinien bereitzustellen.

| Verwendung | TagKey | TagValue |
|---|---|---|
| Erstellen und Verwalten von Firewalls | `CloudNGFWFirewallAdmin` | Ja |
| Erstellen und Verwalten lokaler Regelstapel | `CloudNGFWRulestackAdmin` | Ja |

| Verwendung | TagKey | TagValue |
|---|---|---|
| Erstellen und Verwalten globaler Regelstapel | `CloudNGFWGlobalRulestackAdmin` | `Yes` |
| AWS-Konto einbinden | `CloudNGFWAccountAdmin` | Ja |




Sie können derselben Rolle mehrere Tags zuweisen. Diese Tags können für den Zugriff auf verschiedene Rollentoken für den programmgesteuerten Zugriff in Cloud NGFW verwendet werden.

**STEP 5 |** (Überspringen Sie die Schritte 7 bis 9, wenn Sie die Beispiele für den programmgesteuerten Zugriff in Cloud NGFW verwenden) Verwenden Sie die Beispiele in den `API`- und `CFT`-Ordnern unter dem Git-Repository, um auf das Tool für den programmgesteuerten Zugriff bzw. CFTs zuzugreifen.

*Laden Sie das gesamte Verzeichnis `programmatic_access` herunter, um Beispiele von Palo Alto Networks auszuführen.*

Das Tool übernimmt intern die Rolle und generiert den Zugriffsschlüssel und den geheimen Schlüssel für Ihre Rolle sowie den SigV4-Header. Außerdem wird die spezifische Endpunktrolle aufgerufen, um das Token für den programmgesteuerten Zugriff für Cloud NGFW abzurufen.

**STEP 6 |** Übernehmen Sie nach Bedarf Rollen mit den in Schritt 5 genannten Tagschlüssel/Tagwert-Paaren mithilfe der Befehlszeilenschnittstelle von AWS.

```
$ aws sts assume-role --role-arn arn:aws:iam::<AWS-ACCOUNT-
ID>:role/<ROLE-NAME> --profile <AWS-PROFILE-TO-ASSUME> --role-
session-name <SESSION-NAME> { "Credentials": { "AccessKeyId":
 "<ACCESS-KEY>", "SecretAccessKey": "<SECRET-ACCESS-KEY>",
 "SessionToken": "<SESSION-TOKEN>", "Expiration": "<CREDENTIALS-
EXPIRATION>" }, "AssumedRoleUser": { "AssumedRoleId": "<ROLE-
ID>:<SESSION-NAME>", "Arn": "arn:aws:iam::<AWS-ACCOUNT-ID>:role/
<ROLE-NAME>/<SESSION-NAME>" } }
```

Wenn Sie die Rolle übernehmen, werden ein temporärer Zugriffsschlüssel und ein temporärer geheimer Schlüssel für Ihr Konto generiert. Weitere Informationen finden Sie im Artikel zum Übernehmen von Rollen mit einem bestimmten Tag.

**STEP 7 |** Generieren Sie einen Signature-Version-4(SigV4)-Header anhand der temporären Anmeldeinformationen, die Sie in Schritt 7 erhalten haben. Weitere Informationen finden Sie im Artikel zum Signieren von AWS-Anforderungen mit SigV4.

Nachfolgend ist ein Beispiel für einen mit AWS SigV4 signierten Header aufgeführt.

```
AWS4-HMAC-SHA256 Credential=<ACCESS-KEY>/20220421/<REGION>/execute-
api/aws4_request, SignedHeaders=host;x-amz-date;x-amz-security-
token, Signature=<SIGNATURE>
```

**STEP 8 |** Generieren Sie `SubcriptionKey` und `TokenID`.

Um über REST-APIs auf Cloud NGFW zuzugreifen, verwenden Sie diesen Pfad vor dem API-Aufruf: `api.<region-name>.aws.cloudngfw.paloaltonetworks.com`. Weitere Informationen finden Sie in der API-Dokumentation.

- Für die Rolle des Cloud-Firewall-Administrators: `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudfirewalladmin`
- Für die Rolle des Cloud-Regelstapel-Administrators: `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudrulestackadmin`
- Für die Rolle des Cloud-Administrators für globalen Regelstapel: `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudglobalrulestackadmin`

**Token abrufen**

Nachfolgend ist ein Beispiel für den cURL-Befehl zum Abrufen eines Tokens aufgeführt.

```
$ curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/
cloudfirewalladmin' \ > --header 'X-Amz-Security-Token: <SESSION-
TOKEN>' \ > --header 'X-Amz-Date: <CREDENTIALS-EXPIRATION-AMZ-DATE-
FORMAT>' \ > --header 'Authorization: <AWS-V4-SIGNED-HEADER>'
```

**Antwort**

```
{"Response": {"TokenId": "<CLOUD-NGFW-PROGRAMMATIC-ACCESS-TOKEN>",
 "SubscriptionKey": "<SUBSCRIPTION-KEY>", "ExpiryTime": 30,
 "Enabled": true}, "ResponseStatus": {"ErrorCode": 0}}
```

**STEP 9 |** Fügen Sie die Antwortdaten dem Abschnitt **Header** in der Cloud NGFW-Konsole hinzu.

| Überschrift | Wert |
|---|---|
| Autorisierung | <TokenID> |

| Überschrift | Wert |
| --- | --- |
| x-api-key | <SubscriptionKey> |

Nachfolgend ist ein Beispiel für einen API-Aufruf in Cloud NGFW aufgeführt.

```
curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/config/rulestacks/
rs-1' \ > --header 'Authorization: <CLOUD-NGFW-PROGRAMMATIC-ACCESS-
TOKEN>' \ > --data-raw ''
```

**Antwort**

```
{"Response": {"RuleStackName": "rs-1", "RuleStackCandidate":
 {"Scope": "Local", "MinAppIdVersion": "8433-6838", "Profiles":
 {"AntiSpywareProfile": "BestPractice", "AntiVirusProfile":
 "BestPractice", "VulnerabilityProfile": "BestPractice",
 "URLFilteringProfile": "None", "FileBlockingProfile":
 "BestPractice"}, "UpdateToken": "1"}, "RuleStackState":
 "Uncommitted"}, "ResponseStatus": {"ErrorCode": 0}}
```

**STEP 10 |** Um den programmgesteuerten Zugriff zu widerrufen, verwenden Sie den Zugriffsschlüssel, den geheimen Schlüssel und den Abonnementschlüssel zum Aufrufen der Token-API: `DELETE https://:<region-name>.aws.cloudngfw.paloaltonetworks.comv1/mgmt/tokens/{TokenID}`.

*Zugriffsschlüssel und geheimer Schlüssel sind temporär. Generieren Sie einen neuen Zugriffsschlüssel und einen neuen geheimen Schlüssel, wenn diese ablaufen.*

# Terraform-Unterstützung für Cloud NGFW für AWS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

HashiCorp Terraform ist ein Open-Source-Infrastructure-as-Code-Tool für Teams, die Multi-Cloud-Umgebungen verwalten. Hiermit können Sie eine Konfiguration definieren, die den Zielzustand Ihrer Cloud-Infrastruktur beschreibt und daraus automatisch die notwendigen Schritte zum Erreichen des definierten Ziels berechnet, während die relevanten Änderungen zur Bereitstellung und Verwaltung der Cloud-Infrastruktur ausgeführt werden. Diese Terraform-Konfigurationen verwenden Plugins, die als *Provider* bezeichnet werden. Die Plug-ins interagieren mit Providern wie AWS, um die Wiederverwendung zu erleichtern, indem sie wiederholbare Schritte zum Erstellen und Warten der Cloud-Infrastruktur erstellen und so einfache Ergänzungen zu Ihrer CI/CD-Pipeline sicherstellen.

Palo Alto Networks fügt den cloudngfwaws-Provider hinzu, um den Aufbau der Sicherheitsinfrastruktur zu automatisieren und die Netzwerksicherheitslage mithilfe von NGFW-Regelstapeln aufrechtzuerhalten. Dieser Provider fungiert als Übersetzungsschicht, die die Kommunikation zwischen dem Client (dem Gerät, auf dem Terraform ausgeführt wird) und den APIs erleichtert, die der Cloud NGFW für AWS-Dienst bietet.

Lesen Sie die Palo Alto Networks Entwicklerdokumentation, um mehr über die Bereitstellung von Cloud NGFW für AWS mit Terraform zu erfahren und die Terraform-Referenzinformationen anzuzeigen.

Sie können den Terraform-Provider in Ihrer Konfiguration für folgende Aufgaben verwenden:

- Starten von Cloud NGFW.
- Konfigurieren des Regelstapels, mit dem Cloud NGFW Richtlinieninformationen abruft. Der Regelstapel enthält relevante Richtlinieninformationen wie Sicherheitsregeln, intelligente Feeds und verschiedene Objekte.

Verwenden Sie den Terraform-Provider **cloudngfwaws**, um auf Ressourcen zur Verwaltung von Cloud NGFW für AWS zuzugreifen. Der Provider **cloudngfwaws** authentifiziert sich bei AWS mithilfe der STS-Annahmerolle, die temporäre Anmeldeinformationen generiert. Zu diesen temporären Anmeldeinformationen, die während der ersten Authentifizierungssequenz kurz verwendet werden, gehören der Zugriffsschlüssel, der geheime Schlüssel und ein Sitzungstoken. Während dieser Sequenz geschieht Folgendes:

1. Die Authentifizierung nutzt die AWS STS-Annahmerolle mithilfe der AWS-API. Sie müssen den API-Zugriff aktivieren.
2. STS-Anmeldeinformationen werden verwendet, um das Cloud NGFW-Administratortoken mithilfe der Cloud NGFW für AWS-API zu aktualisieren. Mit diesen Anmeldeinformationen wird auch das Administratortoken des Regelstapels aktualisiert.

3. Das Cloud NGFW-Administratortoken und das Administratortoken des Regelstapels werden für die Konfigurationsverwaltung mithilfe der Cloud NGFW für AWS-API verwendet.

Erwägen Sie Folgendes:

- Nach erfolgreicher Authentifizierung bei AWS ruft der Provider die JWTs für die Firewall- und Regelstapelverwaltung ab.
- Sie können den AWS-Zugriff und den geheimen Schlüssel im Providerblock statisch angeben. Wenn Sie diese Anmeldeinformationen nicht angeben, werden sie automatisch aus der freigegebenen Anmeldeinformationsdatei abgerufen. Verwenden Sie die Parameter access_key und secret_key, um AWS-Anmeldeinformationen statisch bereitzustellen.
- Beim Einrichten des Providers verwendet der AWS-Authentifizierungsworkflow das AWS Go SDK, um zur Authentifizierung gehörende Variablen zu steuern. Sie können mithilfe von AWS-Umgebungsvariablen Anmeldeinformationen für die AWS-Authentifizierung konfigurieren.
- Der Provider benötigt API-Zugriff.

Providerparameter werden auf unterschiedliche Weise priorisiert. Bei überlappenden Werten werden diese Parameter in der folgenden Reihenfolge angegangen:

1. Statisch konfiguriert im Providerblock.
2. Umgebungsvariablen.
3. Abgerufen aus der JSON-Konfigurationsdatei.

**Beispiel eines Terraform-Providers für Cloud NGFW**

Terraform 0.13 und höher:

```
terraform { required_providers { cloudngfwaws = { source =
 "paloaltonetworks/terraform-provider-cloudngfwaws" version
 = "1.0.0" } } } provider "cloudngfwaws" { json_config_file =
 "~/.cloudngfwaws_creds.json" }
```

JSON-Konfigurationsdatei:

```
{ "host": "api.us-east-1.aws.cloudngfw.paloaltonetworks.com",
 "region": "us-east-1", "arn": "arn:aws:iam::123456789:role/MyRole" }
```

# Automatisierte Einbindung von Konten konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW für AWS unterstützt jetzt die automatisierte Einbindung von Konten für Umgebungen, die eine große Anzahl von AWS-Konten bedienen. Mit dieser Funktion müssen Sie einzelne Konten nicht mehr manuell einbinden. Wenn Sie die automatisierte Einbindung von Konten verwenden, sollten Sie Folgendes berücksichtigen:

- Es können bis zu 100 Konten gleichzeitig eingebunden werden. Um mehr als 100 Konten einzubinden, müssen Sie mehrere Module definieren, die jeweils 100 Konten enthalten. Weitere Informationen hierzu enthält die Terraform-Dokumentation.
- Die automatisierte Einbindung von Konten kann etwa 10 Minuten dauern.
- Wenn Sie ein AWS-Profil für AUTH nutzen, verwenden Sie das Profil `CloudNGFWGAccountAdmin` für das Onboarding von Konten.
- Erstellen Sie eine Rolle mit der CloudFormation-Vorlage (CloudFormation Template, CFT) und *wenden Sie Berechtigungen* in jedem der einzubindenden Konten an.
- Sie müssen die Cloud NGFW über den Marketplace abonniert haben und das Konto sollte erfolgreich eingebunden worden sein.
- Es sind zwei Rollen erforderlich:
  - Erstellen Sie die Rolle `CloudNGFWAccountAdmin` im Administratorkonto.
  - Erstellen Sie eine Rolle, die das Ausführen von CFTs in jedem der Konten ermöglicht, die Sie mit Terraform einbinden möchten.

*Diese Rollen werden im folgenden Verfahren beschrieben.*

Um auf die Funktion für die automatisierte Einbindung von Konten zugreifen zu können, müssen Sie die neueste Terraform-Vorlage herunterladen und den programmgesteuerten Zugriff aktivieren.

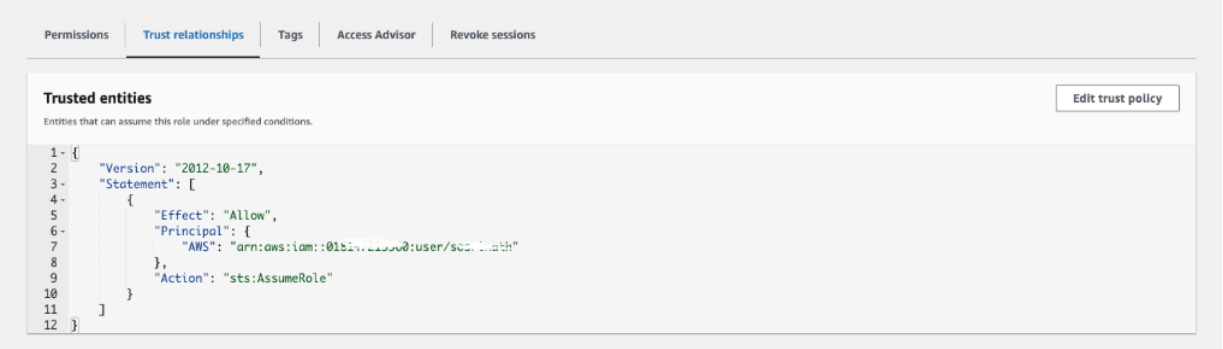
So konfigurieren Sie die automatisierte Einbindung von Konten:

**STEP 1 |** Erstellen Sie für alle derzeit eingebundenen Konten die Rolle `AccountAdmin` für den programmgesteuerten Zugriff. Führen Sie die Schritte 1 bis 4 unter „Programmgesteuerten Zugriff aktivieren“ aus, um eine Rolle mit dem Tag `CloudNGFWAccountAdmin` zu erstellen.

**STEP 2 |** Erstellen Sie in jedem einzubindenden Konto eine Rolle zum Ausführen der CloudFormation-Vorlage (CFT):

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::ACCOUNT_ID:user/USERNAME" },
 "Action": "sts:AssumeRole" } ] }
```

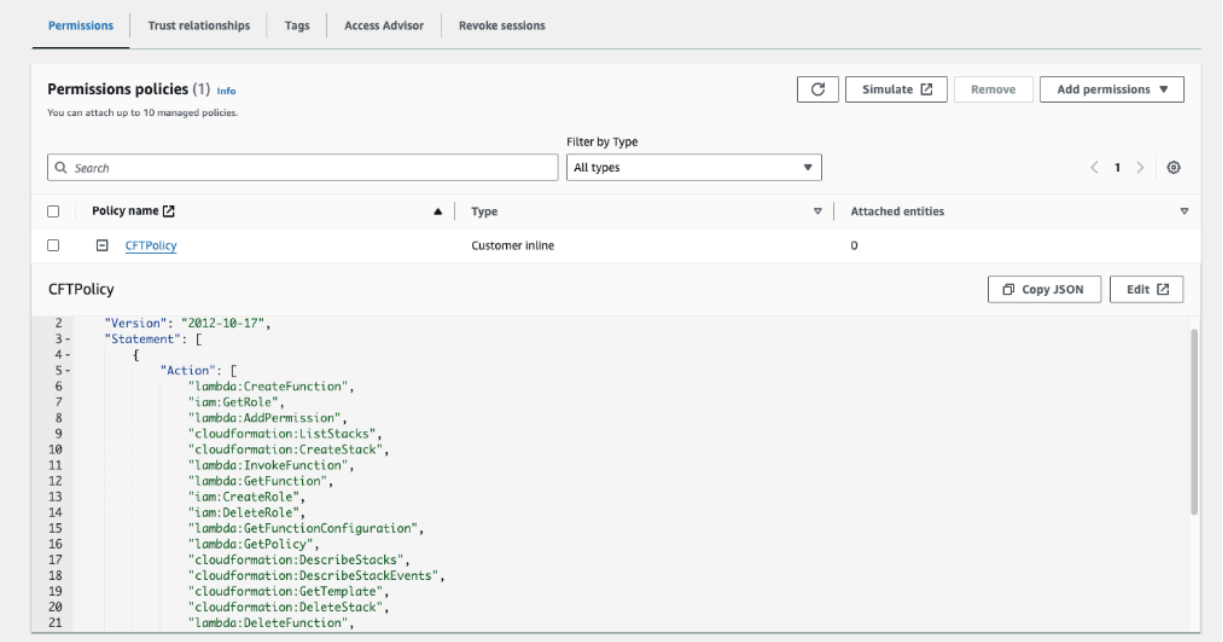



Die Berechtigungsrichtlinie der Rolle wird mit der Option **Create Inline Policy (Inline-Richtlinie erstellen)** definiert. Beispiel:

```
"Statement": [ { "Action": [ "lambda:CreateFunction",
 "iam:GetRole", "lambda:AddPermission",
 "cloudformation:ListStacks", "cloudformation:CreateStack",
 "lambda:InvokeFunction", "lambda:GetFunction", "iam:CreateRole",
 "iam:DeleteRole", "lambda:GetFunctionConfiguration",
 "lambda:GetPolicy", "cloudformation:DescribeStacks",
 "cloudformation:DescribeStackEvents",
 "cloudformation:GetTemplate", "cloudformation:DeleteStack",
 "lambda:DeleteFunction", "iam:DeleteRolePolicy",
 "iam:DetachRolePolicy", "iam:AttachRolePolicy",
```

```
"iam:PutRolePolicy", "iam:PassRole" ], "Resource": "*", "Effect":
"Allow", "Sid": "VisualEditor1" } ] }
```




*Das Beispiel eines Vertrauensverhältnisses (oben) gilt für einen bestimmten Benutzer in einem bestimmten Konto, dem die Berechtigung zum Ausführen der CFT erteilt wurde. Weitere Informationen zum Definieren einer eigenen Vertrauensrichtlinie finden Sie unter* How to use trust policies with IAM roles.

**STEP 3 |** Führen Sie Terraform Apply aus.

Nachdem Sie die Änderungen auf die CFT angewendet haben, bindet die Cloud NGFW-Ressource die einzelnen Konten ein:

- Das Modul zur Einbindung von Konten führt die Kontorolleneinrichtungs-CFT im Konto aus.
- Die kontoübergreifende Rollen-CFT sendet Rollen-ARNs an die Cloud NGFW-Ressource.

Das Modul zur Einbindung von Konten wartet eine gewisse Zeit (unter Umständen länger als 10 Minuten), bis alle Konten erfolgreich eingebunden wurden.

## Beispiel für eine Terraform-Datei

Das folgende Beispiel veranschaulicht eine Terraform-Datei, die die Provider- und Moduldefinitionen enthält. In diesem Beispiel bezieht sich „account_admin_arn“ auf die programmgesteuerte Zugriffsrolle, die in Schritt 1 erstellt wurde. Das Feld **account_ids** stellt die Liste der AWS-Konten dar, die eingebunden werden müssen. Das Feld **cft_role_name** stellt die Rolle dar, die in Schritt 2 in jedem der integrierten Konten erstellt wurde.

```
terraform { required_providers { cloudngfwaws = { source
 = "paloaltonetworks/cloudngfwaws" } } } provider
 "cloudngfwaws" { account_admin_arn = "arn:aws:iam::11222333344:role/
fwaas_prog_onboard" json_config_file = "./.cloudngfwaws_creds.json" }
 module "account_onboarding1" { source = “github.com/
PaloAltoNetworks/terraform-provider-cloudngfwaws/modules/
account_onboarding" account_ids = ["ACCOUNT_1", "ACCOUNT_2"....,
 “ACCOUNT_100”] cft_role_name = "cft_apply_role" } module
 "account_onboarding2" { source = “github.com/PaloAltoNetworks/
terraform-provider-cloudngfwaws/modules/account_onboarding"
 account_ids = ["ACCOUNT_101", "ACCOUNT_102"...., “ACCOUNT_200”]
 cft_role_name = "cft_apply_role" }
```

## Eingebundenes Konto löschen

Verwenden Sie Terraform **destroy**. Weitere Informationen hierzu finden Sie in der Terraform-Dokumentation.

## Eingebundenes Konto auflisten

Verwenden Sie Terraform **list**. Weitere Informationen hierzu finden Sie in der Terraform-Dokumentation.

# Cloud NGFW-Ressourcen für Ihre AWS CFT bereitstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Die Cloud NGFW bietet Flexibilität bei der Bereitstellung von Ressourcen für Ihre AWS CloudFormation-Vorlage (CFT), indem Sie Ihre eigenen Ressourcen erstellen können.

*Aktivieren Sie den programmatischen Zugriff, bevor Sie CloudFormation Registry mit der Cloud NGFW verwenden.*

Verwenden Sie die Schemas **PaloAltoNetworks::CloudNGFW::RuleStack** und **PaloAltoNetworks::CloudNGFW::NGFW**, um die Cloud NGFW in Ihre AWS CloudFormation-Vorlage zu integrieren. Definieren Sie mit der in diesem Dokument bereitgestellten Syntax Cloud NGFW-Konfigurationseinstellungen, die Sie in AWS CloudFormation Registry integrieren können.

**Schema PaloAltoNetworks::CloudNGFW::RuleStack**

- JSON

```
{ "Type" : "PaloAltoNetworks::CloudNGFW::RuleStack", "Properties" :
 { "RuleStackName" : String, "RuleStack" : RuleStack,
 "RuleList" : [ Rule, ... ], "SecurityObjects" : SecurityObjects,
 "CustomSecurityProfiles":CustomSecurityProfiles, } }
```

- YAML

```
Type:PaloAltoNetworks::CloudNGFW::RuleStack Properties:
 RuleStackName: String RuleStack: RuleStack RuleList: - Rule
 SecurityObjects: SecurityObjects CustomSecurityProfiles:
 CustomSecurityProfiles ProgrammaticAccessToken: String
```

| Element | Beschreibung |
|---|---|
| RuleStackName | Geben Sie einen beschreibenden **Namen** für Ihren Regelstapel ein.<br>**JSON**<br>`„RuleStackName“: String,` |

| Element | Beschreibung |
| --- | --- |
| | **YAML**<br>`RuleStackName: String` |
| RuleStack | Geben Sie eine **Beschreibung** für Ihren Regelstapel ein. Die Beschreibung beinhaltet:<br>**JSON**<br>`{ "Scope" : String, "Profiles" : RuleStackProfiles, "Description" : String "Deploy" : String }`<br>**YAML**<br>`Scope: String Profiles: RuleStackProfiles Description: String Deploy: String` |
| RuleStackProfiles | Geben Sie **Profile** für den angegebenen Regelstapel an. Profile beinhalten:<br>**JSON**<br>`{ "AntiSpywareProfile" : String, "AntiVirusProfile" : String, "VulnerabilityProfile" : String, "URLFilteringProfile" : String, "FileBlockingProfile" : String, "OutboundTrustCertificate" : String, "OutboundUntrustCertificate" : String }`<br>**YAML**<br>`AntiSpywareProfile: String AntiVirusProfile: String VulnerabilityProfile: String URLFilteringProfile: String FileBlockingProfile: String OutboundTrustCertificate: String OutboundUntrustCertificate: String` |
| Regel | Richten Sie **Regeln** für den Regelstapel ein. Regeln beinhalten:<br>**JSON**<br>`{ "RuleName" : String, "Description" : String, "RuleListType" : String, "Priority" : Integer, "Enabled" : Boolean, "Source" : RuleSource, "NegateSource" : Boolean, "Destination" : RuleDestination, "NegateDestination" : Boolean, "Applications" : [ String, ... ], "Category" : UrlCategory, "Protocol" : String, "AuditComment" : String, "Action" : String,` |

| Element | Beschreibung |
| --- | --- |
| | <pre>"Logging" : Boolean, "DecryptionRuleType" : String, "Tags" : [ Tag, ... ] }</pre><br>**YAML**<br><pre>RuleName: String Description: String RuleListType: String Priority: Integer Enabled: Boolean Source: RuleSource NegateSource: Boolean Destination: RuleDestination NegateDestination: Boolean Applications: - String Category: UrlCategory Protocol: String AuditComment: String Action: String Logging: Boolean DecryptionRuleType: String Tags: - Tag</pre> |
| RuleSource | Legen Sie die Sammlung von Regeln mithilfe von **RuleSource** fest. RuleSource beinhaltet:<br><br>**JSON**<br><pre>{ "Cidrs" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }</pre><br>**YAML**<br><pre>cidrs: - String PrefixLists: - String Countries: - String Feeds: - String</pre> |
| RuleDestination | Legen Sie **RuleDestination** für den Webdienst fest, der die Bestätigungs-URL und eine oder mehrere Datenerfassungs-URLs unterstützt. RuleDestination beinhaltet:<br><br>**JSON**<br><pre>{ "Cidrs" : [ String, ... ], "FqdnLists" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }</pre><br>**YAML**<br><pre>Cidrs: - String FqdnLists: - String PrefixLists: - String Countries: - String Feeds: - String</pre> |
| Tag | Geben Sie ein **Tag** für den Regelstapel an. Ein Tag beinhaltet:<br><br>**JSON**<br><pre>{ "Key" : String, "Value" : String }</pre> |

| Element | Beschreibung |
| --- | --- |
| | **YAML**<br>`Key: String Value: String` |
| UrlCategory | Verwenden Sie **UrlCategory**, um Kriterien in Authentifizierungs-, Entschlüsselungs-, QoS- und Sicherheitsrichtlinienregeln abzugleichen. UrlCategory beinhaltet:<br>**JSON**<br>`{ "URLCategoryNames" : [ String, ... ], "Feeds" : [ String, ... ] }`<br>**YAML**<br>`URLCategoryNames: - String Feeds: - String` |
| SecurityObjects | Legen Sie die **SecurityObjects** für den Regelstapel fest. SecurityObjects beinhalten:<br>**JSON**<br>`{ "PrefixList" : PrefixList, "FqdnLists" : FqdnList, "CustomUrlCategories" : CustomUrlCategory, "IntelligentFeeds" : IntelligentFeed, "CertificateLists" : CertificateList }`<br>**YAML**<br>`PrefixList: PrefixList FqdnList: FqdnList CustomUrlCategory: CustomUrlCategory IntelligentFeed: IntelligentFeed CertificateList: CertificateList` |
| CustomSecurityProfiles | Legen Sie **CustomSecurityProfiles** fest, um die Antivirenprüfung des Datenverkehrs zwischen vertrauenswürdigen Sicherheitszonen zu minimieren und die Prüfung des Datenverkehrs aus nicht vertrauenswürdigen Zonen wie dem Internet sowie des Datenverkehrs, der an hochsensible Ziele wie Serverfarmen gesendet wird, zu maximieren. CustomSecurityProfiles beinhalten:<br>**JSON**<br>`{ "FileBlocking" : FileBlocking }` |

| Element | Beschreibung |
| --- | --- |
| | **YAML**<br>`FileBlocking: FileBlocking` |
| PrefixLists | Verwenden Sie **PrefixList**, um Routen basierend auf Präfixen zu filtern. Durch die Definition einer Ordnungsnummer und von IP-Präfixen kann eine Zweigstelle oder ein ION-Gerät im Rechenzentrum Routen zulassen oder ablehnen. Die dynamische, automatisch generierte Präfixliste basiert auf dem, was das ION-Gerät ankündigt. Präfixe können geteilt oder nicht geteilt sein. Eine PrefixList beinhaltet:<br>**JSON**<br>`{ "Name" : String, "PrefixList" : [ String, ... ], "AuditComment" : String, "Description" : String }`<br>**YAML**<br>`Name: String PrefixList: - String AuditComment: String Description: String` |
| FqdnLists | Mit dem Objekt **FqdnLists** stellt DNS die FQDN-Auflösung für die IP-Adressen bereit, sodass die IP-Adressen nicht mehr bekannt sein und nicht jedes Mal manuell aktualisiert werden müssen, wenn der FQDN in eine neue IP-Adresse aufgelöst wird. FqdnLists beinhalten:<br>**JSON**<br>`{ "Name" : String, "Description" : String, "FqdnList" : [ String, ... ], "AuditComment" : String }`<br>**YAML**<br>`Name: String Description: String FqdnList: - String AuditComment: String` |
| CustomUrlCategories | Verwenden Sie **CustomURLCategories**, um ein benutzerdefiniertes URL-Filterungsobjekt zu erstellen, um Ausnahmen für die Durchsetzung von URL-Kategorien anzugeben und um eine benutzerdefinierte URL-Kategorie basierend auf mehreren URL-Kategorien zu erstellen:<br>• Ausnahmen für die Durchsetzung von URL-Kategorien definieren: Erstellen Sie eine benutzerdefinierte Liste von URLs, die Sie als Übereinstimmungskriterien in einer Sicherheitsrichtlinienregel verwenden möchten. Dies ist eine gute Möglichkeit, Ausnahmen für URL-Kategorien anzugeben, bei denen Sie bestimmte URLs anders erzwingen möchten als die URL-Kategorie, zu der sie gehören. |

| Element | Beschreibung |
| --- | --- |
| | • Eine benutzerdefinierte URL-Kategorie basierend auf mehreren PAN-DB-Kategorien definieren: Auf diese Weise können Sie die Durchsetzung für Websites, die einer Reihe von Kategorien entsprechen, gezielt bewirken. Die Website oder Seite muss mit allen Kategorien übereinstimmen, die als Teil der benutzerdefinierten Kategorie definiert sind.<br><br>CustomURLCategories beinhalten:<br><br>**JSON**<br><br>`{ "URLTargets" : [ String, ... ], "Name" : String, "Description" : String, "Action" : String, "AuditComment" : String }`<br><br>**YAML**<br><br>`URLTargets: - String Name: String Description: String Action: String AuditComment: String` |
| IntelligentFeeds | Verwenden Sie **IntelligentFeeds**, um die aktuellsten Bedrohungsdaten kontinuierlich bereitzustellen. IntelligentFeeds beinhalten:<br><br>**JSON**<br><br>`{ "Name" : String, "Description" : String, "Certificate" : String, "FeedURL" : String, "Type" : String, "Frequency" : String, "Time" : Integer, "AuditComment" : String }`<br><br>**YAML**<br><br>`Name: String Description: String Certificate: String FeedURL: String Type: String Frequency: String Time: Integer AuditComment: String` |
| CertificateObjects | Verwenden Sie **CertificateObjects**, um Elemente des Zertifikats zu definieren. CertificateObjects beinhaltet:<br><br>**JSON**<br><br>`{ "Name" : String, "Description" : String, "CertificateSignerArn" : String, "CertificateSelfSigned" : Boolean, "AuditComment" : String }`<br><br>**YAML**<br><br>`Name: String Description: String CertificateSignerArn: String` |

| Element | Beschreibung |
| --- | --- |
| | CertificateSelfSigned: Boolean AuditComment: String |
| FileBlocking | Verwenden Sie **FileBlocking**, um bestimmte Dateitypen zu kennzeichnen, die Sie blockieren oder überwachen möchten. Für den größten Teil des Datenverkehrs (einschließlich des Datenverkehrs in Ihrem internen Netzwerk) sollten Sie Dateien blockieren, von denen bekannt ist, dass sie Bedrohungen enthalten, oder die keinen wirklichen Anwendungsfall für Upload oder Download haben. FileBlocking beinhaltet:<br><br>**JSON**<br><br>{ "Direction" : String, "FileType" : String, "Description" : String, "Action" : String, "AuditComment" : String }<br><br>**YAML**<br><br>Direction: String FileType: String Description: String Action: String AuditComment: String |

**Schema PaloAltoNetworks::CloudNGFW::NGFW**

- JSON

```
{ "Type": "PaloAltoNetworks::CloudNGFW::NGFW", "Properties" :
 { "Description" : String, "EndpointMode" : String,
 "FirewallName" : String, "RuleStackName" : String,
 "RuleStackName" : String, "SubnetMappings" : [ String, ... ],
 "Tags" : [ Map, ... ], "VpcId" : String, "UpdateToken" :
 String, "LogDestinationConfigs" : [ LogProfileConfig, ... ],
 "CloudWatchMetricNamespace" : String, }
```

- YAML

```
Type: PaloAltoNetworks::CloudNGFW::NGFWProperties: AppIdVersion:
 String AutomaticUpgradeAppIdVersion: Boolean Description:
 String EndpointMode: String FirewallName: String RuleStackName:
 String RuleStackName: String SubnetMappings: - String Tags: -
 Map VpcId: String UpdateToken: String LogDestinationConfigs:
 - LogProfileConfig CloudWatchMetricNamespace: String
 ProgrammaticAccessToken: String
```

| Element | Beschreibung |
| --- | --- |
| LogProfileConfig | Verwenden Sie **LogProfileConfig**, um Einträge für Änderungen an der Firewallkonfiguration anzuzeigen. |

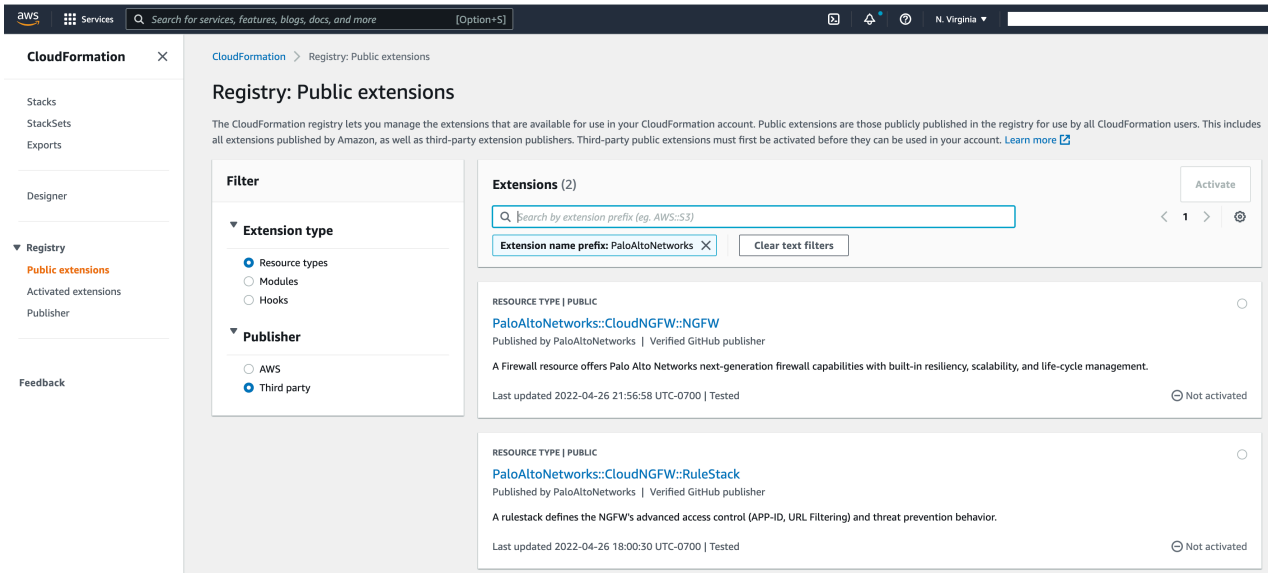
 

| Element | Beschreibung |
| --- | --- |
| | **JSON**<br>`{ "LogDestination" : String, "LogDestinationType" : String, "LogType" : String}`<br>**YAML**<br>`LogDestination: String LogDestinationType: String LogType: String` |

**Öffentliche Erweiterungen aktivieren**

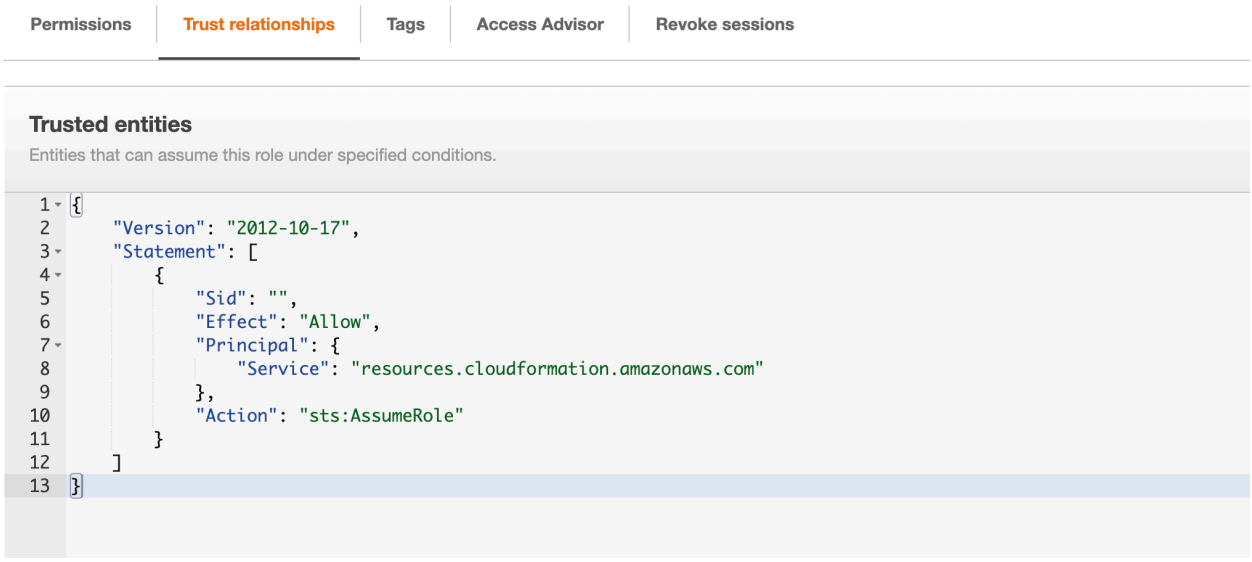
Aktivieren Sie die öffentlichen Erweiterungen **PaloAltoNetworks::CloudNGFW::NGFW** und **PaloAltoNetworks::CloudNGFW::RuleStack** für Ihr Konto:



Erstellen Sie einen Ausführungsrollen-ARN für die Erweiterungen. Beide Erweiterungen können dieselbe Rolle verwenden. Richten Sie Vertrauensbeziehungen in der Rolle ein, um die CloudFormation-Vorlagen zu verwenden:




Aktivieren Sie nach dem Einrichten der Vertrauensbeziehung die Erweiterungen:


Um Protokolle in AWS CloudWatch zu versenden, konfigurieren Sie die Protokollierung oder verwenden Sie Cloud NGFW für AWS.

### Stapelausgaben

Sie können auf diese Ressourcenattribute als Stapelausgaben zugreifen:

```
FirewallResource: "/properties/ReadFirewall", "/properties/
ReadFirewall/AccountId", "/properties/ReadFirewall/AppIdVersion",
 "/properties/ReadFirewall/AutomaticUpgradeAppIdVersion", "/
properties/ReadFirewall/EndpointMode", "/properties/ReadFirewall/
FirewallName", "/properties/ReadFirewall/MultiVpcEnable", "/
properties/ReadFirewall/Description", "/properties/ReadFirewall/
VpcId", "/properties/ReadFirewall/SubnetMappings", "/properties/
ReadFirewall/LinkId", "/properties/ReadFirewall/Attachments", "/
properties/ReadFirewall/LinkStatus", "/properties/ReadFirewall/
FirewallStatus", "/properties/ReadFirewall/RuleStackStatus",
 "/properties/ReadFirewall/FailureReason", "/properties/
```

```
ReadFirewall/EndpointServiceName", "/properties/ReadFirewall/
Tags", "/properties/ReadFirewall/RuleStackName", "/properties/
ReadFirewall/GlobalRuleStackName" RuleStackResource: "/properties/
RuleStackCandidate", "/properties/RuleStackRunning", "/properties/
RuleStackCandidate/AccountId", "/properties/RuleStackRunning/
AccountId", "/properties/RuleStackCandidate/Scope", "/properties/
RuleStackRunning/Scope", "/properties/RuleStackCandidate/
MinAppIdVersion", "/properties/RuleStackRunning/MinAppIdVersion",
 "/properties/RuleStackCandidate/Description", "/properties/
RuleStackRunning/Description", "/properties/RuleStackRunning/
Profiles/AntiSpywareProfile", "/properties/RuleStackCandidate/
Profiles/AntiSpywareProfile", "/properties/RuleStackRunning/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/Profiles/
VulnerabilityProfile", "/properties/RuleStackRunning/Profiles/
VulnerabilityProfile", "/properties/RuleStackCandidate/Profiles/
URLFilteringProfile", "/properties/RuleStackRunning/Profiles/
URLFilteringProfile", "/properties/RuleStackCandidate/Profiles/
FileBlockingProfile", "/properties/RuleStackRunning/Profiles/
FileBlockingProfile
```

**Ausführungsrolle**

Verwenden Sie Folgendes für die Ausführungsrolle:

Vertrauensverhältnis:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "Service":
 "resources.cloudformation.amazonaws.com" }, "Action":
 "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": "{customer-account-id}" },
 "StringLike": { "aws:SourceArn": "arn:aws:cloudformation:*:
{customer-account-id}":type/resource/PaloAltoNetworks-
CloudNGFW-NGFW/*" } } }, { "Effect": "Allow", "Principal":
 { "Service": "resources.cloudformation.amazonaws.com" },
 "Action": "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": {customer-account-id}" }, "StringLike":
 { "aws:SourceArn": "arn:aws:cloudformation:*:{customer-
account-id}":type/resource/PaloAltoNetworks-CloudNGFW-
RuleStack/*" } } } ] } Tags: CloudNGFWRulestackAdmin: Yes
 CloudNGFWFirewallAdmin: Yes CloudNGFWGlobalRulestackAdmin: Yes
 Permissions: AmazonAPIGatewayInvokeFullAccess
```

*Erstellen Sie eine Rolle und verwenden Sie dann den ARN der Rolle, um den ARN der Ausführungsrolle während der Aktivierung zu konfigurieren. Sie können keine Ressource erstellen, ohne die Ausführungsrolle während der Aktivierung zu konfigurieren.*

**Beispiel für CloudFormation Firewall-Ressourcenschema**

Verwenden Sie als Beispiel für das Regelstapelschema:

```
{ "typeName": "PaloAltoNetworks::CloudNGFW::NGFW", "description":
 "A Firewall resource offers Palo Alto Networks next-generation
 firewall capabilities with built-in resiliency, scalability,
```

```
 and life-cycle management.", "sourceUrl": "https://github.com/
aws-cloudformation/aws-cloudformation-rpdk.git", "definitions" :
 { "LogProfileConfig": { "title": "LogProfileConfig", "description":
 "Add Log profile config", "type": "object", "properties":
 { "LogDestination": { "title": "Logdestination", "minLength":
 1, "maxLength": 128, "type": "string" }, "LogDestinationType":
 { "title": "Logdestinationtype", "enum": ["S3", "CloudWatchLogs",
 "KinesisDataFirehose"], "type": "string" }, "LogType": { "title":
 "Logtype", "enum": ["TRAFFIC", "DECRYPTION", "THREAT"], "type":
 "string" } }, "required": ["LogDestination", "LogDestinationType",
 "LogType"], "additionalProperties": false }, "SubnetMappings":
 { "type": "array", "items": { "type": "object", "properties":
 { "AvailabilityZone": { "title": "availabilityZone", "type":
 "string" }, "SubnetId": { "title": "subnetId", "type": "string" } },
 "additionalProperties": false } } }, "properties": { "AccountId":
 { "title": "Accountid", "pattern": "^[0-9]+$", "type": "string",
 "minLength": 1 }, "AppIdVersion": { "title": "Appidversion",
 "minLength": 1, "maxLength": 64, "pattern": "^[0-9]+-[0-9]+
$", "type": "string" }, "AutomaticUpgradeAppIdVersion":
 { "title": "Automaticupgradeappidversion", "default": true,
 "type": "boolean" }, "Description": { "title": "Description",
 "type": "string", "minLength": 1 }, "EndpointMode": { "title":
 "Endpointmode: CustomerManaged Or ServiceManaged", "enum":
 ["ServiceManaged", "CustomerManaged"], "type": "string" },
 "FirewallName": { "title": "Firewallname", "minLength": 1,
 "maxLength": 128, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" },
 "MultiVpcEnable": { "title": "MultiVpcEnable", "type": "boolean" },
 "RuleStackName": { "title": "Rulestackname", "type": "string",
 "minLength": 1 }, "SubnetMappings": { "$ref": "#/definitions/
SubnetMappings" }, "AssociateSubnetMappings": { "$ref": "#/
definitions/SubnetMappings" }, "DisassociateSubnetMappings":
 { "$ref": "#/definitions/SubnetMappings" }, "Tags": { "title":
 "Tags", "type": "array", "items": { "type": "object" } },
 "VpcId": { "title": "Vpcid", "type": "string", "minLength": 1 },
 "LinkId": { "title": "LinkId", "type": "string", "minLength": 1 },
 "LogDestinationConfigs": { "title": "Logdestinationconfigs", "type":
 "array", "items": { "$ref": "#/definitions/LogProfileConfig" } },
 "CloudWatchMetricNamespace": { "title": "Cloudwatchmetricnamespace",
 "type": "string", "minLength": 1 } }, "additionalProperties":
 false, "required": [ "FirewallName" ], "createOnlyProperties": [ "/
properties/FirewallName" ], "primaryIdentifier": [ "/properties/
FirewallName" ], "handlers": { "create": { "permissions": [ "execute-
api:Invoke" ] }, "read": { "permissions": [ "execute-api:Invoke" ] },
 "update": { "permissions": [ "execute-api:Invoke" ] }, "delete":
 { "permissions": [ "execute-api:Invoke" ] } } }
```

**Beispiel für das Regelstapelschema**

Verwenden Sie das folgende Beispiel für das Regelstapelschema:

```
{ "typeName": "PaloAltoNetworks::CloudNGFW::RuleStack",
 "description": "A rulestack defines the NGFW's advanced access
 control (APP-ID, URL Filtering) and threat prevention behavior.",
 "sourceUrl": "https://github.com/aws-cloudformation/aws-
cloudformation-rpdk.git", "definitions": { "RuleStack": { "title":
 "RuleStack", "type": "object", "properties": { "AccountId":
```

```
 { "title": "Accountid", "pattern": "^[0-9]+$", "type": "string",
 "minLength": 1 }, "Scope": { "title": "Scope", "default":
 "Local", "enum": ["Local", "Global"], "type": "string" },
 "LookupXForwardedFor": { "title": "LookupXForwardedFor",
 "default": "None", "enum": ["SecurityPolicy", "None"], "type":
 "string" }, "MinAppIdVersion": { "title": "Minappidversion",
 "default": "8433-6838", "pattern": "8\\d\\d\\d\\-\\d\\d\\d\
\d", "type": "string" }, "Profiles": { "$ref": "#/definitions/
RuleStackProfiles" }, "Description": { "title": "Description",
 "maxLength": 512, "type": "string" }, "Deploy": { "title": "Deploy",
 "description": "Deploy RuleStack YES/NO", "default": "YES", "type":
 "string" } }, "additionalProperties": false }, "RuleStackProfiles":
 { "title": "RuleStackProfiles", "type": "object", "properties":
 { "AntiSpywareProfile": { "title": "Antispywareprofile", "default":
 "BestPractice", "enum": ["BestPractice", "None"], "type":
 "string" }, "AntiVirusProfile": { "title": "Antivirusprofile",
 "default": "BestPractice", "enum": ["BestPractice", "None"],
 "type": "string" }, "VulnerabilityProfile": { "title":
 "Vulnerabilityprofile", "default": "BestPractice", "enum":
 ["BestPractice", "None"], "type": "string" }, "URLFilteringProfile":
 { "title": "Urlfilteringprofile", "default": "None", "enum":
 ["BestPractice", "None"], "type": "string" }, "FileBlockingProfile":
 { "title": "Fileblockingprofile", "default": "BestPractice",
 "enum": ["Custom", "BestPractice", "None"], "type": "string" },
 "OutboundTrustCertificate": { "title": "Outboundtrustcertificate",
 "maxLength": 63, "type": "string" }, "OutboundUntrustCertificate":
 { "title": "Outbounduntrustcertificate", "maxLength": 63, "type":
 "string" } }, "additionalProperties": false }, "Tag": { "title":
 "Tag", "type": "object", "properties": { "Key": { "title": "Key",
 "minLength": 1, "maxLength": 128, "type": "string" }, "Value":
 { "title": "Value", "minLength": 1, "maxLength": 128, "type":
 "string" } }, "required": ["Key", "Value"], "additionalProperties":
 false }, "Rule" : { "title": "Rule", "type": "object", "properties":
 { "RuleName": { "title": "Rulename", "minLength": 1, "maxLength":
 48, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "Description":
 { "title": "Description", "maxLength": 512, "type": "string" },
 "RuleListType": { "title": "RuleListType", "description":
 "RuleList type: LocalRule, PreRule, PostRule", "type": "string" },
 "Priority": { "title": "Priority", "description": "Priority of
 the Rule", "type": "integer" }, "Enabled": { "title": "Enabled",
 "default": true, "type": "boolean" }, "Source": { "$ref": "#/
definitions/RuleSource" }, "NegateSource": { "title": "Negatesource",
 "default": false, "type": "boolean" }, "Destination": { "$ref":
 "#/definitions/RuleDestination" }, "NegateDestination": { "title":
 "Negatedestination", "default": false, "type": "boolean" },
 "Applications": { "title": "Applications", "default": ["any"],
 "type": "array", "items": { "type": "string", "maxLength":
 63 } }, "Category": { "$ref": "#/definitions/UrlCategory" },
 "Protocol": { "title": "Protocol", "default": "application-default",
 "maxLength": 63, "type": "string" }, "ProtPortList": { "title":
 "ProtPortList", "type": "array", "items": { "type": "string",
 "maxLength": 63 } }, "AuditComment": { "title": "Auditcomment",
 "maxLength": 512, "type": "string" }, "Action": { "title":
 "Action", "default": "Allow", "enum": ["Allow", "DenySilent",
 "DenyResetServer", "DenyResetBoth"], "type": "string" },
 "Logging": { "title": "Logging", "default": false, "type":
```

```
 "boolean" }, "DecryptionRuleType": { "title": "Decryptionruletype",
 "enum": ["SSLOutboundInspection", "SSLInboundInspection",
 "SSLOutboundNoInspection", "SSLInboundNoInspection"], "type":
 "string" }, "InboundInspectionCertificate": { "title":
 "InboundInspectionCertificate", "type": "string", "maxLength":
63 }, "Tags": { "title": "Tags", "maxItems": 200, "type":
 "array", "items": { "$ref": "#/definitions/Tag" } } }, "required":
 ["RuleName", "RuleListType", "Priority"], "additionalProperties":
 false }, "RuleSource": { "title": "RuleSource", "type": "object",
 "properties": { "Cidrs": { "title": "Cidrs", "type": "array",
 "items": { "type": "string", "maxLength": 24 } }, "PrefixLists":
 { "title": "Prefixlists", "type": "array", "items": { "type":
 "string", "maxLength": 63 } }, "Countries": { "title": "Countries",
 "description": "Country code", "type": "array", "items": { "type":
 "string", "maxLength": 2 } }, "Feeds": { "title": "Feeds", "type":
 "array", "items": { "type": "string", "maxLength": 63 } } },
 "additionalProperties": false }, "RuleDestination": { "title":
 "RuleDestination", "type": "object", "properties": { "Cidrs":
 { "title": "Cidrs", "type": "array", "items": { "type": "string",
 "maxLength": 24 } }, "FqdnLists": { "title": "Fqdnlists", "type":
 "array", "items": { "type": "string", "maxLength": 63 } },
 "PrefixLists": { "title": "Prefixlists", "type": "array", "items":
 { "type": "string", "maxLength": 63 } }, "Countries": { "title":
 "Countries", "description": "Country code", "type": "array",
 "items": { "type": "string", "maxLength": 2 } }, "Feeds": { "title":
 "Feeds", "type": "array", "items": { "type": "string", "maxLength":
 63 } } }, "additionalProperties": false }, "UrlCategory": { "title":
 "UrlCategory", "type": "object", "properties": { "URLCategoryNames":
 { "title": "Urlcategorynames", "type": "array", "items": { "type":
 "string", "maxLength": 128 } }, "Feeds": { "title": "Feeds",
 "type": "array", "items": { "type": "string", "maxLength":
 63 } } }, "additionalProperties": false }, "CustomSecurityProfiles":
{ "description": "Custom Security Profiles object", "type":
 "object", "properties": { "FileBlocking": { "$ref": "#/definitions/
FileBlocking" } }, "additionalProperties": false }, "FileBlocking":
{ "title": "FileBlocking", "type": "object", "properties":
 { "Direction": { "title": "Direction", "default": "both", "enum":
 ["upload", "download", "both"], "type": "string" }, "FileType":
 { "title": "FileType", "type": "string" }, "Description": { "title":
 "Description", "minLength": 1, "maxLength": 255, "type": "string" },
 "Action": { "title": "Action", "default": "alert", "enum":
 ["alert", "block", "continue"], "type": "string" }, "AuditComment":
 { "title": "Auditcomment", "type": "string" } }, "required":
 ["FileType"], "additionalProperties": false }, "SecurityObjects":
 { "description": "Security objects", "type": "object", "properties":
 { "PrefixLists": { "type": "array", "uniqueItems": false,
 "items": { "$ref": "#/definitions/PrefixList" } }, "FqdnLists":
 { "type": "array", "uniqueItems": false, "items": { "$ref":
 "#/definitions/FqdnList" } }, "CustomUrlCategories": { "type":
 "array", "uniqueItems": false, "items": { "$ref": "#/definitions/
CustomUrlCategory" } }, "IntelligentFeeds": { "type": "array",
 "uniqueItems": false, "items": { "$ref": "#/definitions/
IntelligentFeed" } }, "CertificateObjects":{ "type": "array",
 "uniqueItems": false, "items": { "$ref": "#/definitions/
CertObject" } } }, "additionalProperties": false }, "PrefixList":
 { "title": "PrefixList", "description": "SecurityObjects
```

```
 PrefixList", "type": "object", "properties": { "Name": { "title":
 "Name", "minLength": 1, "maxLength": 58, "pattern": "^[a-
zA-Z0-9-]+$", "type": "string" }, "PrefixList": { "title":
 "Prefixlist", "type": "array", "items": { "type": "string" } },
 "AuditComment": { "title": "Auditcomment", "maxLength": 512,
 "type": "string" }, "Description": { "title": "Description",
 "maxLength": 512, "type": "string" } }, "required": ["Name",
 "PrefixList"], "additionalProperties": false }, "FqdnList":
{ "title": "FqdnList", "type": "object", "properties": { "Name":
 { "title": "Name", "minLength": 1, "maxLength": 58, "pattern":
 "^[a-zA-Z0-9-]+$", "type": "string" }, "Description": { "title":
 "Description", "maxLength": 512, "type": "string" }, "FqdnList":
 { "title": "Fqdnlist", "type": "array", "items": { "type": "string",
 "minLength": 1, "maxLength": 255, "pattern": "^[a-zA-Z0-9._-]+
$" } }, "AuditComment": { "title": "Auditcomment", "maxLength":
 512, "type": "string" } }, "required": ["Name", "FqdnList"],
 "additionalProperties": false }, "CustomUrlCategory":{ "title":
 "CustomURLCategory", "type": "object", "properties": { "URLTargets":
 { "title": "Urltargets", "type": "array", "items": { "type":
 "string", "minLength": 1, "maxLength": 255 } }, "Name": { "title":
 "Name", "minLength": 1, "maxLength": 58, "pattern": "^[a-zA-Z0-9-]+
$", "type": "string" }, "Description": { "title": "Description",
 "minLength": 1, "maxLength": 255, "type": "string" }, "Action":
 { "title": "Action", "type": "string", "default": "none", "enum":
 ["none", "allow", "alert", "block"] }, "AuditComment": { "title":
 "Auditcomment", "type": "string" } }, "required": ["URLTargets"],
 "additionalProperties": false }, "IntelligentFeed":{ "title":
 "IntelligentFeed", "type": "object", "properties": { "Name":
 { "title": "Name", "minLength": 1, "maxLength": 63, "pattern":
 "^[a-zA-Z0-9-]+$", "type": "string" }, "Description": { "title":
 "Description", "maxLength": 512, "type": "string" }, "Certificate":
 { "title": "Certificate", "type": "string" }, "FeedURL": { "title":
 "Feedurl", "minLength": 1, "maxLength": 255, "pattern": "^(http|
https)://.+$", "type": "string" }, "Type": { "title": "Type",
 "enum": ["IP_LIST", "URL_LIST"], "type": "string" }, "Frequency":
 { "title": "Frequency", "enum": ["HOURLY", "DAILY"], "type":
 "string" }, "Time": { "title": "Time", "default": 3, "minimum":
 0, "maximum": 23, "type": "integer" }, "AuditComment": { "title":
 "Auditcomment", "maxLength": 512, "type": "string" } }, "required":
 ["Name", "FeedURL", "Type", "Frequency"], "additionalProperties":
 false }, "CertObject":{ "title": "Certificate Object", "type":
 "object", "properties": { "Name": { "title": "Name", "minLength":
 1, "maxLength": 63, "pattern": "^[a-zA-Z0-9-]+$", "type":
 "string" }, "Description": { "title": "Description", "maxLength":
 512, "type": "string" }, "CertificateSignerArn": { "title":
 "Certificatesignerarn", "type": "string" }, "CertificateSelfSigned":
 { "title": "Certificateselfsigned", "default": false, "type":
 "boolean" }, "AuditComment": { "title": "Auditcomment",
 "maxLength": 512, "type": "string" } }, "required": ["Name"],
 "additionalProperties": false } }, "properties": { "RuleStackName":
 { "description": "Rule stack name", "minLength": 1, "maxLength":
 128, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "RuleStack":
 { "$ref": "#/definitions/RuleStack" }, "RuleList": { "description":
 "list of rules", "type": "array", "uniqueItems": false, "items":
 { "$ref": "#/definitions/Rule" } }, "SecurityObjects": { "$ref": "#/
definitions/SecurityObjects" }, "CustomSecurityProfiles": { "$ref":
```

```
 "#/definitions/CustomSecurityProfiles" } }, "additionalProperties":
 false, "required": [ "RuleStackName" ], "createOnlyProperties":
 [ "/properties/RuleStackName" ], "primaryIdentifier": [ "/
properties/RuleStackName" ], "handlers": { "create": { "permissions":
 [ "execute-api:Invoke" ] }, "read": { "permissions": [ "execute-
api:Invoke" ] }, "update": { "permissions": [ "execute-
api:Invoke" ] }, "delete": { "permissions": [ "execute-
api:Invoke" ] } } }
```

# Kontoübergreifende Rollen-CFT-Berechtigungen für Cloud NGFW

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Cloud NGFW für AWS | ❑ Cloud NGFW-Abonnement<br>❑ Konto beim Kundensupport von Palo Alto Networks (CSP)<br>❑ AWS Marketplace-Konto<br>❑ Benutzerrolle (entweder Mandant oder Administrator) |

Cloud NGFW erfordert Berechtigungen für den Zugriff auf Informationen und Ressourcen, die Ihren AWS-Konten zugeordnet sind. Wenn Sie ein AWS-Konto einbinden, wird eine CloudFormation-Vorlage (CFT) bereitgestellt, um Ihnen bei der Aktivierung der Berechtigungen zu helfen. Wenn Sie die CFT bereitstellen, erstellt sie eine kontoübergreifende IAM-Rolle in Ihrem AWS-Konto. Diese IAM-Rolle stellt Cloud NGFW die erforderlichen Berechtigungen zum Lesen von VPC-Informationen bereit, die erforderlich sind, um Endpunkte zu erstellen und zu verwalten, Protokolle an Protokollierungsziele zu senden und auf Zertifikate im AWS Secrets Manager zur Entschlüsselung des Datenverkehrs zuzugreifen.

**Endpunktkonfiguration**

Die kontoübergreifende IAM-Rolle erfordert Berechtigungen zum Lesen von Informationen zu Ihren VPC-Ressourcen, damit Sie NGFW-Endpunkte in Ihrer AWS-Umgebung konfigurieren können.

```
{ "Sid": "Allow Cloud NGFW to read VPC resources", "Effect":
 "Allow", "Action": [ # The first four permission are the
 minimum needed "ec2:DescribeVpcs", "ec2:DescribeSubnets",
 "ec2:DescribeAvailabilityZones "ec2:DescribeVpcEndpoints", ],
 "Resource": "*" }
```

**Endpunkterstellung**

(optional) Sie können Cloud NGFW konfigurieren, um NGFW-Endpunkte in Ihrem AWS-Konto zu erstellen und zu verwalten. Wenn Sie diese Berechtigungen nicht konfigurieren möchten, müssen Sie NGFW-Endpunkte manuell erstellen, nachdem Sie Ihre NGFW bereitgestellt haben.

```
{ "Sid": "Allow Cloud NGFW to manage NGFW endpoints",
 "Effect": "Allow", "Action": [ "ec2:deleleVpcEndpoints"
 "ec2:CreateVpcEndpoints" ], "Resource": "*" }
```

**Protokollierung und Metrikverwaltung**

(optional) Die kontoübergreifende Rolle umfasst Berechtigungen, die für die Protokollierung und Metrikverwaltung erforderlich sind. Die Vorlage erstellt nicht die Protokollierungsziele. Stattdessen stellt sie die erforderlichen Berechtigungen für den Zugriff auf die angegebenen Protokollierungsziele bereit. Sie müssen die Protokollierungsziele erstellen, die Sie in der Vorlage angeben.

Die Vorlage stellt den Standardwert **PaloAltoCloudNGFW** für einen CloudWatch-Namespace und Kinesis Date Firehose bereit. Die Vorlage stellt keinen Standardwert für einen S3-Bucket bereit. Sie können den Standardwert durch den Wert eines entsprechenden Protokollierungsziels in Ihrem AWS-Konto ersetzen.

```
{ "Sid": "Allow Cloud NGFW access to one Cloudwatch
 Namespace", "Effect": "Allow", "Resource": "*", "Action":
 "cloudwatch:PutMetricData", "Condition": { "StringEquals":
 { "cloudwatch:namespace": "PaloAltoCloudNGFW" } } }{ "Sid":"Allow
 Cloud NGFW access to write logs in one LogGroup", "Action":
 [ "logs:CreateLogStream", "logs:DescribeLogStreams",
 "logs:PutLogEvents", ], "Effect": "Allow", "Resource":
 [ "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW"
 "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW:log-stream:*" ], }
{ "Sid": "Optionally, Allow Cloud NGFW to write logs to one
 S3 bucket", "Effect": "Allow", "Action": [ "s3:putObject" ],
 "Resource": [ # this is proposal #1 - name is coded
 based on externalid "arn:aws:s3:::<PaloAltoCloudNGFW-
ExternalD>/*" # this is proposal #2 - name is provided by
 customer in CFT. 'arn:aws:s3:::${S3Bucket}/*' ] }{ "Sid":
 " Optionally, Allow Cloud NGFW to write logs to Streams",
 "Effect": "Allow", "Action": [ "firehose:putRecordBatch" ],
 "Resource": [ "arn:aws:kinesis:region:account:deliveryStream/
PaloAltoCloudNGFW*" ], }
```

#### Entschlüsselung

(optional) Die kontoübergreifende Rolle umfasst Berechtigungen für Cloud NGFW, um Zertifikate vom Secrets Manager in Ihrem AWS-Konto abzurufen und damit den Datenverkehr zu entschlüsseln, der durch Ihre NGFW fließt. Diese Berechtigungen verwenden den Mechanismus der attributbasierten Zugriffskontrolle (ABAC), indem ein Tag für den Zugriff angegeben wird. Diese Berechtigungen sind optional und Sie können sich dafür entscheiden, sie nicht zu konfigurieren, wenn Sie die Vorlage bereitstellen.

```
{ "Sid": "Allow Cloud NGFW to pick up certificates", "Effect":
 "Allow", "Action": [ "secretsmanager:GetSecretValue" ],
 "Resource": "*", "Condition": { "StringEquals": { "aws:ResourceTag/
PaloAltoCloudNGFW": "true" } } }
```

#### Kontoüberwachung

(Optional) Der vorhandenen CloudFormation-Vorlage (CloudFormation Template, CFT) Ihres eingebundenen AWS-Kontos können Kontoüberwachungsberechtigungen hinzugefügt werden.

```
{ "Version": "2012-10-17", "Statement": [ { "Action":
 [ "ec2:DescribeVpcs", "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeSecurityGroups", "ec2:DescribeInstances",
 "ec2:DescribeVpcEndpoints", "ec2:DescribeSubnets",
 "ec2:DescribeManagedPrefixLists",
 "elasticloadbalancing:DescribeLoadBalancers",
 "elasticloadbalancing:DescribeTags" ], "Resource": "*", "Effect":
 "Allow" }, { "Action": [ "ec2:GetManagedPrefixListAssociations",
```

```
"ec2:GetManagedPrefixListEntries" ], "Resource":
[ "arn:aws:ec2:*:*:prefix-list/*" ], "Effect": "Allow" } ] }
```