paloalto TECHDOCS

Cloud NGFW für AWS

2.0.0

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

July 26, 2022

Table of Contents

Erste Schritte in Cloud NGFW für AWS

Cloud NGFW für AWS ist eine ML-basierte Next-Generation Firewall (NGFW) von Palo Alto Networks, deren Funktionen als vollständig verwalteter cloudnativer Dienst auf der AWS-Plattform (Amazon Web Services) bereitgestellt werden. Bei diesem Bereitstellungsmodell wird die Leistung von Palo Alto NGFW mit Benutzerfreundlichkeit kombiniert. Der Cloud NGFW-Dienst bietet erweiterte Anwendungstransparenz und Zugriffskontrolle mithilfe der Technologien für App-ID und URL-Filterung von Palo Alto Networks. Er bietet Bedrohungsabwehr und -erkennung durch in der Cloud bereitgestellte Sicherheitsdienste und Bedrohungsabwehrsignaturen.

Informationen zu Cloud NGFW für AWS

Sie können Cloud NGFW im AWS Marketplace finden und in Ihren AWS Virtual Private Clouds (VPC) nutzen. Mit Cloud NGFW können Sie auf die wichtigsten NGFW-Funktionen wie App-ID, URL-Filterung basierend auf URL-Kategorien und Geolokalisierungen, SSL/TLS-Entschlüsselung usw. zugreifen.

Cloud NGFW-Komponenten

Cloud NGFW für AWS erstellt eine Reihe von Komponenten, die zusammen Ihre AWS-Umgebung sichern.

- Der **Cloud NGFW-Mandant** ist eine Instanziierung des Cloud NGFW-Diensts, der Ihrem AWS-Konto zugeordnet ist, wenn einer Ihrer AWS-Benutzer den Dienst abonniert. Cloud NGFW ernennt Sie, den abonnierenden AWS-Benutzer, zum Administrator des Cloud NGFW-Mandanten (Benutzerrolle „TenantAdmin“), der andere Benutzer zum Mandanten einladen kann. Basierend auf der zugewiesenen Rolle können andere Benutzer Cloud NGFW-Ressourcen erstellen und Regelstapel mit dem Mandanten konfigurieren.
- Die **Cloud NGFW-Ressource** (oder einfach NGFW) ist Ihrer VPC zugeordnet und kann sich über mehrere Verfügbarkeitszonen erstrecken. Diese Ressource verfügt über integrierte Ausfallsicherheit, Skalierbarkeit und Lebenszyklusverwaltung.
- Um die Cloud NGFW-Ressource zu verwenden, erstellen Sie ein dediziertes Subnetz in Ihrer VPC für jede gewünschte AWS-Verfügbarkeitszone, erstellen dann **NGFW-Endpunkte** in den Subnetzen und aktualisieren die VPC-Routing-Tabellen, um den Datenverkehr über diese Cloud NGFW-Endpunkte zu leiten.
- **Regelstapel** definieren das Filterverhalten des NGFW-Datenverkehrs, z. B. erweiterte Zugriffskontrolle (App-ID, URL-Filterung) und Bedrohungsabwehr. Ein Regelstapel enthält eine Reihe von Sicherheitsregeln sowie die zugehörigen Objekte und Sicherheitsprofile. Um einen Regelstapel zu verwenden, verknüpfen Sie ihn mit einer oder mehreren NGFW-Ressourcen. Cloud NGFW bietet zwei Typen von Regelstapeln.

  Cloud NGFW unterstützt zwei Typen von Regelstapeln:

  - **Lokaler Regelstapel**: Lokale Kontoadministratoren können einen lokalen Regelstapel mit einer NGFW in ihrem AWS-Konto verknüpfen. Ein lokaler Regelstapel enthält lokale Regeln.
  - **Globaler Regelstapel**: Der AWS Firewall Manager-Administrator kann eine Firewall Manager Service (FMS)-Richtlinie erstellen und ihr einen globalen Regelstapel zuordnen. AWS Firewall Manager verwaltet den globalen Regelstapel in all diesen NGFWs in verschiedenen AWS-Konten einer AWS-Organisation. Ein globaler Regelstapel enthält Vor- und Nach-Regeln.

Cloud NGFW in Aktion

1. **Cloud NGFW-Dienst abonnieren**: Abonnieren Sie zunächst den Cloud NGFW für AWS-Dienst über den AWS Marketplace. Danach können Sie einen Cloud NGFW-Mandanten erstellen. Der abonnierende AWS IAM-Benutzer ist der Mandantenadministrator (TenantAdmin), der zusätzliche Benutzer einladen und Rollen zuweisen kann. Sie müssen Ihr AWS-Konto dem Cloud NGFW-Mandanten hinzufügen. Dadurch werden die erforderlichen Berechtigungen erteilt, die Cloud NGFW zum Speichern von Protokollen, Erstellen von NGFW-Endpunkten und Zugreifen auf die für die Entschlüsselung erforderlichen Schlüssel benötigt.

2. **Regelstapel erstellen**: Nach dem Hinzufügen von Benutzern und dem Zuweisen von Rollen in der Cloud NGFW-Mandantenkonsole können Administratoren für lokale Regelstapel lokale Regeln und Regelstapel erstellen.
3. **NGFWs erstellen**: Stellen Sie NGFW-Ressourcen bereit, um Ihre VPCs zu schützen. Ordnen Sie beim Erstellen Ihrer NGFWs die lokalen Regelstapel zu, die Sie zuvor erstellt haben.

   Sie haben zwei Optionen, Cloud NGFW-Endpunkte zu erstellen. Bei der ersten Option (dienstverwaltet) erstellen Sie ein dediziertes Subnetz in Ihrer VPC für jede gewünschte AWS-Verfügbarkeitszone und geben diese Subnetze dann beim Erstellen von Cloud NGFW-Ressourcen an. Bei dieser Option erstellt Cloud NGFW die NGFW-Endpunkte in Ihren Subnetzen. Alternativ geben Sie bei der zweiten Option (kundenverwaltet) die gewünschten AWS-Verfügbarkeitszonen an, in denen die NGFW-Ressource den Datenverkehr sichern soll. Bei dieser Option erstellt Cloud NGFW nur eine Cloud NGFW-Ressource, die sich als VPC-Endpunktressourcen in Ihrem AWS-Konto manifestiert. Sie sind dann dafür verantwortlich, ein dediziertes Subnetz in Ihrer VPC für jede gewünschte AWS-Verfügbarkeitszone zu erstellen und auch die VPC-Endpunkte zu erstellen.
4. **VPC-Routing-Tabellen aktualisieren**: Nach der Bereitstellung Ihrer Cloud NGFW-Ressource müssen Sie Datenverkehr zu Cloud NGFW für AWS leiten, indem Sie Ihre VPC-Routing-Tabellen aktualisieren. Der Datenverkehr wird dann zur Prüfung und Durchsetzung an die NGFW-Ressource geleitet.

Cloud NGFW-Anwendungsfälle

Cloud NGFW bietet Ihnen Tools und Funktionen zum Sichern von eingehendem Datenverkehr, ausgehendem Datenverkehr und Ost-West-Datenverkehr.

- **Eingehender** Datenverkehr bezieht sich auf jeglichen Datenverkehr, der von außerhalb Ihrer AWS-Region stammt und für Ressourcen innerhalb Ihrer Anwendungs-VPCs bestimmt ist, z. B. Server oder Load Balancer. Cloud NGFW kann verhindern, dass Malware und Sicherheitslücken im eingehenden Datenverkehr, der von AWS-Sicherheitsgruppen zugelassen wird, in Ihre VPC gelangen.
- **Ausgehender** Datenverkehr bezieht sich auf Datenverkehr, der von Ihrer Anwendungs-VPC stammt und für Ziele außerhalb der AWS-Region bestimmt ist. Cloud NGFW schützt ausgehende Datenverkehrsflüsse, indem sichergestellt wird, dass Ressourcen in Ihrer Anwendungs-VPC eine Verbindung zu zulässigen Diensten und zulässigen URLs herstellen, und gleichzeitig die Exfiltration sensibler Daten und Informationen verhindert wird.
- **Ost-West**-Datenverkehr ist Datenverkehr, der sich innerhalb einer AWS-Region bewegt. Insbesondere der Datenverkehr zwischen Quelle und Ziel, der in zwei verschiedenen Anwendungs-VPCs oder in zwei verschiedenen Subnetzen in denselben VPCs bereitgestellt wird. Cloud NGFW kann die Verbreitung von Malware in Ihrer AWS-Umgebung stoppen.

Erste Schritte im AWS Marketplace

Für den Einstieg in Cloud NGFW stehen Ihnen im AWS Marketplace mehrere Möglichkeiten zur Verfügung. Das wichtigste Entscheidungskriterium ist, ob Sie AWS Firewall Manager für die Arbeit mit Cloud NGFW verwenden möchten oder nicht.

- **Erste Schritte über AWS-Mitgliederkonten** – Sie können die Marketplace SaaS-Liste zu Palo Alto Networks Cloud NGFW für AWS über Ihr AWS-Mitgliedskonto abonnieren. Jedes Abonnement führt zum Erstellen eines einzigartigen Cloud NGFW-Mandanten.

  Anschließend können Sie mehrere andere AWS-Konten zum Cloud NGFW-Mandanten hinzufügen. Sie können Cloud NGFW-Ressourcen (auch NGFWs genannt) erstellen und sie VPCs in ihren AWS-Konten zuordnen. Sie können auch Sicherheitsrichtlinien für diese NGFW erstellen. Cloud NGFW überwacht die Nutzung des Cloud NGFW-Mandanten und sendet Messaufzeichnungen an den AWS Marketplace Metering Service. AWS verwendet diese Informationen zur Rechnungsstellung an den Kunden.

  Innerhalb Ihres AWS-Kontos fügen Sie dann einen NGFW-Endpunkt (auch als VPC-Endpunkt bezeichnet) für diese Ressource hinzu. Anschließend fügen Sie VPC-Routenregeln hinzu, um den gesamten Datenverkehr zur Überprüfung an den NGFW-Endpunkt weiterzuleiten. AWS leitet den an den NGFW-Endpunkt gesendeten Datenverkehr automatisch zur Überprüfung an die NGFW-Ressource weiter. An einen NGFW-Endpunkt gesendeter Datenverkehr wird immer an denselben NGFW-Endpunkt zurückgesendet – die NGFW verhält sich wie eine „Unebenheit im Kabel“.

  Sobald Sie mit dieser Methode begonnen haben, können Sie AWS Firewall Manager nicht mehr mit diesem Cloud NGFW-Mandanten verwenden.

- **Erste Schritte mit einem AWS Firewall Manager-Administratorkonto** – Wenn Sie derzeit AWS Firewall Manager verwenden, um Sicherheitsgruppen oder andere Netzwerksicherheitsfunktionen in Ihrer AWS-Organisation zu verwalten, können Sie denselben AWS Firewall Manager verwenden, um NGFWs in mehreren Konten und VPCs innerhalb einer AWS-Organisation bereitzustellen.

  Sie initiieren das AWS Marketplace-Abonnement für die Cloud NGFW-Liste über das angegebene AWS Firewall Manager-Administratorkonto der AWS-Organisation.

  Anschließend verwenden Sie den Richtlinien-Workflow des AWS Firewall Managers, um einen globalen Regelstapel zu erstellen und NGFWs schnell über mehrere AWS-Konten in einer AWS-Organisation hinweg bereitzustellen. Im Hintergrund koordiniert der Firewall Manager alle Komponenten. Hierzu gehört das Aufrufen der Cloud NGFW-APIs zum Erstellen der NGFWs und das Aufrufen der AWS-APIs zum Erstellen der NGFW-Endpunkte in den Kunden-VPCs.

  Weitere Einzelheiten zur Integration von AWS Firewall Manager in Cloud NGFW für AWS finden Sie im Blog und im Video zur Integration von AWS Firewall Manager.

  Wenn Sie mit dieser Methode begonnen haben, sollten Sie stets einen AWS Firewall Manager verwenden, um AWS-Konten zum Cloud NGFW-Mandanten hinzuzufügen.

Ihren Cloud NGFW-Mandanten bei einem Palo Alto Networks Supportkonto 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 ein registrierter Benutzer eines oder mehrerer vorhandener Palo Alto Networks Supportkonten sind, können Sie **Ihren Cloud NGFW-Mandanten bei der ersten Anmeldung bei einem dieser Konten registrieren**.

Möglicherweise haben Sie für das Abonnement von Cloud NGFW eine E-Mail-Adresse verwendet, die sich von der unterscheidet, die Sie für den Zugriff auf das Palo Alto Networks Supportkonto verwenden. 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**.

Ihren Cloud NGFW-Mandanten bei der ersten Anmeldung registrieren

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

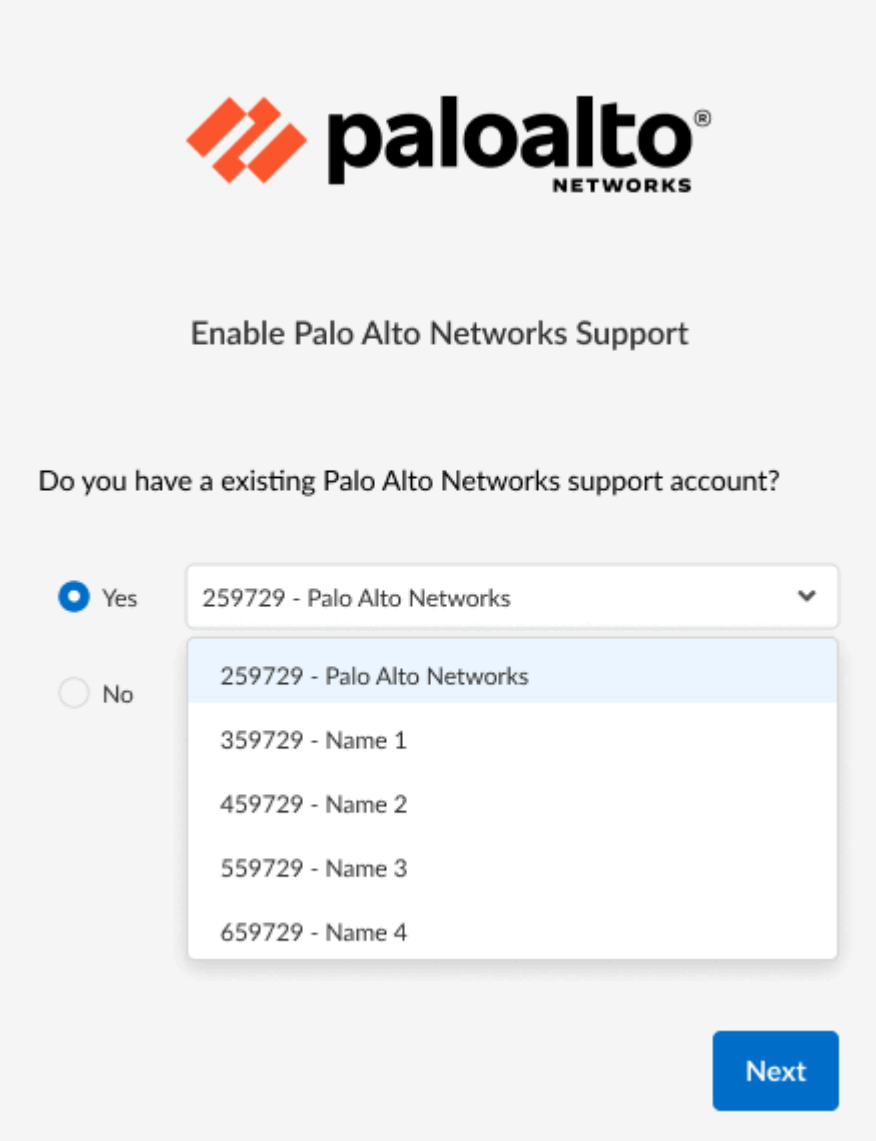
STEP 1 | Melden Sie sich bei der Cloud NGFW-Konsole an.

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. Siehe Ihren Cloud NGFW-Mandanten über das Customer Support Portal registrieren und*

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

STEP 4 | Klicken Sie auf **Next (Weiter)**.



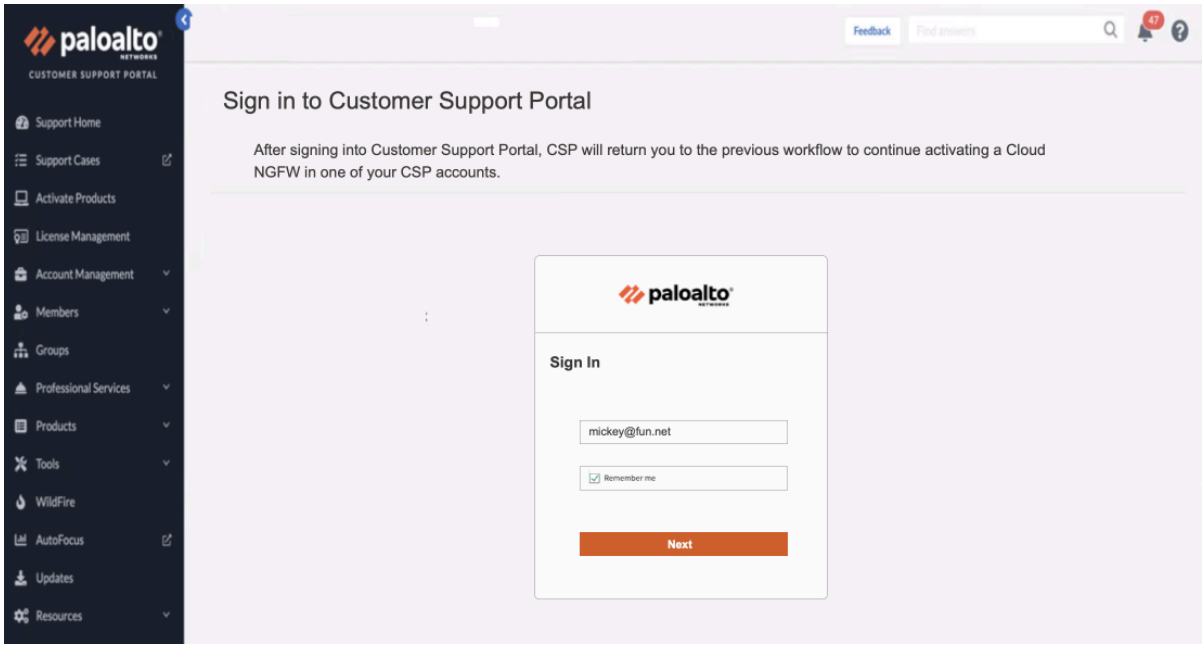
Wenn Sie sich bereits beim Customer Support Portal (CSP) registriert haben, werden in der Dropdown-Liste die vorhandenen Konten angezeigt. Wenn Sie jedoch ein neuer Benutzer sind und noch kein Konto haben, verwenden Sie die CSP-Seite, um ein Konto zu erstellen. Weitere Informationen finden Sie unter 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

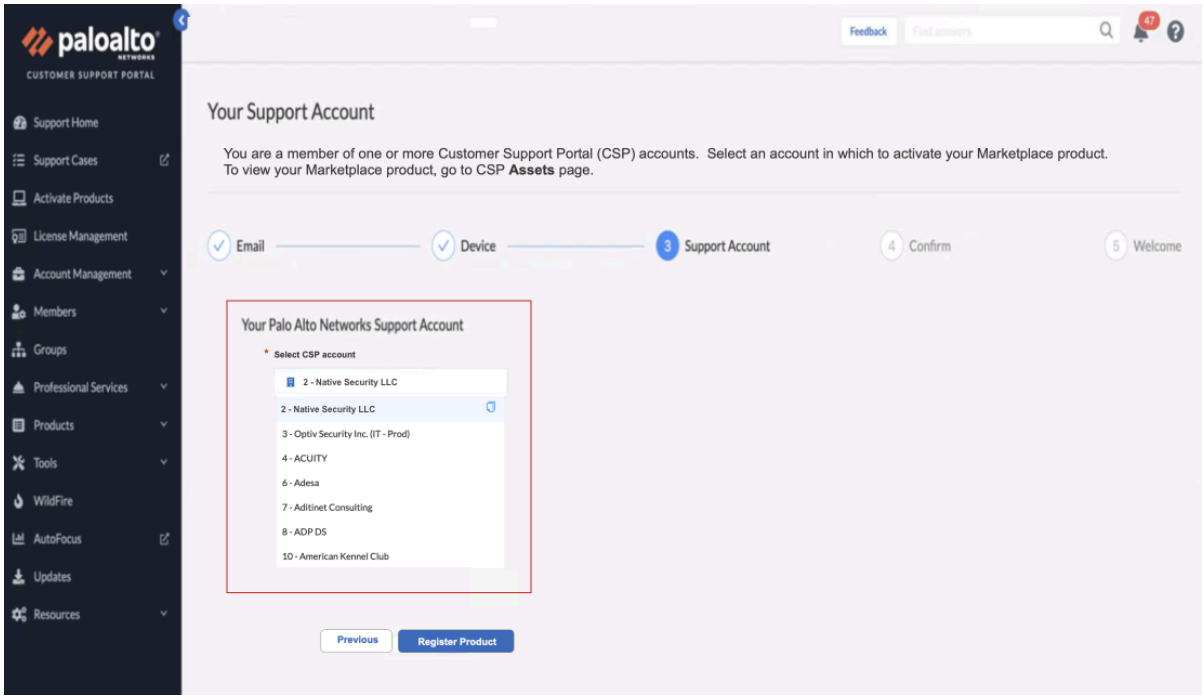
Sie können das Customer Support Portal verwenden, um Ihren Cloud NGFW-Mandanten zu registrieren.

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

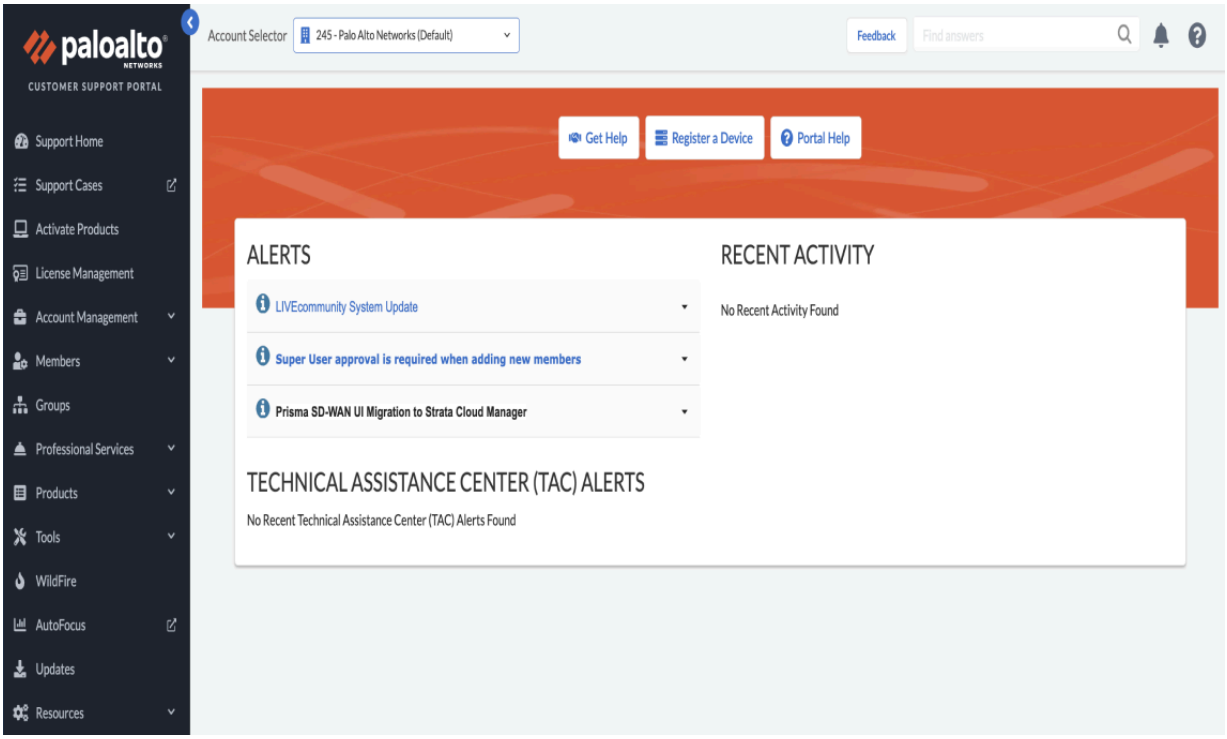
STEP 1 | Geben Sie im Customer Support Portal Ihre Anmeldeinformationen ein und klicken Sie dann auf **Next (Weiter)**.



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:



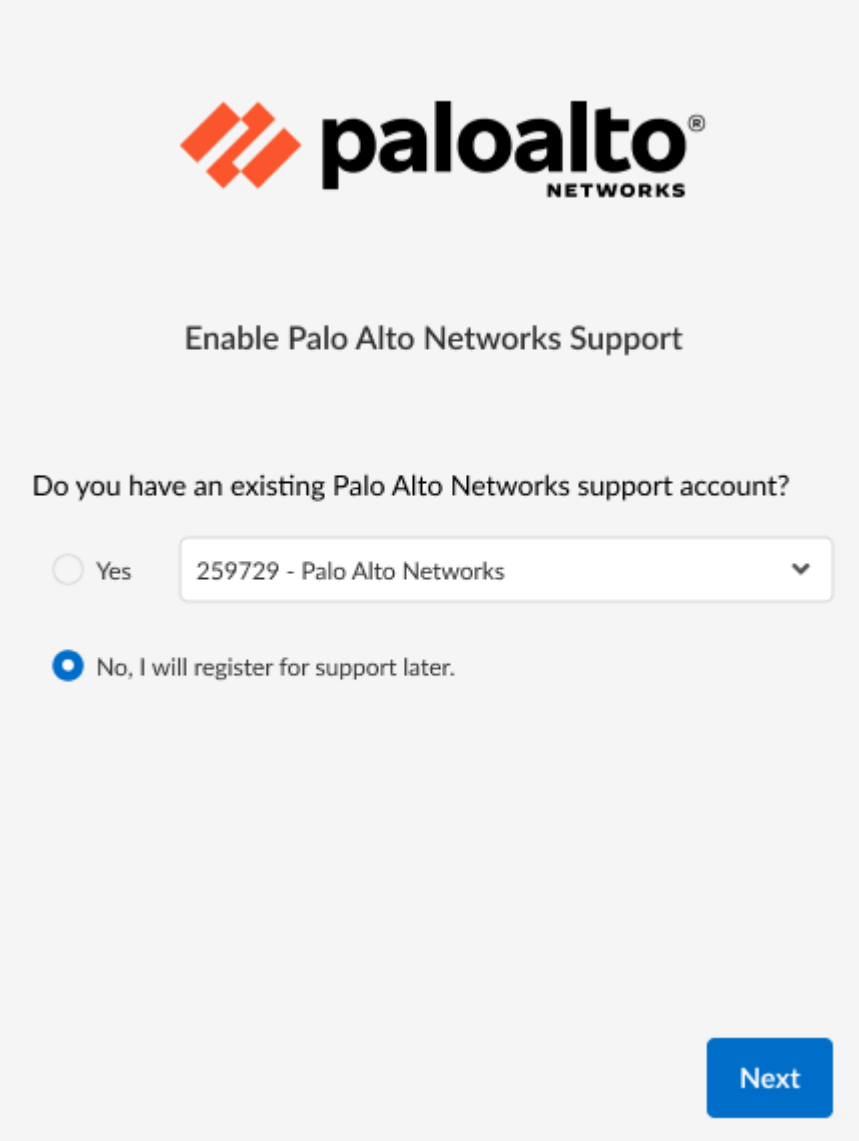
Ihren Cloud NGFW-Mandanten mithilfe der Cloud NGFW-Konsole im Customer Support Portal registrieren

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.

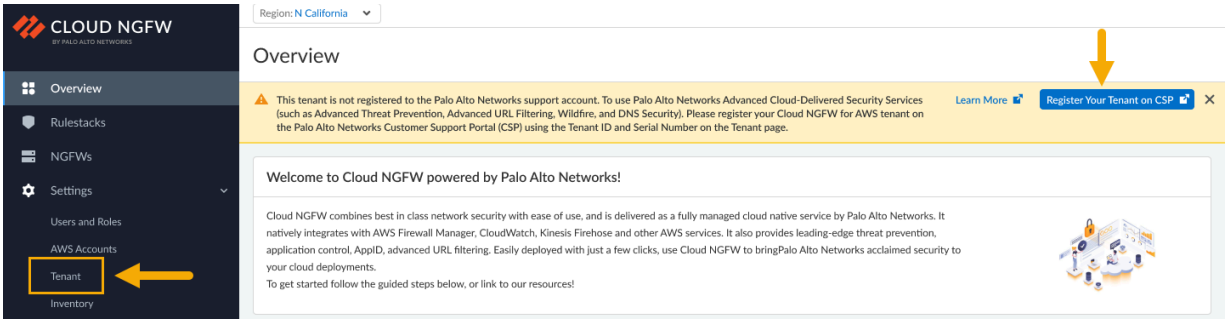
STEP 2 | Wählen Sie auf der Seite **Enable Palo Alto Networks Support (Palo Alto Networks Support aktivieren)** die Option **No (Nein)** aus.

STEP 3 | Klicken Sie auf **Next (Weiter)**.



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

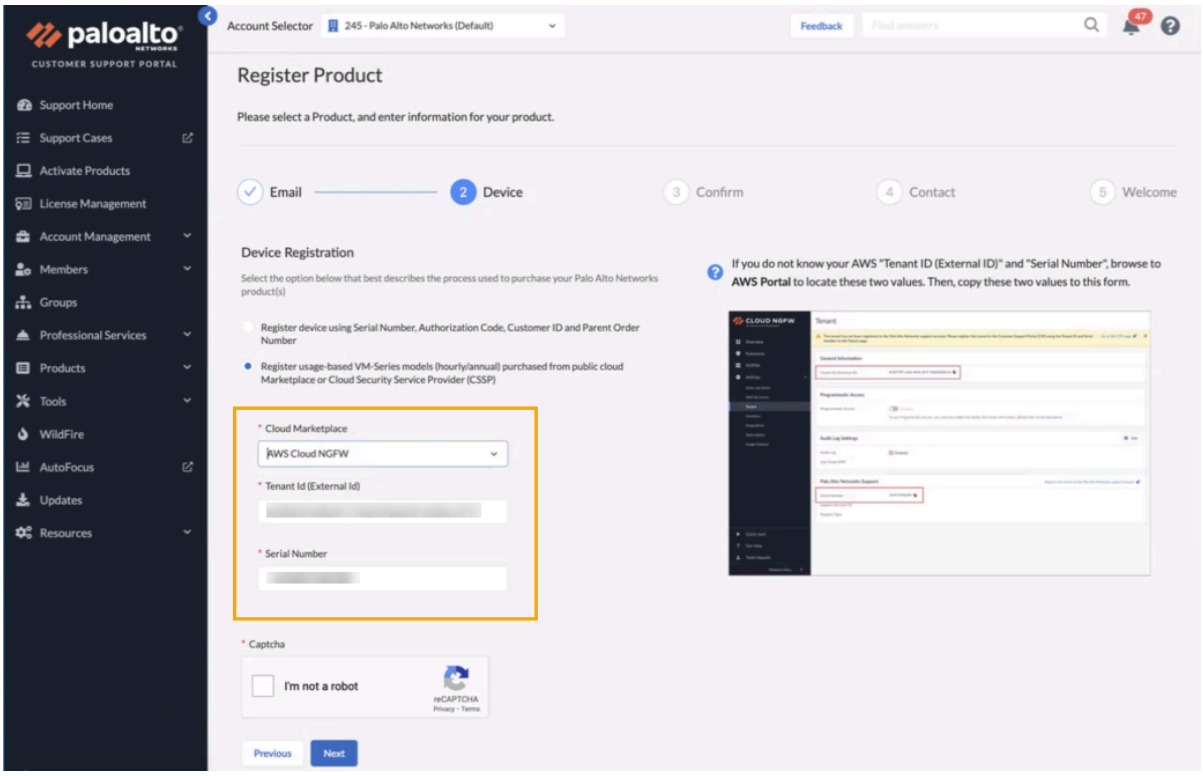
*Um Ihren Cloud NGFW-Mandanten einem Customer-Support-Portal-Konto zuzuordnen, benötigen Sie Ihre Geräteregistrierungsinformationen, einschließlich Ihrer **Mandanten-ID** und der **Seriennummer** für Ihre Cloud NGFW-Ressource. Sie finden diese Informationen auf der Seite **Tenant (Mandant)** in der Cloud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



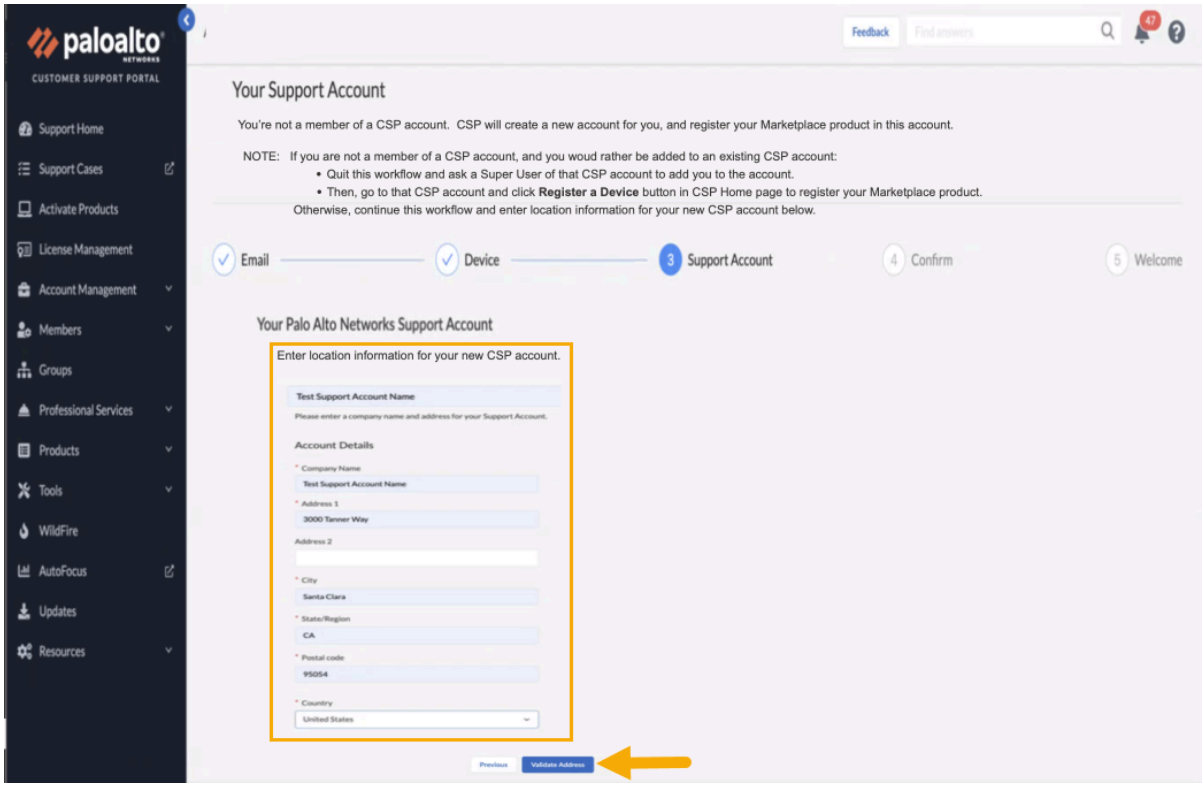
STEP 5 | Wählen Sie im Customer Support Portal auf der Seite **Register Product (Produkt registrieren)** im Dropdown-Menü die Option **AWS Cloud NGFW** für den **Cloud-Marketplace** aus. Geben Sie die **Mandanten-ID** und die **Seriennummer** ein und lösen Sie das Captcha.

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

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

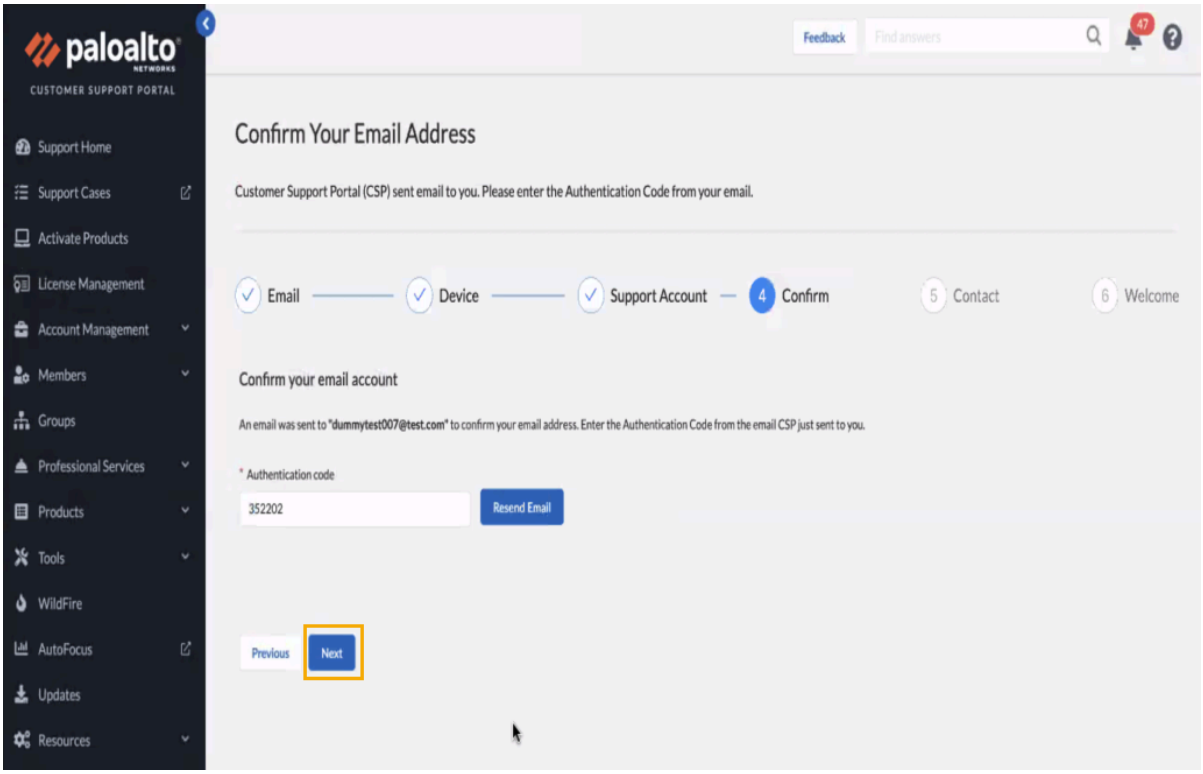


STEP 7 | Erstellen Sie Ihr Supportkonto. Geben Sie die **Kontodetails** ein und klicken Sie dann auf **Validate Address (Adresse überprüfen)**.



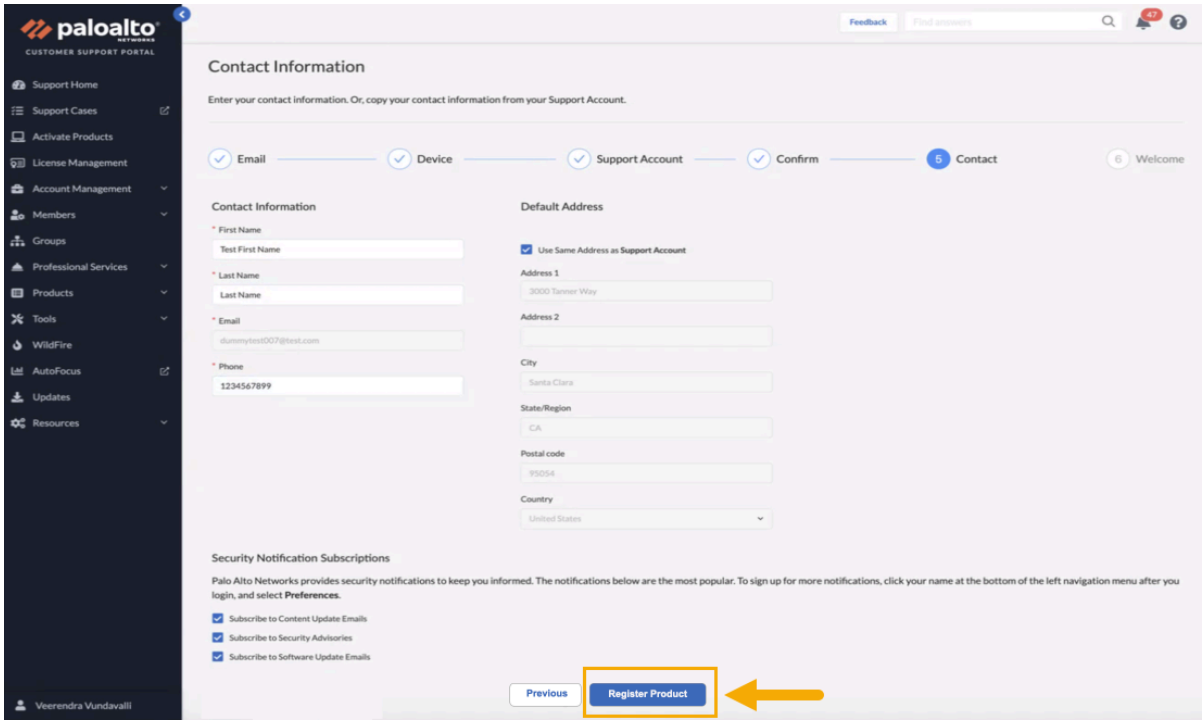
Möglicherweise werden Sie aufgefordert, Ihre Adresse für das neue Supportkonto zu bestätigen. Bestätigen Sie gegebenenfalls Ihre Adresse und klicken Sie auf **OK**, um eine Authentifizierungsanfrage an die angegebene E-Mail-Adresse zu senden.

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

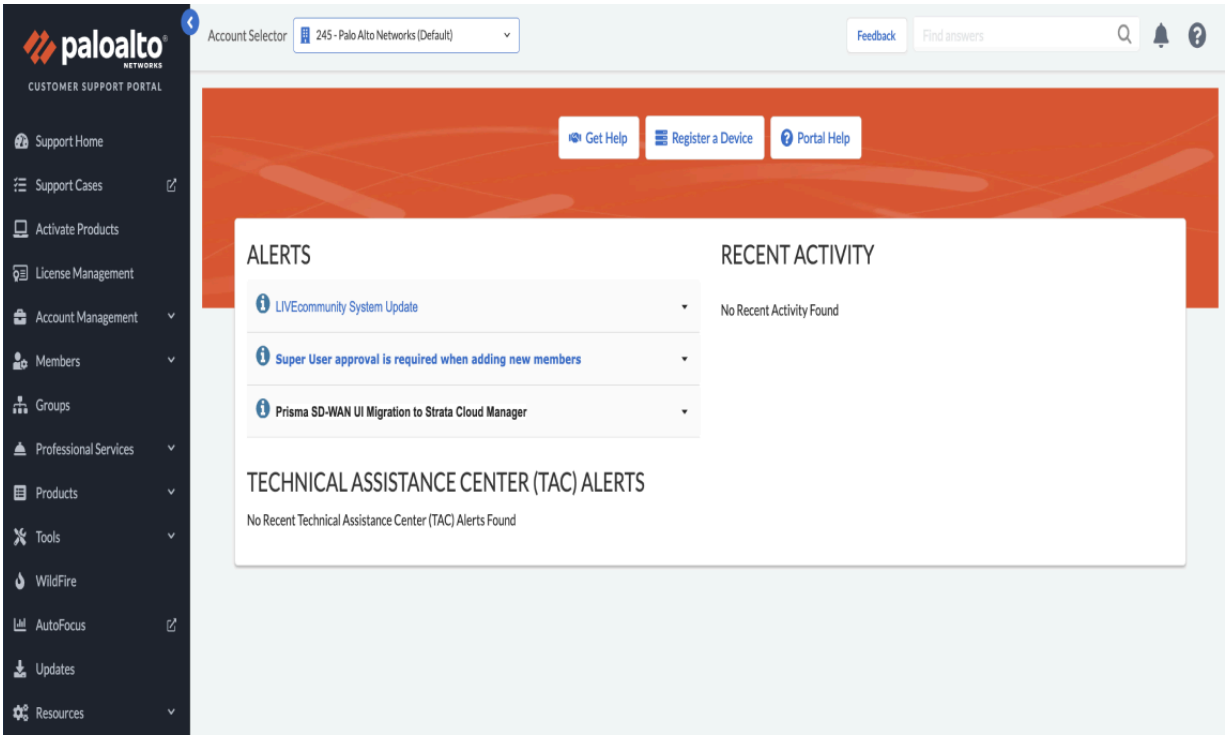


STEP 9 | Bestätigen Sie Ihre E-Mail-Adresse für Ihr Customer-Support-Portal-Konto und klicken Sie dann auf **Next (Weiter)**.

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

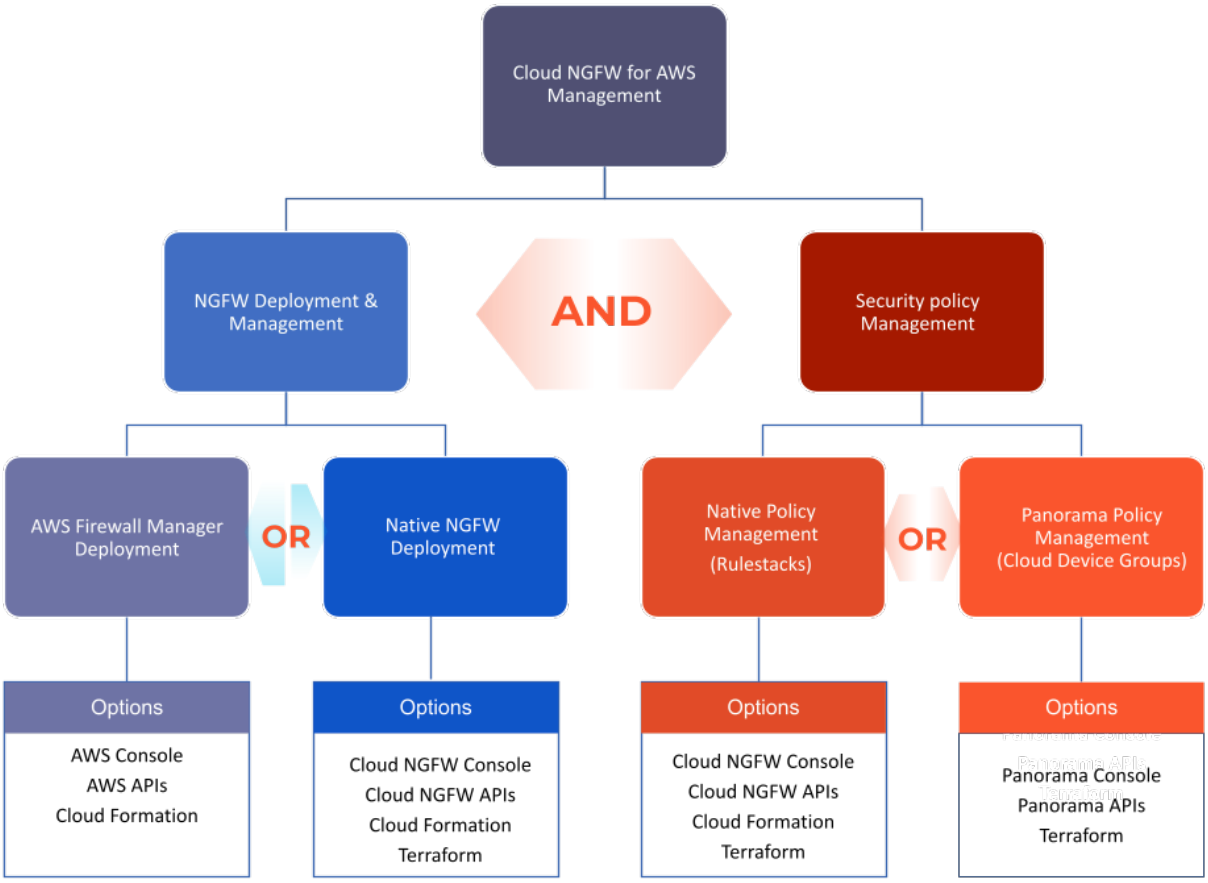


Sobald die Registrierung abgeschlossen ist, wird ein Bestätigungsfenster und anschließend die Seite des Customer Support Portals angezeigt:



Arbeiten mit Cloud NGFW für AWS

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



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 Sicherheitsrichtlinien 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 Sicherheitsrichtlinien 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 zugeordneten Objekte und Sicherheitsprofile.
- **Panorama-Richtlinienverwaltung** – Sie können Ihren Cloud NGFW-Mandanten mit einer Panorama-Appliance verknüpfen, um Richtlinien 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.

Weitere Informationen

- NGFW-Verwaltung und -Bereitstellung
- Sicherheitsfunktionen
- Unterstützte Regionen und Zonen in Cloud NGFW für AWS
- Unterstützte Bereitstellungen in Cloud NGFW für AWS

NGFW-Verwaltung und -Bereitstellung

Palo Alto Networks Cloud NGFW für AWS unterstützt die folgenden Verwaltungs- und Bereitstellungsfunktionen.

NGFW-Bereitstellung und -Verwaltung	Beschreibung	Native NGFW-Bereitstellung	Bereitstellung von AWS Firewall Manager
Tools	Ihnen stehen mehrere Konfigurationsoptionen zum Bereitstellen und Verwalten von Cloud NGFW-Ressourcen zur Verfügung.	• Cloud NGFW-Konsole • Cloud NGFW-APIs • CloudFormation • Terraform	• AWS-Konsole • AWS-APIs • CloudFormation
AWS-Regionen	Cloud NGFW für AWS ist ein regionaler AWS-Dienst. Die von Ihnen bereitgestellten Cloud NGFWs schützen Ihren VPC-Ein- und -Ausgangsdatenverkehr in dieser AWS-Region.	• 21	• 16
Bereitstellungsarchitekturen	Mit Cloud NGFW für AWS sind mehrere Bereitstellungsmodelle verfügbar. Das richtige Modell hängt vom Anwendungsfall und den Anforderungen ab.	• Zentralisiert • Verteilt • Kombiniert (Multi-VPC-NGFW-Ressource)	• Zentralisiertes Modell • Verteiltes Modell

Sicherheitsfunktionen

Die Palo Alto Networks Cloud NGFW für AWS unterstützt die folgenden Sicherheitsfunktionen.

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlinien	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Tools	Es stehen mehrere Konfigurationsoptionen zum Erstellen von Richtlinien für Ihre Cloud NGFWs zur Verfügung.	• Cloud NGFW-Konsole • Cloud NGFW-APIs • CloudFormation • Terraform	• Panorama-Konsole • Panorama-APIs • Terraform
Protokolltypen	Cloud NGFW generiert mit Zeitstempeln versehene	• Verkehrs-Protokolle • Bedrohungsprotokolle • Entschlüsselungsprotokolle	• Verkehrs-Protokolle • Bedrohungsprotokolle

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlinien	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	Protokolle, die einen Prüfpfad für von der Firewall überwachte Netzwerkverkehrsereignisse darstellen. 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 Cloud NGFW ein Bedrohungsprotokoll, um Datenverkehr aufzuzeichnen, der mit einer Spyware-, Sicherheitslücken- oder Virensignatur übereinstimmt.	• Auditierungslog	• URL-Filterungs-Protokolle • Entschlüsselungsprotokolle
Protokollziele	Cloud NGFW kann die generierten Protokolle an AWS-Ziele und Cortex Data Lake übermitteln.	• Amazon Simple Storage Service(S3)-Bucket • Amazon CloudWatch-Protokollgruppe • Amazon Kinesis Data Firehose	• Amazon Simple Storage Service(S3)-Bucket • Amazon CloudWatch-Protokollgruppe • Amazon Kinesis Data Firehose • Cortex Data Lake • Protokolle von Cortex Data Lake an

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlinien	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
			einen Syslog-Server weiterleiten • Protokolle von Cortex Data Lake an einen HTTPS-Server weiterleiten
Protokollvisualisierung und -analyse	Überprüfen Sie die Cloud NGFW-Protokolle, um zahlreiche Informationen zu Ihrem VPC-Datenverkehr zu verifizieren. Einige Beispiele für diese Informationen sind Quelle, Ziel, URLs, Port-Protokolle, App-ID, Bedrohungen, Länder, URLs usw.	• Protokolle in Amazon Destinations erkunden	• Protokolle in Amazon Destinations erkunden • Protokolle in Cortex Data Lake erkunden • Protokolle in Panorama überwachen • Application Command Center (ACC) in Panorama überwachen
Berichte	Erstellen Sie vordefinierte und benutzerdefinierte Berichte zu Anwendungen, Bedrohungen und URL-Aktivitäten Ihres VPC-Datenverkehrs.	-	• Geplante und benutzerdefinierte Berichte
Paketerfassung	Palo Alto Networks Firewall zum Durchführen einer benutzerdefinierten Paketerfassung oder einer Bedrohungspaketerfassung.	-	-

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Sicherheitsrichtlinie	Die Sicherheitsrichtlinie schützt Ihren VPC-Datenverkehr vor Bedrohungen und Störungen. Individuelle Sicherheitsregeln bestimmen, ob eine VPC-Datenverkehrssitzung basierend auf Datenverkehrsattributen wie Quell- und Ziel-Sicherheitszone, Quell- und Ziel-IP-Adresse, Anwendung, Benutzer und Dienst abgelehnt oder zugelassen wird.	• Lokaler Regelstapel • Globaler Regelstapel	• Sicherheitsrichtlinien • Vor-Regeln • Nach-Regeln • Standardregeln
Adresse	Sie können ein Adressobjekt so angeben, dass es IPv4-Adressen, einen FQDN oder eine Platzhalteradresse (IPv4-Adresse gefolgt von einem Schrägstrich und einer Platzhaltermaske) enthält.	• Präfixlisten • FQDN-Liste	• IPv4-Netzmaske • IPv4-Bereiche • IPv4-Platzhaltermaske • FQDNs
Adressgruppen	Sie können bestimmte Quell- oder Zieladressen gruppieren, für die die gleiche Richtliniendurchsetzung erforderlich ist.	-	• Adressgruppen
Regionen	Sie können Datenverkehr von (oder zu) IP-Adressen basierend auf ihrem geografischen Standort,	• Länder	• Vordefinierte Regionen • Benutzerdefinierte Regionen

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	beispielsweise einem Land, zulassen oder blockieren. Die Region ist als Option verfügbar, wenn Sie die Quelle und das Ziel für Ihre Richtlinien angeben. Sie können aus einer Standardliste von Ländern wählen oder eine benutzerdefinierte Region/ Geolokalisierung zusammen mit den zugeordneten IP-Adressen angeben.		
Dienst (Port und Protokoll)	Sie können die Nutzung von VPC-Datenverkehrssitzungen für bestimmte Ports in Ihrem Netzwerk präzise steuern (mit anderen Worten, Sie können den Standardport für die Anwendung definieren). Cloud NGFW umfasst zwei vordefinierte Dienste – service-http und service-https –, die die TCP-Ports 80 und 8080 für HTTP und den TCP-Port 443 für HTTPS verwenden. Sie können jedoch jeden benutzerdefinierten Dienst auf einem beliebigen TCP/ UDP-Port Ihrer Wahl erstellen.	• Port und Protokoll	• Dienste
Dienstgruppen	Sie können Dienste mit denselben	-	• Dienstgruppen

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	Sicherheitseinstellungen in Dienstgruppen zusammenfassen, um die Anzahl der Regeln in der Sicherheitsrichtlinie zu reduzieren.		
Externe dynamische Liste	Sie können Ihren VPC-Datenverkehr mithilfe einer dynamischen Liste von IP-Adressen, Domänen oder URLs präzise steuern. Gespeichert in einer Datei, die auf einem externen Webserver gehostet wird. Palo Alto Networks bietet außerdem integrierte EDLs (Bulletproof, High-Risk, Known Malicious und Tor Exit-IP-Adresse). Darüber hinaus umfasst das Angebot von Palo Alto Networks auch einen kostenlosen EDL-Hosting-Dienst, der die stets dynamische Liste der IP-Adressen für Microsoft 365, Azure, Amazon Web Services (AWS) und Google Cloud Platform (GCP) verwaltet. Sie können diese EDLs verwenden, um Ihren VPC-Ein- und -Ausgangsverkehr zu steuern.	• Intelligenz-Feeds • Integrierte Feeds • EDL-Hosting-Dienst-Feeds	• Externe dynamische Listen • Integrierte EDL • EDL-Hosting-Dienst-Listen
Anwendungen	Sie können Ihren VPC-Datenverkehr mithilfe des App-ID™-	• APP-IDs	• APP-IDs

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	Verkehrsklassifizierungssystems von Palo Alto Networks präzise steuern. Dieses System basiert auf Anwendungssignaturen, um die Anwendungen in Ihrem Netzwerk genau zu identifizieren.		• Benutzerdefinierte Anwendungssignaturen
Anwendungsgruppe	Sie können eine Reihe von App-IDs gruppieren, für die die gleiche Richtliniendurchsetzung erforderlich ist.	-	• Anwendungsgruppen
Anwendungsfilter	Sie können Ihren VPC-Datenverkehr präzise steuern, indem Sie einen Anwendungsfilter definieren, der aktuelle App-IDs und alle zukünftigen App-IDs gruppiert, die bestimmten Attributen entsprechen. Beispielsweise können Sie einen Anwendungsfilter nach einem oder mehreren Attributen erstellen – Kategorie, Unterkategorie, Technologie, Risiko, Merkmale. Wenn von nun an aufgrund einer Inhaltsaktualisierung eine neue App-ID in Cloud NGFW eingeführt wird, werden alle neuen Anwendungen, die den Filterkriterien	-	• Anwendungsfilter

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	entsprechen, automatisch zu Ihrem Satz hinzugefügt.		
Anwendungsüberschreibung	Sie können Cloud NGFW so konfigurieren, dass die normale Anwendungskennung (App-ID) von bestimmtem Datenverkehr, der durch die Firewall läuft, überschrieben wird. Sobald die Anwendungsüberschreibungsrichtlinie in Kraft tritt, werden alle weiteren App-ID-Überprüfungen des Datenverkehrs gestoppt und die Sitzung wird mit den von Ihnen bereitgestellten benutzerdefinierten Anwendungssignaturen identifiziert.	-	• Anwendungsüberschreibung
Tags	Mit Tags können Sie Objekte anhand von Schlüsselwörtern oder Ausdrücken gruppieren. Sie können Tags auf Adressobjekte, Adressgruppen (statisch und dynamisch), Anwendungen, Zonen, Dienste, Dienstgruppen und Richtlinienregeln anwenden.	-	• Tags
Dynamische Benutzergruppe	Ermöglicht Ihnen, eine Liste von Benutzern aus der	-	-

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	lokalen Datenbank, einer externen Datenbank oder gemäß Übereinstimmungskriterien zu erstellen und sie zu gruppieren.		
Geräte	Diese Seite wird auch als Gerätewörterbuch bezeichnet und enthält Metadaten für Geräteobjekte.	-	-

Zertifikate und Entschlüsselung	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Zertifikatverwaltung	Cloud NGFW verwendet Zertifikate, um auf einen intelligenten Feed zuzugreifen und die ein- und ausgehende Entschlüsselung zu ermöglichen. Jedes Zertifikat enthält einen kryptografischen Schlüssel zum Verschlüsseln von Klartext bzw. Entschlüsseln von verschlüsseltem Text. Jedes Zertifikat enthält außerdem eine digitale Signatur zur Authentifizierung der Identität des Ausstellers.	• TLS/SSL-Zertifikate im AWS Secrets Manager	• Selbstsignierte CA-Stammzertifikate • Importieren eines Zertifikats und eines privaten Schlüssels • TLS/SSL-Zertifikate im AWS Secrets Manager • Generieren von Zertifikaten • Abrufen eines Zertifikats von einer externen Zertifizierungsstelle (CA) • Online-Certificate-Status-Protocol(OCSP)-Responder • Vertrauenswürdige Standardzertifizierungsstellen • Zertifikatprofil

Zertifikate und Entschlüsselung	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Entschlüsselung	Cloud NGFW kann Ihren VPC-Ein- und -Ausgangsdatenverkehr auf der Grundlage einer richtlinienbasierten Entscheidung entschlüsseln, prüfen und erneut verschlüsseln. Sie können präzise steuern, welcher VPC-Datenverkehr entschlüsselt wird und welcher nicht, und welche Art der SSL-Entschlüsselung Sie für den angegebenen Datenverkehr durchführen möchten. Um die Entschlüsselung zu aktivieren, richten Sie die erforderlichen Zertifikate ein, die benötigt werden, um als vertrauenswürdige dritte Partei für eine Sitzung zu fungieren.	• Ausgehende SSL-Entschlüsselung • SSL-Eingangsinspektion	• Entschlüsselungsrichtlinie • Entschlüsselungsprofil • SSL-Forward-Proxy (ausgehende Entschlüsselung) • SSL-Eingangsinspektion • SSH-Proxy • Überprüfung des Serverzertifikats • Ausschluss der Entschlüsselung • Vorübergehende Deaktivierung der SSL-Entschlüsselung

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Schutz vor IPS-Sicherheitslücken	Der Sicherheitslückenschutz schützt vor eingehenden Bedrohungen, bei denen ein Angreifer versucht, eine Sicherheitslücke im System auszunutzen,	• Best Practices	• Standardprofil • Strenges Profil • Benutzerdefiniertes Profil (Bedrohungsausnahmen) • Benutzerdefinierte Signaturen für Sicherheitslücken

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	um in Ihr Netzwerk einzudringen. Die Sicherheitslücken im System können in Form von Pufferüberläufen, der Ausführung illegalen Codes usw. auftreten.		• Signaturen für Snort/Suricata
Anti Spyware	Anti-Spyware erkennt und blockiert ausgehende Bedrohungen, insbesondere Command-and-Control(C2)-Aktivitäten, die (nach einem Cyberangriff) durch mit Malware infizierte Workloads in Ihrer AWS VPC initiiert werden. Sie können auch benutzerdefinierte Muster für reguläre Ausdrücke definieren, um die private Telefonkommunikation mit Spyware zu bestimmen.	• Best Practices	• Standardprofil • Strenges Profil • Benutzerdefiniertes Profil (Bedrohungsausnahmen) • Benutzerdefinierte Signaturen für Spyware • Signaturen für Snort/Suricata
Dateiblockade	Durch Dateiblockaden können Sie Dateitypen in Ihrem VPC-Datenverkehr in eine bestimmte Richtung (eingehend/ausgehend/beides) präzise steuern. Sie können Dateien proaktiv blockieren, von denen bekannt ist, dass sie eine Bedrohung darstellen oder für deren Hoch- und Herunterladen es	• Best Practices und Anpassungen	• Basisprofil • Strenges Profil • Benutzerdefiniertes Profil

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	keinen tatsächlichen Anwendungsfall gibt.		
Antivirus	Antivirus erkennt und schützt vor Malware, die in komprimierten Dateien, ausführbaren Dateien, PDF-Dateien sowie HTML- und JavaScript-Viren in Ihrem VPC-Datenverkehr versteckt ist	• Best Practices	• # Standardprofil • Benutzerdefiniertes Profil (Bedrohungsausnahmen)
WildFire-Analyse	Cloud NGFW erkennt Dateien und ausführbare Dateien in Ihrem VPC-Datenverkehr, leitet sie zur Analyse an den WildFire™-Cloud-Dienst weiter und führt für bestimmte Dateien auch Inline-ML-Analysen durch. Wenn in den Dateien eine Bedrohung erkannt wird, erstellt WildFire Schutzmaßnahmen zum Blockieren der Malware und verteilt den Schutz vor dieser Bedrohung in weniger als fünf Minuten weltweit.	-	-
URL Filtering	Die URL-Filterung analysiert den VPC-Datenverkehr und steuert die URLs, auf die Ihre VPC-Workloads zugreifen (sowohl im Klartext- als auch im verschlüsselten	• Zugriffskontrolle für von Palo Alto Networks verwaltete URL-Kategorien • Benutzerdefinierte URL-Kategorien	• Zugriffskontrolle für von Palo Alto Networks verwaltete URL-Kategorien und benutzerdefinierte URL-Kategorien

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	Datenverkehr), indem sie eine Inline-Analyse durchführt und sie mit den von Palo Alto Networks verwalteten URL-Kategorien oder den von Ihnen bereitgestellten benutzerdefinierten Kategorien vergleicht.		• Cloud-Inline-Kategorisierung
DNS Security	DNS Security schützt von Ihren VPCs ausgehende DNS-Anfragen vor Bedrohungen wie DNS-Tunneling, Domain-Generation-Algorithm(DGA)-Erkennung, Malware-Domänen usw.	-	• Ihre Bereitstellung vor DNS-basierten Bedrohungen absichern
Datenfilterung und Enterprise DLP	Bei der Datenfilterung werden vertrauliche Informationen in Ihrem VPC-Datenverkehr erkannt – etwa Kreditkarten- oder Sozialversicherungsnummern oder interne Unternehmensdokumente – und es wird verhindert, dass diese Daten Ihre AWS-Umgebung verlassen. Mit Enterprise DLP profitieren Sie von der erweiterten Datenfilterung Ihres VPC-Datenverkehrs mit einer vordefinierten Liste von Datenmustern mit cloudbasierter Analyse.	-	• Vordefinierte Muster, reguläre Ausdrücke und Dateieigenschaften Enterprise DLP wird derzeit NICHT unterstützt

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Sicherheitsprofilgruppen	Eine Sicherheitsprofilgruppe ist ein Satz von Sicherheitsprofilen, die als Einheit behandelt und dann einfach zu Sicherheitsrichtlinien hinzugefügt werden können.	-	• Sicherheitsprofilgruppen

Sicherheitszonen und Schutz	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
Sicherheitszonen	Sicherheitszonen sind eine logische Möglichkeit, Schnittstellen auf der Firewall und Cloud NGFW-Endpunkte zu gruppieren, um den VPC-Datenverkehr zu steuern und zu protokollieren.	-	-
Zonenschutz	Der Zonenschutz verteidigt Netzwerksicherheitszonen vor Flood-Angriffen, Reconnaissance-Versuchen und paketbasierten Angriffen.	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
XFF	Der Datenverkehr zu Ihren VPC-Workloads hat möglicherweise mehr als einen Proxyserver (wie CDN oder ALB) passiert, bevor er die Cloud NGFW erreicht. Wenn ein XFF-Header vorhanden ist, hängen diese Proxys seine IP-Adresse an oder fügen den XFF-Header mit seiner IP-Adresse hinzu. Daher kann der XFF-Anforderungsheader mehrere durch Kommas getrennte IP-Adressen enthalten. Cloud NGFW verwendet das HTTP-Headerfeld „X-Forwarded-For“ (XFF), um die ursprüngliche Client-IP-Adresse zu identifizieren. Die NGFW verwendet immer die zuletzt hinzugefügte Adresse im XFF-Header, um Richtlinien durchzusetzen.	• XFF-Header-Unterstützung in Richtlinien • XFF-Werte in Protokollen anzeigen	• XFF-Werte in der Richtlinie verwenden • XFF-Werte in Protokollen anzeigen • XFF-Werte in Berichten anzeigen
NAT	Die Firewalls von Palo Alto Networks können Ziel-NAT für Ihren eingehenden VPC-Datenverkehr und Quell-NAT für Ihren ausgehenden VPC-Datenverkehr erzwingen.	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
DNS-Proxy	Wenn Sie Cloud NGFW als DNS-Proxy konfigurieren, übernimmt der Dienst die Aufgabe eines Vermittlers zwischen Clients und Servern und eines DNS-Servers, indem er Abfragen aus seinem DNS-Cache auflöst oder Abfragen an andere DNS-Server weiterleitet. Auf dieser Seite können Sie die Einstellungen konfigurieren, die bestimmen, wie die Firewall als DNS-Proxy dient.	-	-
Schnittstellenverwaltung	Mit den Firewalls von Palo Alto Networks können Sie VLANs, virtuelle Leitungen, Link Layer Discovery Protocol (LLDP) und Bidirectional Forwarding Detection (BFD) an ihren Schnittstellen konfigurieren.	-	-
QoS	Mit den Firewalls von Palo Alto Networks können Sie Datenverkehr angeben, der eine bevorzugte Behandlung oder Bandbreitenbeschränkung erfordert. Mithilfe von QoS-Regeln können Sie Anwendungen und Datenverkehr mit hoher	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	Priorität zuverlässig bei begrenzter Netzwerkkapazität ausführen.		
Routenverwaltung	Mit den Firewalls von Palo Alto Networks können Sie statisches Routing und Routing-Protokolle (BGP, BFD, OSPF, OSPFv3, Multicast, RIPv2 und Filter) konfigurieren.	-	-
IPSec-Tunnelverwaltung	Firewalls von Palo Alto Networks beenden IPSec-Tunnel und prüfen den getunnelten Datenverkehr	-	-
GlobalProtect-Verwaltung	Die Firewalls von Palo Alto Networks sichern mobile Arbeitskräfte ab, indem sie Algorithmen zur Authentifizierung und Verschlüsselung in VPN-Tunneln zwischen einem GlobalProtect-Gateway-Modul und dem Client festlegen.	-	-
GRE-Tunnelverwaltung	Die Firewalls von Palo Alto Networks beenden Generic-Routing-Encapsulation(GRE)-Tunnel und überprüfen den getunnelten Datenverkehr.	-	-
SD-WAN-Linkverwaltung	Die Firewalls von Palo Alto Networks binden mehrere WAN-Verbindungen (ADSL/	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	DSL, Kabelmodem, Ethernet, Glasfaser, LTE/3G/4G/5G, MPLS, Mikrowelle/ Radio, Satellit, WLAN) an eine virtuelle Schnittstelle und unterstützen eine dynamische, intelligente Pfadauswahl basierend auf Anwendungen und Diensten sowie den Bedingungen der Verbindungen, die jede Anwendung oder jeder Dienst nutzen darf.		
Richtlinienbasierte Weiterleitung	Die auf Richtlinien basierenden Weiterleitungsregeln der Firewalls von Palo Alto Networks ermöglichen es dem Datenverkehr, aus Sicherheits- oder Leistungsgründen einen alternativen Pfad zu nehmen. Angenommen, Ihr Unternehmen verfügt zwischen der Firmenzentrale und der Zweigstelle über zwei Verbindungen: eine günstigere Internetverbindung und eine teurere Standleitung. Zur Erhöhung der Sicherheit können Sie PBF verwenden, um Anwendungen mit unverschlüsseltem Datenverkehr (z. B. FTP-Datenverkehr)	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltung (Regelstapel)	Panorama-Richtlinienverwaltung (Cloud-Gerätegruppen)
	über die private Standleitung und den gesamten übrigen Datenverkehr über die Internetverbindung zu senden. Oder Sie können aus Leistungsgründen festlegen, dass geschäftskritische Anwendungen über die Standleitung geroutet werden, während der gesamte übrige Datenverkehr, z. B. das Surfen im Internet, über die günstigere Verbindung gesendet wird.		

Unterstützte Regionen und Zonen in Cloud NGFW für AWS

Die Palo Alto Networks Cloud NGFW für AWS unterstützt die folgenden Regionen.

Regionsname	Regionscode	Zonen-ID	AWS Firewall Manager	AWS CloudFormation Registry
Westen der USA (Nordkalifornien)	us-west-1	usw1-az1 usw1-az3		
Westen der USA (Oregon)	us-west-2	usw2-az1 usw2-az2 usw2-az3		
Osten der USA (Nord-Virginia)	us-east-1	use1-az1 use1-az2 use1-az4 use1-az5		

Regionsname	Regionscode	Zonen-ID	AWS Firewall Manager	AWS CloudFormation Registry
		use1-az6		
Osten der USA (Ohio)	us-east-2	use2-az1 use2-az2 use2-az3		
Kanada (zentral)	ca-central-1	cac1-az1 cac1-az2 cac1-az4		
Europa (Irland)	eu-west-1	euw1-az1 euw1-az2 euw1-az3		
Europa (London)	eu-west-2	euw2-az1 euw2-az2 euw2-az3		
Europa (Paris)	eu-west-3	euw3-az1 euw3-az2 euw3-az3		
Europa (Frankfurt)	eu-central-1	euc1-az1 euc1-az2 euc1-az3		
Europa (Stockholm)	eu-north-1	eun1-az1 eun1-az2 eun1-az3		
Europa (Mailand)	eu-south-1	eus1-az1 eus1-az2 eus1-az3	-	-
Asien-Pazifik (Osaka)	ap-northeast-3	apse1-az1 apse1-az2		

Regionsname	Regionscode	Zonen-ID	AWS Firewall Manager	AWS CloudFormation Registry
		apse1-az3		
Asien-Pazifik (Singapur)	ap-southeast-1	apse1-az1 apse1-az2 apse1-az3		
Asien-Pazifik (Sydney)	ap-southeast-2	apse2-az1 apse2-az2 apse2-az3		
Asien-Pazifik (Tokio)	ap-northeast-1	apne1-az1 apne1-az2 apne1-az4		
Asien-Pazifik (Seoul)	ap-northeast-2	apne2-az1 apne2-az2 apne2-az3		
Asien-Pazifik (Osaka)	ap-northeast-3	apne3-az1 apne3-az2 apne3-az3	-	-
Asien-Pazifik (Mumbai)	ap-south-1	aps1-az1 aps1-az2 aps1-az3		
Asien-Pazifik (Hongkong)	ap-east-1	ape1-az1 ape1-az2 ape1-az3	-	-
Südamerika (São Paulo)	sa-east-1	sae1-az1 sae1-az2 sae1-az3		
Naher Osten (Bahrain)	me-south-1	mes-az1 mes-az2	-	-

Regionsname	Regionscode	Zonen-ID	AWS Firewall Manager	AWS CloudFormation Registry
		mes-az3		
Afrika (Kapstadt)	af-south-1	afs-az1 afs-az2 afs-az3	-	-

Unterstützte Bereitstellungen in Cloud NGFW für AWS

Sie können Cloud NGFW in einem zentralisierten Modell hinter einem Transit Gateway (TGW) mit einer Cloud NGFW-Ressource bereitstellen, die in einer dedizierten Sicherheits-VPC bereitgestellt wird, oder in einem verteilten Modell, bei dem jeder VPC eine Cloud NGFW-Ressource zugeordnet ist.

Zentralisierte Bereitstellung

Bei einer zentralisierten Bereitstellung bietet eine dedizierte Sicherheits-VPC einen zentralen Ansatz zur Verwaltung der Zugriffskontrolle und Bedrohungsabwehr des eingehenden, ausgehenden und Ost-West-Datenverkehrs Ihrer VPCs. Sie müssen die Sicherheits-VPC und Subnetze angeben, wenn Sie Cloud NGFW konfigurieren. Die NGFW-Endpunkte werden in der angegebenen VPC und den Subnetzen erstellt und bereitgestellt. Anschließend müssen Sie Routingregeln auf den Anwendungs-VPCs und dem TGW konfigurieren, um den Datenverkehr zur Überprüfung an die Sicherheits-VPC umzuleiten, sowie Routingregeln für den Rückdatenverkehr.

Weitere Informationen und Beispiele für zentralisierte Bereitstellungen finden Sie unter Zentralisierte Bereitstellungen in Cloud NGFW für AWS.

Verteilte Bereitstellung

Das verteilte Bereitstellungsmodell ermöglicht die Verteilung von Cloud NGFWs auf mehrere VPCs, während die zentrale Sicherheitskontrolle beibehalten wird. Bei diesem Modell wird empfohlen, dass Sie den AWS Firewall Manager verwenden, um eine Firewall Manager-Richtlinie zu erstellen, die die Bereitstellung von NGFWs über mehrere AWS-Konten einer AWS-Organisation hinweg erleichtert. Sie werden dann zur Cloud NGFW-Konsole weitergeleitet, um globale Regelstapel zu erstellen und sie der Firewall Manager-Richtlinie zuzuordnen. Der Firewall-Manager ruft dann Cloud NGFW-APIs auf, um die NGFW mit den zugehörigen globalen Regelstapeln zu erstellen, die Ihre Anwendungs-VPCs schützen. Darüber hinaus verwendet der AWS Firewall Manager AWS VPC-APIs, um NGFW-Endpunkte in den von Ihnen angegebenen VPCs zu erstellen.

Weitere Informationen und Beispiele für zentralisierte Bereitstellungen finden Sie unter Verteilte Bereitstellungen in Cloud NGFW für AWS.

Cloud NGFW für AWS – Preise

Pay-as-you-go-Preismodell

Cloud NGFW ist als Pay-as-you-go (PAYG)-Abonnement im AWS Marketplace verfügbar. Bei diesem Modell zahlen Sie nur für das, was Sie jeden Monat nutzen, wobei alle Gebühren auf der Rechnung zusammengefasst sind, die Sie von AWS erhalten. Sie können auch die Vorteile des AWS Marketplace nutzen, wie z. B. die konsolidierte Fakturierung des Amazon Web Services Enterprise-Rabattprogramms (EDP).

Weitere Informationen finden Sie unter Ihr PAYG-Konto mit Cloud NGFW-Credits verknüpfen.

Sie zahlen einen Stundensatz für jede Cloud NGFW-Ressource. Sie zahlen auch für die Menge des Datenverkehrs, abgerechnet nach Gigabyte, die von der NGFW-Ressource verarbeitet wird. Darüber hinaus zahlen Sie einen Stundensatz und für die Menge des von Ihrer Cloud NGFW-Ressource verarbeiteten Datenverkehrs, wenn Sie Security-Services-Add-ons (z. B. Bedrohungsabwehr, erweiterte URL-Filterung, DNS Security oder WildFire) oder das Centralized-Management-Add-on (Panorama-Verwaltung) konfigurieren. Der für den Datenverkehr berechnete Tarif hängt auch vom aggregierten Datenverkehr ab, der von allen NGFWs im Mandanten während des Monats verarbeitet wird (auch *gestaffeltes Preismodell für den Datenverkehr* genannt).

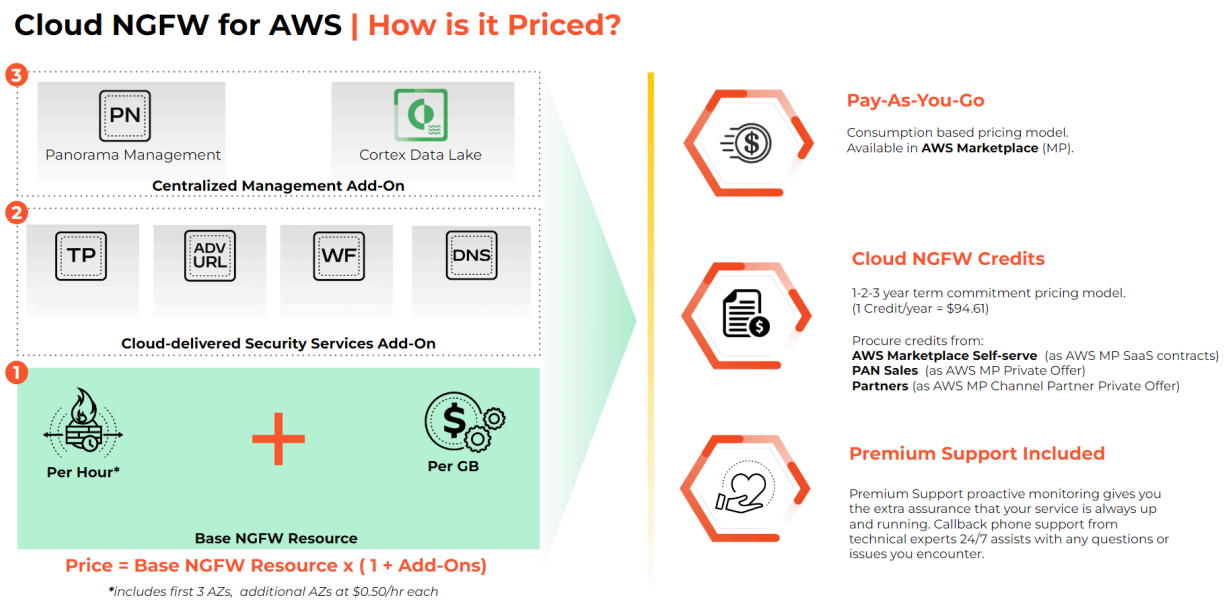
Credits-Preismodell

Sie können Cloud NGFW für AWS Credits erwerben und Ihrem Mandanten zuordnen, indem Sie eine Vorauszahlung für einen langfristigen Vertrag von einem, zwei oder drei Jahren leisten. Sie können diese Credits direkt über AWS Marketplace (AWS SaaS-Verträge) oder zu einem privaten Preis von Palo Alto Networks (AWS Private Offer) oder seinen Partnern (AWS Consulting Partner Private Offer) beziehen. Sie erwerben diese Credits, während Sie die Vorteile von AWS Marketplace nutzen, wie z. B. die konsolidierte Fakturierung, AWS EDP und automatisierte oder konfigurierbare Verlängerungen. Mit Cloud NGFW-Credits können Sie Cloud NGFW-Ressourcen in Ihrem Mandanten bis zu einer bestimmten Kapazität bis zum Ablauf Ihres Vertrags zu geringeren Kosten nutzen. Informationen zum Hinzufügen von Vertrags-Credits finden Sie unter Cloud NGFW für AWS abonnieren.

Wenn Ihr durchschnittlicher Verbrauch pro Monat die erworbenen Credits übersteigt, werden die nicht abgedeckten Kosten zu den PAYG-Tarifen berechnet.

Wenn Sie Cloud NGFW-Credits während eines kostenlosen Testzeitraums hinzufügen, beginnt die Laufzeit Ihres Vertrags sofort und der Vertrag hat Vorrang vor der kostenlosen Testversion.

Verwenden Sie den Preisschätzer für Cloud NGFW für AWS*, um die AWS-Preise für Ihren Cloud NGFW-Mandanten zu bestimmen.*



Messung und Abrechnung

Der Cloud NGFW-Verbrauch wird in stündliche Pay-as-you-go-Preise oder in Cloud NGFW-Credits umgerechnet, wie in den folgenden Tabellen beschrieben.

Basis-NGFW-Ressourcenverbrauch

Sie zahlen einen Stundensatz für jede Cloud NGFW-Ressource. Sie zahlen auch für die Menge des Datenverkehrs, abgerechnet nach Gigabyte, die von der NGFW-Ressource verarbeitet wird.

Basis-NGFW-Ressource		Preis (pro Stunde)	Preis (pro GB)	Entsprechende Cloud NGFW-Credits
Nutzungsstunde	Bis zu 3 AZs	1,50 $		125,0
	Jede weitere AZ	0,50 $		41,7
Gesicherter Datenverkehr	Erste 15 TB/Monat		0,065 $	5,4
	Nächste 15 TB/Monat		0,045 $	3,7
	Über 30 TB/Monat		0,030 $	2,5

Nutzungsstunde wird auf jeder NGFW-Ressource gemessen, die Sie bereitstellen. Datenverkehr wird über alle NGFW-Ressourcen hinweg gemessen, die in Ihrem Cloud NGFW-Mandanten bereitgestellt werden.

Verbrauch der Cloud-Delivered-Security-Services(CDSS)-Add-ons

Wenn Sie Security-Services-Add-ons konfiguriert haben, wird der Verbrauch für jede NGFW-Ressource und für jede Stunde, in der Sie das Add-on aktiviert haben, sowie anhand der Menge des von dieser NGFW verarbeiteten Datenverkehrs gemessen. Der für den Datenverkehr berechnete Tarif hängt auch vom

aggregierten Datenverkehr ab, der von allen NGFWs im Mandanten während des Monats verarbeitet wird (auch *gestaffeltes Preismodell für den Datenverkehr* genannt).

Threat-Prevention-Add-on		**Preis (pro Stunde)**	**Preis (pro GB)**	**Entsprechende Cloud NGFW-Credits**
Nutzungsstunde*	Bis zu 3 AZs	0,300 $		25,0
	Jede weitere AZ	0,100 $		8,3
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,013 $	1,1
	Nächste 15 TB/Monat		0,009 $	0,7
	Über 30 TB/Monat		0,006 $	0,5

Advanced Threat Prevention-Add-on		**Preis (pro Stunde)**	**Preis (pro GB)**	**Entsprechende Cloud NGFW-Credits**
Nutzungsstunde*	Bis zu 3 AZs	0,450 $		0,8
	Jede weitere AZ	0,150 $		0,3
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,020 $	1,7
	Nächste 15 TB/Monat		0,014 $	1,2
	Über 30 TB/Monat		0,009 $	0,7

DNS Security-Add-on		**Preis (pro Stunde)**	**Preis (pro GB)**	**Entsprechende Cloud NGFW-Credits**
Nutzungsstunde*	Bis zu 3 AZs	0,300 $		25,0
	Jede weitere AZ	0,100 $		8,3
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,013 $	1,1
	Nächste 15 TB/Monat		0,009 $	0,7
	Über 30 TB/Monat		0,006 $	0,5

WildFire-Add-on		Preis (pro Stunde)	Preis (pro GB)	Entsprechende Cloud NGFW-Credits
Nutzungsstunde*	Bis zu 3 AZs	0,300 $		25,0
	Jede weitere AZ	0,100 $		8,3
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,013 $	1,1
	Nächste 15 TB/Monat		0,009 $	0,7
	Über 30 TB/Monat		0,006 $	0,5

Advanced URL Filtering-Add-on		Preis (pro Stunde)	Preis (pro GB)	Entsprechende Cloud NGFW-Credits
Nutzungsstunde*	Bis zu 3 AZs	0,450 $		37,5
	Jede weitere AZ	0,150 $		12,5
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,020 $	1,7
	Nächste 15 TB/Monat		0,014 $	1,2
	Über 30 TB/Monat		0,009 $	0,7

DLP-Add-on		Preis (pro Stunde)	Preis (pro GB)	Entsprechende Cloud NGFW-Credits
Nutzungsstunde*	Bis zu 3 AZs	0,600 $		50,0
	Jede weitere AZ	0,200 $		16,7
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,026 $	2,2
	Nächste 15 TB/Monat		0,018 $	1,5
	Über 30 TB/Monat		0,012 $	1,0

**Nutzungsstunde wird auf jeder NGFW-Ressource gemessen, für die das CDSS-Add-on aktiviert ist.*

Verbrauch des Centralized-Management-Add-ons

Sie können eine virtuelle Panorama-Appliance verwenden, um Richtlinienregeln in Ihrem Cloud NGFW-Mandanten zu verwalten. In diesem Fall wird der Verbrauch Ihres Centralized-Management-Add-ons (wenn Sie es konfiguriert haben) auf jeder NGFW-Ressource und für jede Stunde gemessen, die Sie einer Panorama-Appliance zugeordnet haben, und für die Menge des Datenverkehrs, der von dieser NGFW verarbeitet wurde. Der Tarif, der Ihnen für den Datenverkehr berechnet wird, hängt auch vom aggregierten Datenverkehr ab, der von allen NGFWs im Mandanten während des Monats verarbeitet wird (auch *gestaffeltes Preismodell für den Datenverkehr* genannt).

Sie zahlen nicht für zusätzliche Gerätelizenzen zur Verwaltung von Richtlinienregeln in Cloud NGFW-Ressourcen. Panorama rechnet diese NGFW-Ressourcen nicht auf die Anzahl der verwalteten Gerätelizenzen an.

Cloud NGFW sendet Protokolle an denselben Cortex Data Lake-Mandanten, der derzeit Ihrer Panorama-Instanz zugeordnet ist. Sie zahlen nicht für zusätzlichen Speicherplatz im Cortex Data Lake. Bei Verwendung mit Cloud NGFW für AWS wird Cortex Data Lake automatisch zusammen mit den Ressourcen von Cloud NGFW für AWS skaliert. Mit zunehmendem Datenverkehrsdurchsatz auf diesen Cloud NGFW-Ressourcen steigt auch Ihr verfügbarer CDL-Speicher, sodass Sie sich keine Gedanken über manuelle Anpassungen am Cortex Data Lake-Speicher machen müssen, um Ihre Protokolldaten speichern zu können.

Palo Alto Networks Centralized-Management-Add-on		**Preis (pro Stunde)**	**Preis (pro GB)**	**Entsprechende Cloud NGFW-Credits**
Nutzungsstunde	Bis zu 3 AZs	0,300 $		25,0
	Jede weitere AZ	0,100 $		8,3
Abgesicherter Datenverkehr	Erste 15 TB/Monat		0,013 $	1,1
	Nächste 15 TB/Monat		0,009 $	0,7
	Über 30 TB/Monat		0,006 $	0,5

Nutzungsstunde wird auf jeder NGFW-Ressource gemessen, die einer virtuellen Panorama-Appliance zugeordnet ist.

Messmechanismus in AWS Marketplace

Cloud NGFW verwendet das AWS SaaS-Abonnementpreismodell, bei dem der Verbrauch des Mandanten in **Einheiten** für mehrere **benutzerdefinierte** Dimensionen umgerechnet wird, und meldet diese an AWS Marketplace, wie in der folgenden Tabelle dargestellt. Dieser Mechanismus bietet die Flexibilität, den Verbrauch Ihres gesamten Mandanten basierend auf einigen Dimensionen zu aggregieren. Zu diesen Dimensionen gehören die Bereitstellungsstunden aller NGFWs, die Menge des von diesen gesicherten Datenverkehrs und die Anzahl der von ihnen verwendeten Sicherheitsfunktionen pro Stunde. Cloud NGFW rechnet den Verbrauch der Sicherheitsdienste und der zentralen Verwaltung in Cloud NGFW-Credits um und meldet sie als zusätzliche Einheiten an den AWS Metering Service.

AWS Marketplace	Cloud NGFW SaaS-Abonnementpreis
Basis-NGFW-Nutzungsstunden	1,5 $/Einheit
(1 Einheit = 1 Nutzungsstunde) bis zu 3 AZs	
(0,333 Einheiten = 1 Nutzungsstunde) für zusätzliche AZs	
Abgesicherter Datenverkehr > Erste 15 TB/Monat	0,065 $/Einheit
(1 Einheit = 1 GB abgesichert)	
Abgesicherter Datenverkehr > Nächste 15 TB/Monat	0,045 $/Einheit
(1 Einheit = 1 GB abgesichert)	
Abgesicherter Datenverkehr > Über 30 TB/Monat	0,030 $/Einheit
(1 Einheit = 1 GB abgesichert)	
Add-ons	0,012 $/Einheit
(1 Einheit = 1 Cloud NGFW-Credit)	
Weitere Informationen finden Sie weiter oben in den Tabellen zu den verschiedenen Add-ons.	

Ihr PAYG-Konto mit Cloud NGFW-Credits verknüpfen

Beim Integrieren von Credits in Ihr Cloud NGFW für AWS-Abonnement gibt es drei Szenarien:

- Sie haben Ihren Vertrag angenommen, verfügen jedoch nicht über ein Pay-as-you-go(PAYG)-Abonnement.
- Sie verfügen über ein bestehendes PAYG-Abonnement und haben einen neuen Credits-Vertrag mit demselben AWS Marketplace-Konto angenommen.
- Sie haben ein bestehendes PAYG-Abonnement und haben einen neuen Credits-Vertrag über ein anderes AWS-Konto angenommen. Bei diesem Szenario müssen Sie Ihre Konten verknüpfen.

  Die Informationen in den folgenden Abschnitten beschreiben die Aktionen für jedes Szenario.

Palo Alto Networks sendet eine E-Mail mit Informationen zum Cloud NGFW-Credits-Vertrag, die Sie für Ihre Cloud NGFW-Ressource verwenden können. Diese E-Mail enthält Informationen zum Erstellen eines Mandanten für Ihr Cloud NGFW-Abonnement. Sie enthält Informationen zu Ihrem Abonnement, einschließlich der Anzahl der zugewiesenen Credits, der Seriennummer Ihres Kontos, eines Start- und Enddatums und Ihrer Angebots-ID.

Dear Customer,

Please create your tenant by:

1. Going to AWS Marketplace
2. Following the steps in this documentation

Details are as follows:

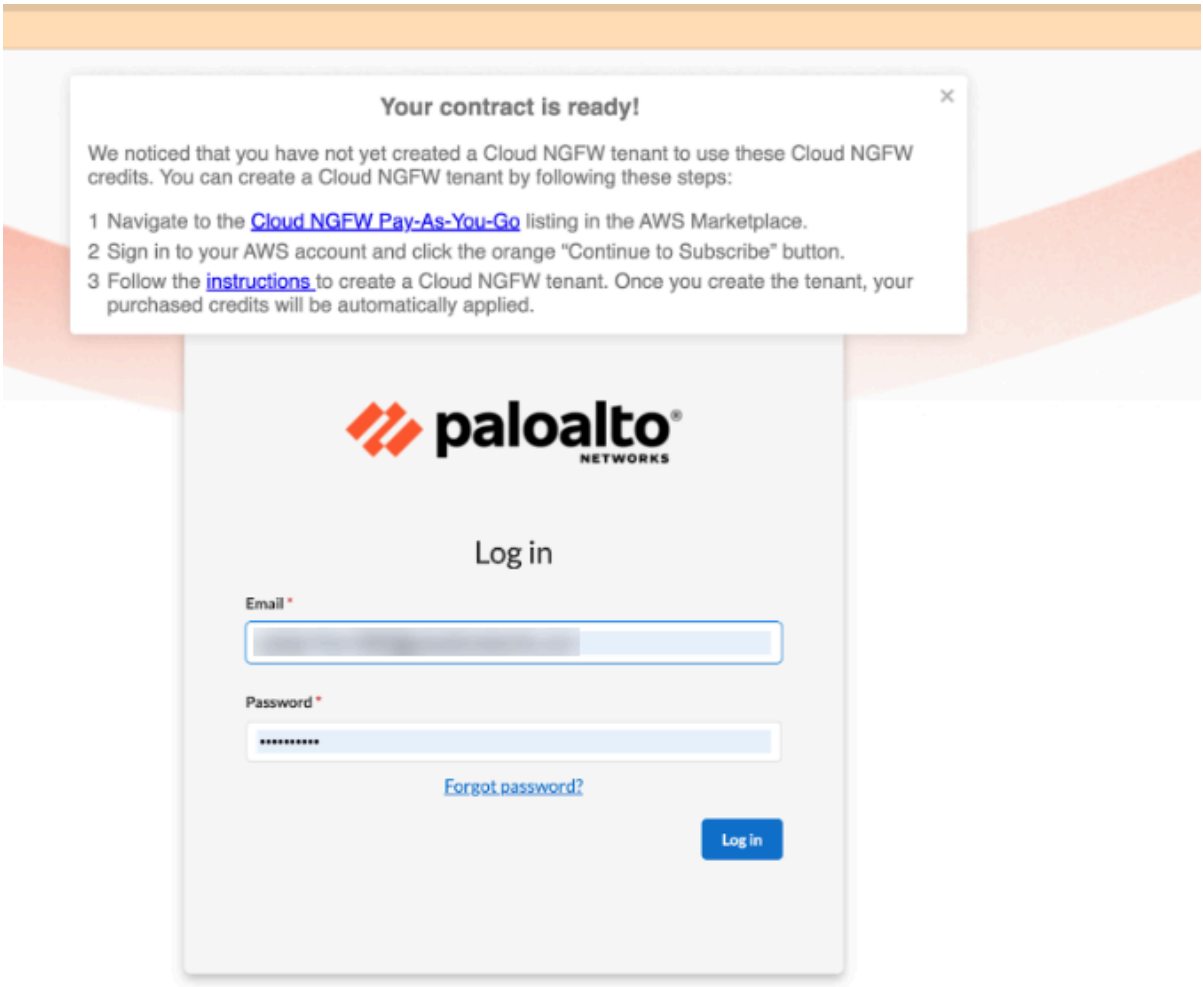
- Credits - {{CREDITS_NUM}}
- Serial Number - {{SERIAL_NUM}}
- Start Date - {{START_DATE}}
- End Date - {{END_DATE}}
- Offer ID - {{OFFER_ID}}

For further help, please navigate to the Cloud NGFW Live Community Page where you can search the documentation, knowledge base and community. Please do not hesitate to contact us if you need any assistance or have any questions.

Credits-Vertrag angenommen, aber es ist kein PAYG-Abonnement vorhanden

Sie haben Ihren Vertrag angenommen, verfügen jedoch nicht über ein PAYG-Abonnement.

STEP 1 | Wenn kein PAYG-Abonnement vorhanden ist, wird Ihnen auf dem Cloud NGFW-Anmeldebildschirm die folgende Meldung angezeigt:



STEP 2 | Melden Sie sich bei der AWS-Konsole mit den Anmeldeinformationen an, die Sie für AWS Marketplace verwenden.

STEP 3 | Entdecken Sie Produkte, indem Sie zur Option **Cloud Next Generation Firewall (PAYG with 30-Day Free Trial) (Cloud Next Generation Firewall (PAYG mit 30-tägiger kostenloser Testversion))** navigieren.

STEP 4 | Klicken Sie auf **Subscribe (Abonnieren)**.

STEP 5 | Klicken Sie auf **Set up product (Produkt einrichten)**.

STEP 6 | Befolgen Sie die Schritte, um PAYG für Ihr Konto zu konfigurieren.

Nach der Einrichtung von PAYG werden Ihre Credits automatisch angewendet.

PAYG-Abonnement vorhanden und Sie haben einen Credits-Vertrag für dasselbe AWS-Konto angenommen

Sie verfügen über ein bestehendes PAYG-Abonnement und haben einen neuen Credits-Vertrag mit demselben AWS Marketplace-Konto angenommen.

STEP 1 | Melden Sie sich bei der AWS-Konsole mit den Anmeldeinformationen an, die Sie für AWS Marketplace verwenden.

STEP 2 | Navigieren Sie in AWS Marketplace zur Option **Cloud NGFW for AWS (Cloud NGFW für AWS)**.

STEP 3 | Klicken Sie auf **Subscribe (Abonnieren)**.

STEP 4 | Klicken Sie für die Option **Palo Alto Networks Cloud NGFW for AWS Credits (Credits für Palo Alto Networks Cloud NGFW für AWS)** auf **Set up Product (Produkt einrichten)**. Verwenden Sie die Anmeldeinformationen Ihres vorhandenen AWS-Kontos.

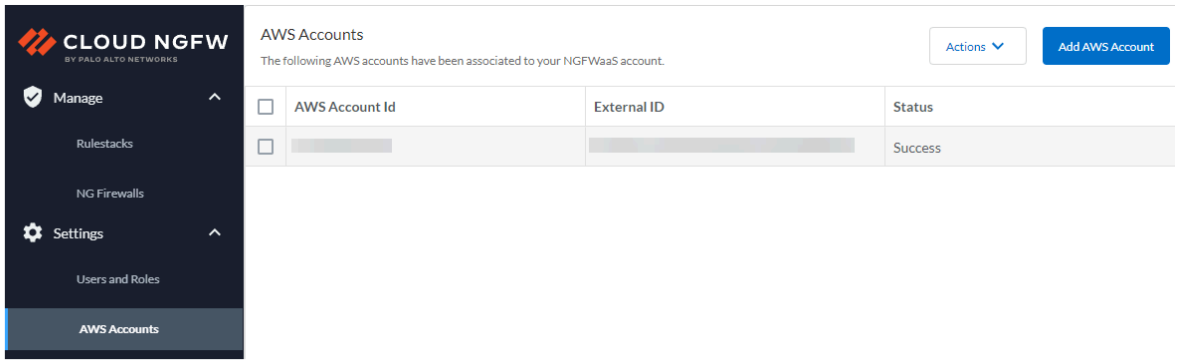
STEP 5 | Befolgen Sie die Schritte, um PAYG für Ihr Konto zu konfigurieren.

Ihre Cloud NGFW-Credits werden nach der Anmeldung angezeigt.

PAYG-Abonnement vorhanden und Sie haben einen Credits-Vertrag für ein anderes AWS-Konto angenommen

Sie haben ein bestehendes PAYG-Abonnement und einen neuen Credits-Vertrag über ein anderes AWS-Konto angenommen. Bei diesem Szenario müssen Sie Ihre Konten verknüpfen.

STEP 1 | Fügen Sie in der Cloud NGFW-Konsole ein zusätzliches Konto für den neuen Credits-Vertrag hinzu. Wählen Sie **Settings > Accounts > Add AWS Account (Einstellungen > Konten > AWS-Konto hinzufügen)**



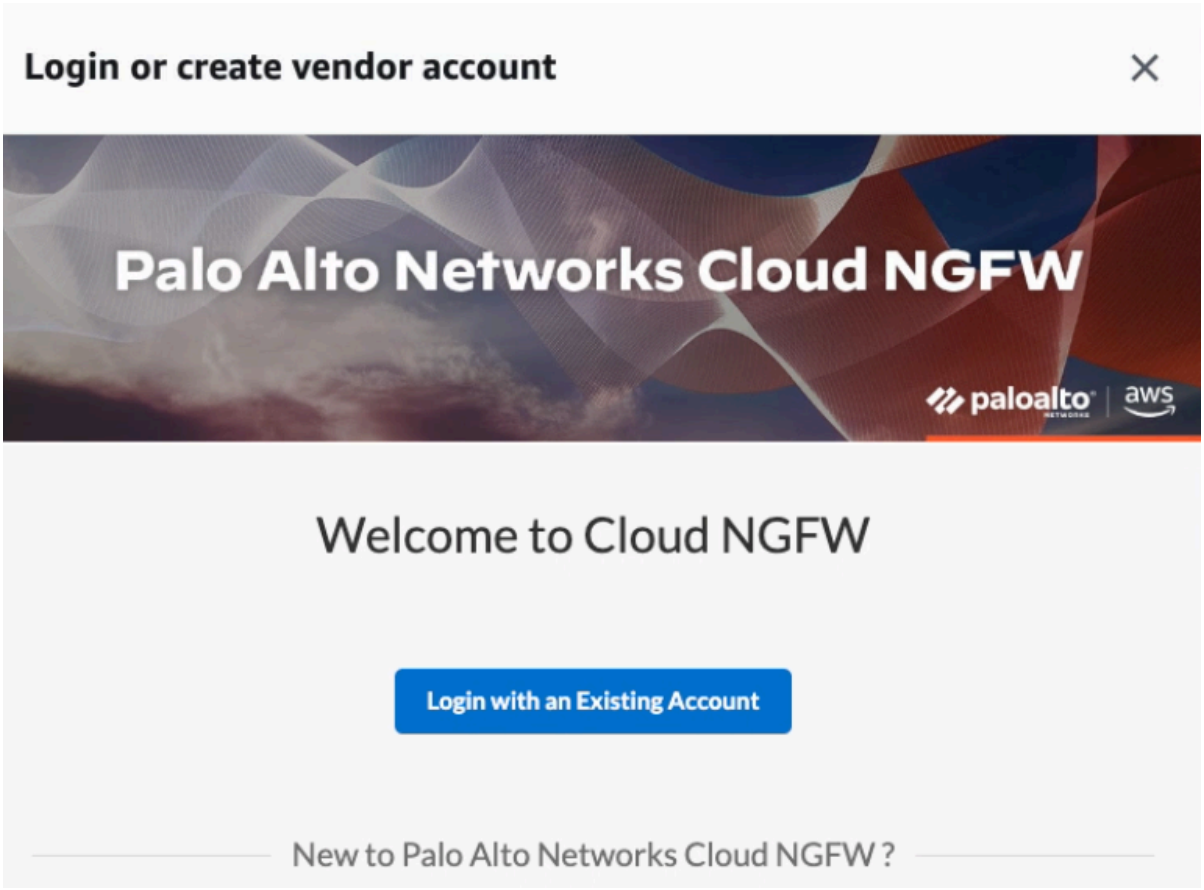
STEP 2 | Aktivieren Sie für das neue Konto, das Sie in der Cloud NGFW-Konsole hinzugefügt haben, das PAYG-Abonnement:

1. Melden Sie sich bei der AWS-Konsole an.

STEP 3 | Navigieren Sie in AWS Marketplace zur Option **Cloud NGFW for AWS (Cloud NGFW für AWS)**.

STEP 4 | Klicken Sie auf **Set up product (Produkt einrichten)**.

STEP 5 | Wählen Sie **Login with Existing Account (Mit bestehendem Konto anmelden)** aus



Ihre Cloud NGFW-Credits werden nach der Anmeldung angezeigt.

*Erstellen Sie während der Kontoeinrichtung keine neuen Mandanten. Stellen Sie sicher, dass Sie **Login with Existing Accounts (Mit vorhandenen Konten anmelden)** auswählen.*

Kostenlose Testversion von Cloud NGFW für AWS

Wenn Sie Cloud NGFW über AWS Marketplace abonnieren, werden Sie automatisch für eine kostenlose Testversion registriert. Navigieren Sie zur Seite **Subscription Management (Abonnementverwaltung)**, um zu prüfen, ob Ihr Cloud NGFW-Mandant mit dem AWS Marketplace-Abonnementeintrag **Palo Alto Networks Cloud NGFW Pay-As-You-Go** verknüpft ist und ob Ihre kostenlose Testversion mit Guthaben aktiv ist.

Um diese kostenlose Testversion zu aktivieren, verknüpft die Cloud NGFW das Guthaben für die kostenlose Testversion mit Ihrem neu erstellten Mandanten. Mit diesem Guthaben können Sie bis zu zwei Firewalls erstellen, die bis zu 100 GB Datenverkehr sichern. Sie können folgende Aktionen ausführen:

- Einbinden Ihrer AWS-Konten bei Ihren Mandanten
- Erstellen von bis zu zwei NGFW-Ressourcen auf Ihren AWS-VPCs
- Erstellen von Regelstapeln

Wenn die kostenlose Testphase endet, zahlen Sie für den Verbrauch. Sie können zur Seite **Subscription Management (Abonnementverwaltung)** navigieren, um zu prüfen, ob Ihr Cloud NGFW-Mandant weiterhin mit dem AWS Marketplace-Abonnementeintrag **Palo Alto Networks Cloud NGFW Pay-As-You-Go** verknüpft ist und Ihre kostenlose Testphase nicht mehr aktiv ist. Bedenken Sie Folgendes:

- Sie können die kostenlose Testphase nicht unterbrechen.
- Am Ende Ihrer kostenlosen Testphase fallen für Sie Gebühren an, wenn Sie die Cloud NGFW nutzen.

Grenzwerte und Kontingente in Cloud NGFW für AWS

In den folgenden Tabellen sind die Grenzwerte für Cloud NGFW aufgeführt. Sofern nicht anders angegeben, können Sie eine Erhöhung dieser Grenzwerte beantragen.

Verwenden Sie den Preisschätzer für Cloud NGFW für AWS, um die AWS-Grenzwerte und -Kontingente für Ihr Cloud NGFW-Abonnement zu bestimmen.

Lokale Richtlinienverwaltung mit Regelstapeln

Name	Standardgrenzwerte pro Cloud NGFW-Mandant
Anzahl der Cloud-Konten (AWS) in einem Mandanten	200
Cloud NGFW-Ressourcen in einem Mandanten	50 pro Konto und Region
Cloud NGFW-Endpunkte in einem Mandanten	50 pro Konto und Region
Cloud NGFW-Endpunkte für jede NGFW-Ressource	50
Ausstehende globale Regelstapel, die keinen NGFW-Ressourcen zugeordnet sind	10
Ausstehende lokale Regelstapel, die keinen NGFW-Ressourcen zugeordnet sind	10

Native Richtlinienverwaltung (Regelstapel)

Attribut	Maximaler Grenzwert pro Cloud NGFW-Ressource
Sicherheitsregeln	1.000
Adressobjekte (FQDN-Liste und IP-Präfixlisten)	1.000
Anzahl der IP-Präfixlisten	1.000
FQDN-Objekte in allen FQDN-Listen	2.000
Präfixobjekte für jede IP-Präfixliste	2.500
Benutzerdefinierte URL-Kategorien	500
URLs in allen URL-Kategorien	25.000

Attribut	Maximaler Grenzwert pro Cloud NGFW-Ressource
Intelligente Feeds (einschließlich der fünf vordefinierten Feeds)	30
IP-Adressen über alle Feeds hinweg	50.000
Zertifikatobjekte	100

Panorama-Richtlinienverwaltung

Attribut	Maximaler Grenzwert pro Cloud NGFW-Ressource*
Richtlinien	
Sicherheitsregeln	6.000
Entschlüsselungsregeln	1.000
Objekte	
Adressobjekte	10.000
Adressgruppen	1.000
Mitglieder pro Adressgruppe	2.500
FQDN-Adressgruppen	2.000
Dienstobjekte	2.000
Dienstgruppen	500
Mitglieder pro Dienstgruppe	500
EDL	
Maximale DNS-Anzahl pro Domänensystem	500.000
Maximale Anzahl von IPs pro System	50.000
Maximale Anzahl von URLs pro System	100.000
Maximale Anzahl benutzerdefinierter Listen	30

Attribut	Maximaler Grenzwert pro Cloud NGFW-Ressource*
URL Filtering	
Gesamtzahl der Entitäten für Zulassungslisten-, Sperrlisten- und benutzerdefinierte Kategorien	25.000
Maximale Anzahl benutzerdefinierter Kategorien	500

*Die angegebenen Grenzwerte für Richtlinien und Objekte sind eindimensionale Maximalwerte. Palo Alto Networks empfiehlt zusätzliche Tests in Ihrer Umgebung, um sicherzustellen, dass Sie Ihre Ziele bei der Richtlinienerstellung erreichen.

Cloud NGFW für AWS abonnieren

Führen Sie die folgenden Schritte aus, um den Cloud NGFW-Dienst zu abonnieren – Sie können ein Cloud NGFW-Pay-as-you-go(PAYG)-SaaS-Abonnement abschließen.

Der erste Schritt bei diesem Verfahren besteht in der Erstellung Ihres ersten Benutzers – eines Mandantenadministrators. Ein Mandantenadministrator ist die höchste Benutzerebene im Cloud NGFW-Dienst. Er bietet die Möglichkeit, AWS-Konten zum Cloud NGFW-Dienst hinzuzufügen und zusätzliche Benutzer einzubinden.

Sie müssen ein Cloud NGFW-PAYG-SaaS-Abonnement erstellen, bevor Sie sich für einen Cloud NGFW für AWS Credits-Vertrag anmelden können.

- Cloud NGFW-PAYG-SaaS-Abonnement
- Ihren aktuellen Cloud NGFW-Zugriff mit SSO und MFA absichern
- Ihrem Mandanten Cloud NGFW für AWS Credits hinzufügen
- Multi-Mandanten-Benutzer eines einzelnen Benutzers, der auf mehreren Mandanten unterstützt wird
- Mehrere AWS-Konten hinzufügen
- CloudFormation-Vorlage manuell hinzufügen

Cloud NGFW-PAYG-SaaS-Abonnement

Bevor Sie Cloud NGFW für AWS abonnieren und in Ihrer AWS-Umgebung bereitstellen, müssen Sie Folgendes berücksichtigen und erstellen. Während des Abschlussprozesses des Abonnements werden Sie aufgefordert, die unten beschriebenen Parameter in einer CloudFormation-Vorlage (CloudFormation Template, CFT) zu definieren, um die Erstkonfiguration abzuschließen.

- **Endpunktkonfiguration** (erforderlich) – Die kontoübergreifende IAM-Rolle enthält Berechtigungen, die es Cloud NGFW ermöglichen, VPC-Ressourceninformationen zu lesen, die für die Konfiguration von NGFW-Endpunkten erforderlich sind.
- **Endpunkterstellung** (optional) – Sie können Cloud NGFW so konfigurieren, dass NGFW-Endpunkte in Ihrer AWS-Umgebung erstellt und verwaltet werden. Indem Sie **Yes (Ja)** auswählen, erteilen Sie Cloud NGFW die Berechtigung, die erforderlichen Endpunkte in Ihren VPCs zu erstellen und zu verwalten. Wenn Sie **No (Nein)**auswählen, müssen Sie manuell NGFW-Endpunkte erstellen und anzeigen.
- **Berechtigungen für die Protokollierung** (optional): Mit Cloud NGFW können Sie Datenverkehrs-, Bedrohungs- und Entschlüsselungsprotokolle an einen S3-Bucket, eine CloudWatch-Protokollgruppe oder Kinesis Data Firehose senden. Damit Cloud NGFW diese Protokolle an das vorgesehene Ziel senden kann, müssen Sie die erforderlichen Berechtigungen bereitstellen.

  Die Cloud NGFW-Konsole leitet Sie zur AWS CloudFormation-Konsole weiter und fordert Sie auf, einen Stapel zu erstellen. Dieser Stapel richtet kontoübergreifende IAM-Rollen ein, legt Protokollierungsziele fest (erstellt sie jedoch nicht) und ermöglicht Cloud NGFW den Zugriff auf Zertifikate im Secrets Manager Ihres AWS-Kontos zur Entschlüsselung.

  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, sollten Sie dieses Ziel erstellen und den Standardwert durch diesen Namen ersetzen, bevor Sie die Stapelerstellung abschließen.

Für einen S3-Bucket als Protokollziel müssen Sie den Namen des Ziel-Buckets angeben.

Wenn Sie Kinesis Data Firehose verwenden, muss die Quelle für diesen Bereitstellungsstream **Direct PUT** sein.

- **Audit Logging (Überwachungsprotokollierung)** (optional) – Sie können Überwachungsprotokolle, die Administratoraktivitäten nachverfolgen, an eine CloudWatch-Protokollgruppe senden. Der CFT-Stapel enthält ein standardmäßiges CloudWatch-Protokollgruppenziel mit dem Namen **PaloAltoCloudNGFWAuditLog**. Sie können eine Cloudwatch-Protokollgruppe mit dem Standardnamenswert erstellen oder den Standardwert durch den Namen einer anderen Cloudwatch-Protokollgruppe ersetzen.
- **Permissions for Decryption (Berechtigungen zur Entschlüsselung)** (optional) – Um Cloud NGFW zur Untersuchung verschlüsselter Datenverkehrsströme zu verwenden, müssen Sie Cloud NGFW erlauben, das erforderliche Zertifikat vom AWS Secrets Manager abzurufen. Sie müssen ermöglichen, dass Cloud NGFW die attributbasierte Zugriffssteuerung verwendet, indem Sie beim Starten des CFT-Stapels ein Tag angeben.

  Standardmäßig enthält die CFT das Tag **PaloAltoCloudNGFW**. Sie können dieses Tag ändern, indem Sie den ARN im Dienst konfigurieren und den Standardwert in der CFT ersetzen.

Führen Sie dieses Verfahren durch, um ein Cloud NGFW-PAYG-SaaS-Abonnement zu aktivieren.

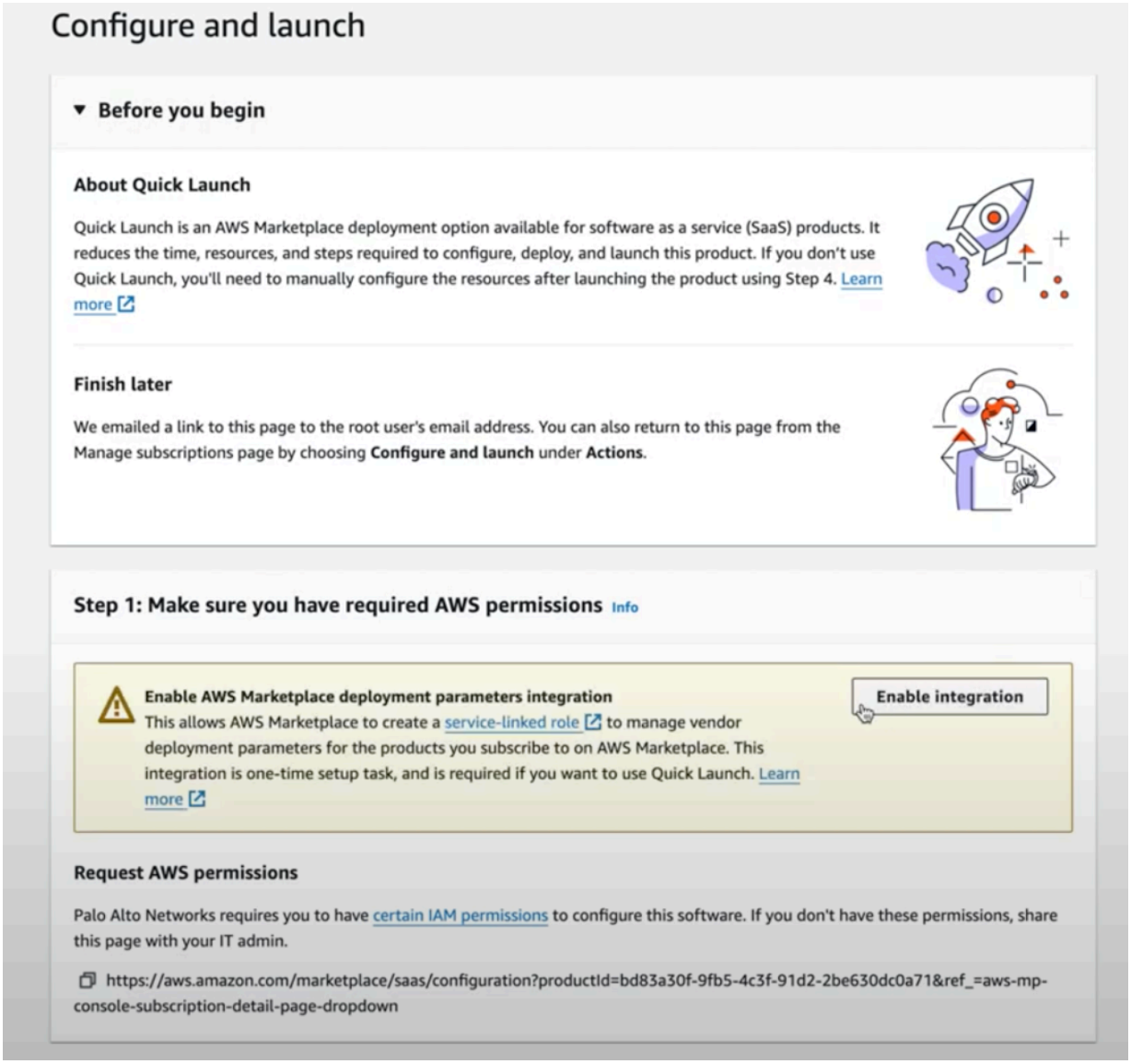
STEP 1 | Melden Sie sich bei der AWS-Konsole an.

STEP 2 | Navigieren Sie im AWS Marketplace zu Cloud NGFW für AWS.

STEP 3 | Klicken Sie auf **Subscribe (Abonnieren)**.

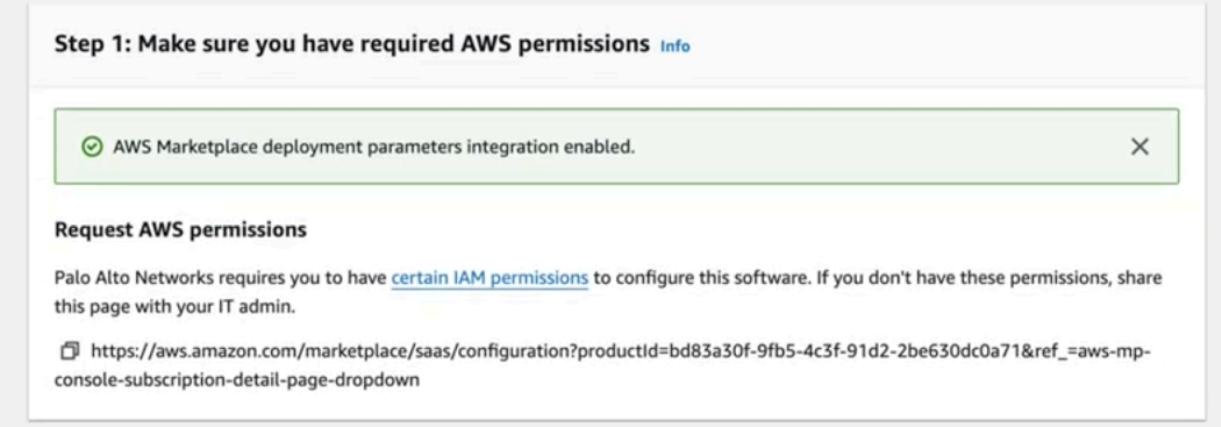
STEP 4 | Klicken Sie auf **Set up product (Produkt einrichten)**. Dadurch wird die Seite „Configure and Launch“ (Konfigurieren und Starten), SaaS-Schnellstart, in AWS Marketplace geöffnet. Palo Alto

Networks hat eine Schnellstart-Funktion für seine Cloud NGFW-Produkte aktiviert, sodass Sie jetzt mit dem Schnellstart einen neuen Mandanten erstellen und bereitstellen können.



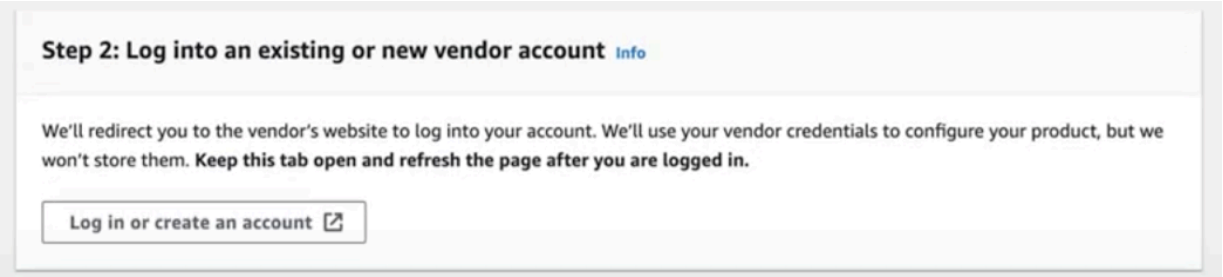
STEP 5 | Klicken Sie auf der Seite „Configure and Launch“ (Konfigurieren und Starten) des Schnellstarts auf **Enable Integration (Integration aktivieren)**, um sicherzustellen, dass Sie über die erforderlichen IAM-Berechtigungen von AWS verfügen.

Wenn Sie ein neuer Benutzer sind, wird die Schaltfläche „Enable Integration“ (Integration aktivieren) automatisch in Schritt 1 der Seite „Configure and Launch“ (Konfigurieren und Starten) angezeigt.



STEP 6 | Klicken Sie auf die Schaltfläche **Login or create an account (Anmelden oder Konto erstellen)**, um sich entweder bei einem vorhandenen Konto anzumelden oder ein neues Konto auf der Website

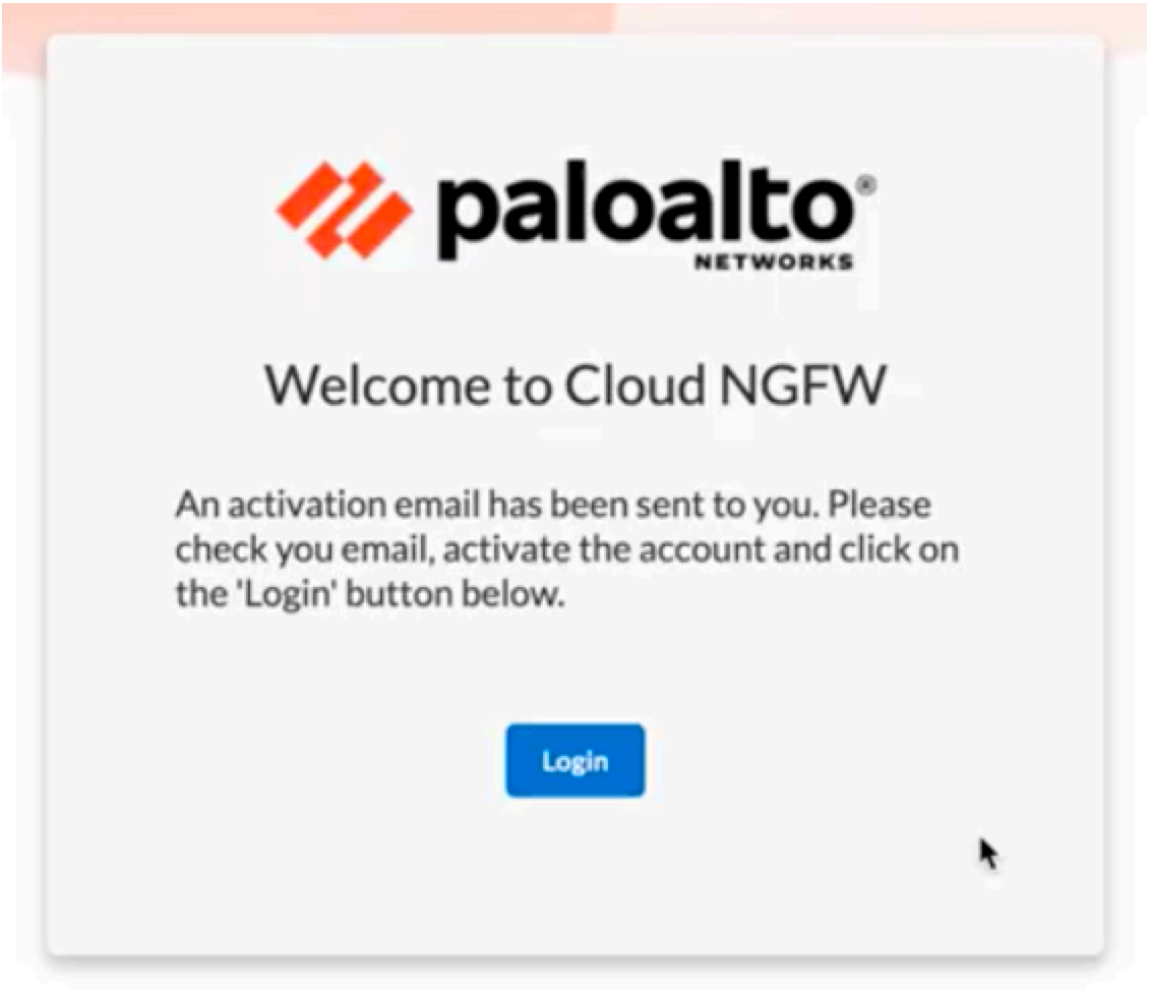
des Anbieters zu erstellen. Dadurch gelangen Sie zu einer Registrierungsseite zum Erstellen eines Mandanten des Cloud NGFW für AWS-Mandanten.



1. Wenn Sie ein ***neuer Benutzer*** sind, müssen Sie ein Cloud NGFW-Konto erstellen. Geben Sie Ihre E-Mail-Adresse ein.

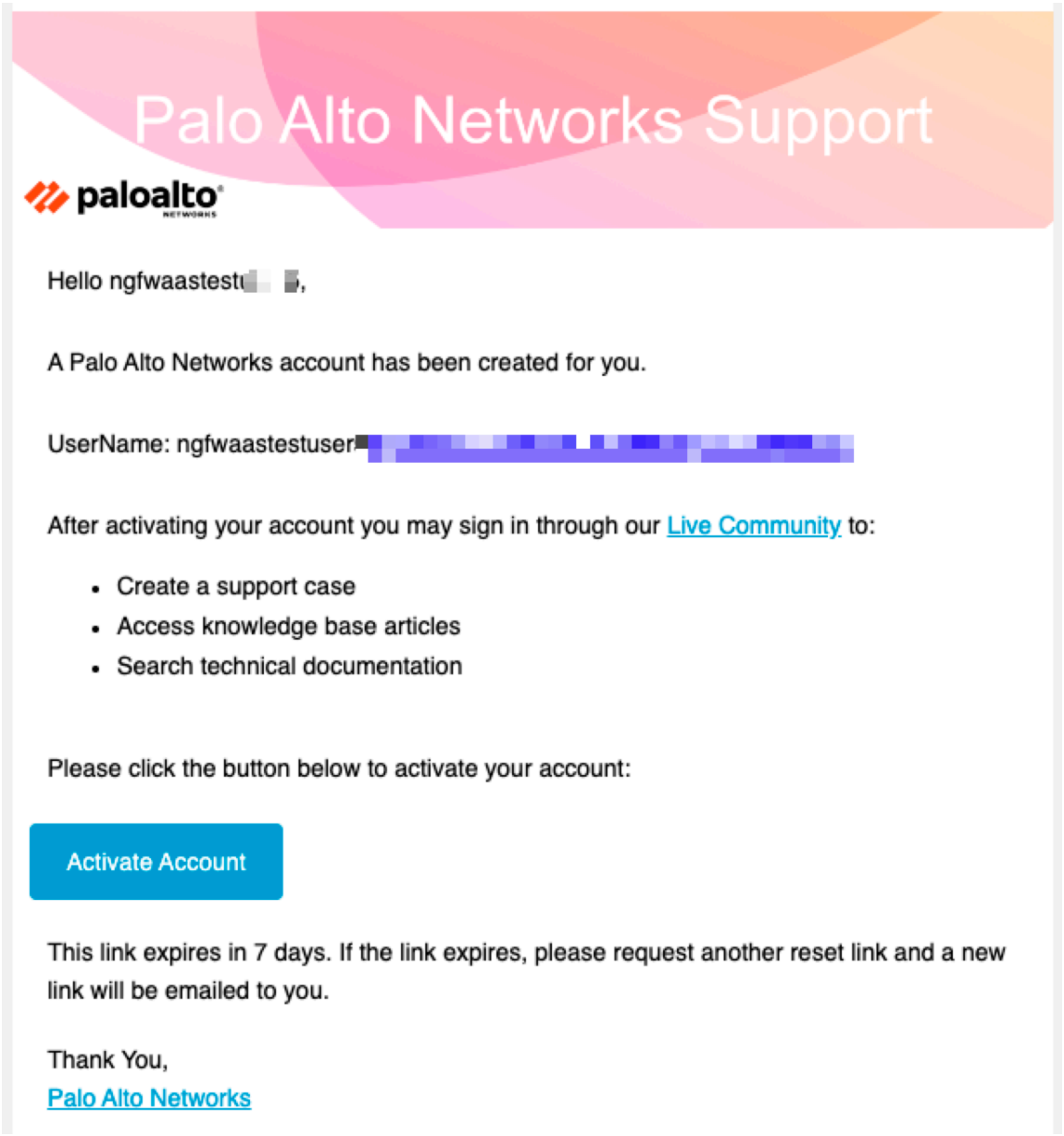
   Die von Ihnen eingegebene E-Mail-Adresse muss identisch mit derjenigen sein, die Sie für die erste Anmeldung beim Cloud NGFW-Dienst verwendet haben. Darüber hinaus wird diese E-Mail-Adresse bei der erstmaligen Anmeldung verwendet, um den ersten Benutzer zu erstellen – den Mandantenadministrator. Außerdem muss die E-Mail-Domäne von den vom Mandantenadministrator eingeladenen Benutzern mit der E-Mail-Domäne des Mandantenadministrators übereinstimmen.
2. Geben Sie unter **First Name (Vorname)** und **Last Name (Nachname)** Ihren Vor- und Nachnamen ein.
3. Klicken Sie auf **Create (Erstellen)**.

   Nachdem Sie auf **Create (Erstellen)** geklickt haben, wird eine E-Mail mit einer Aktivierungsschaltfläche an die oben eingegebene E-Mail-Adresse gesendet.

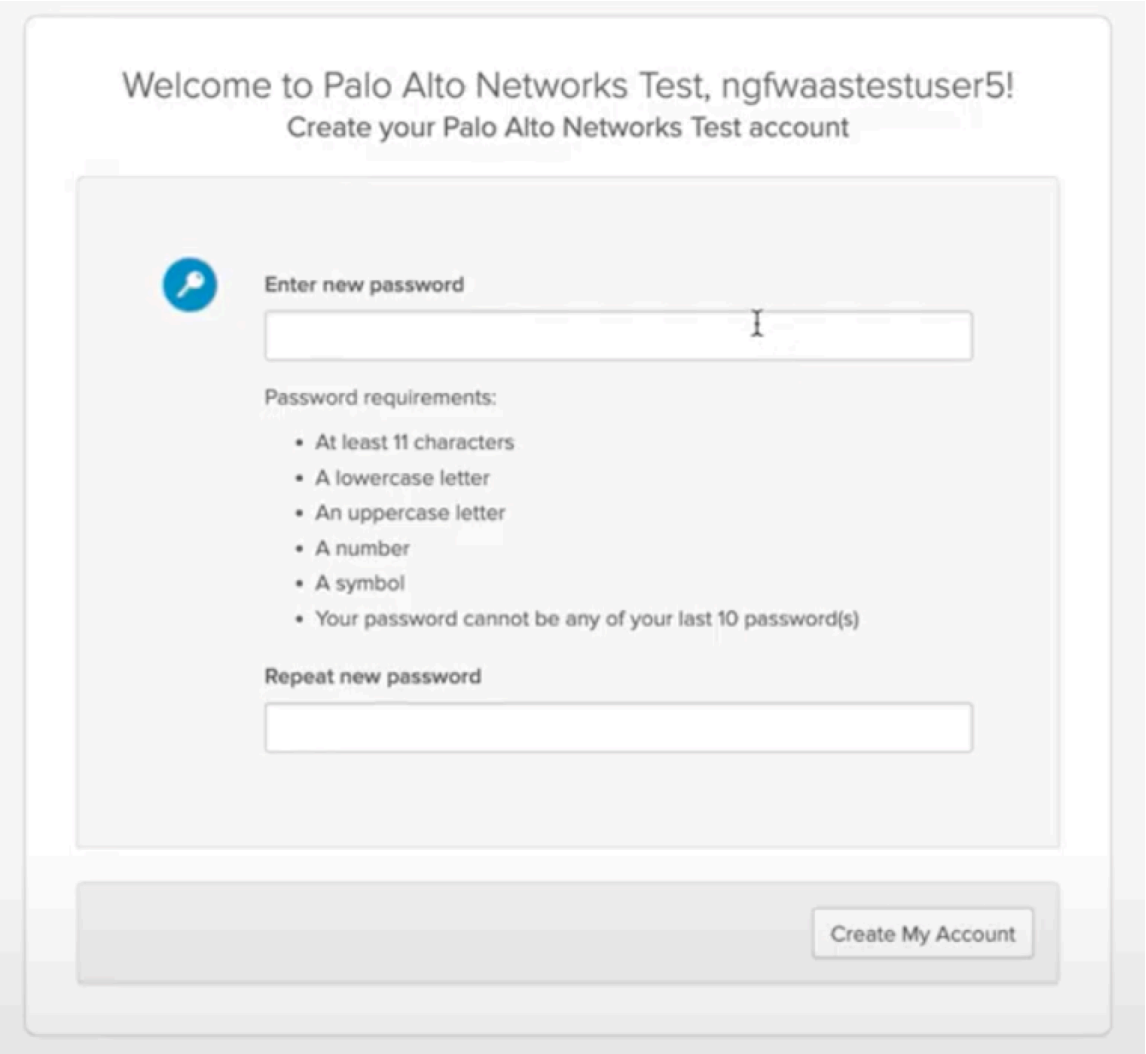


4. Klicken Sie in der E-Mail, die Sie erhalten haben, auf die Schaltfläche **Activate Account (Konto aktivieren)**.

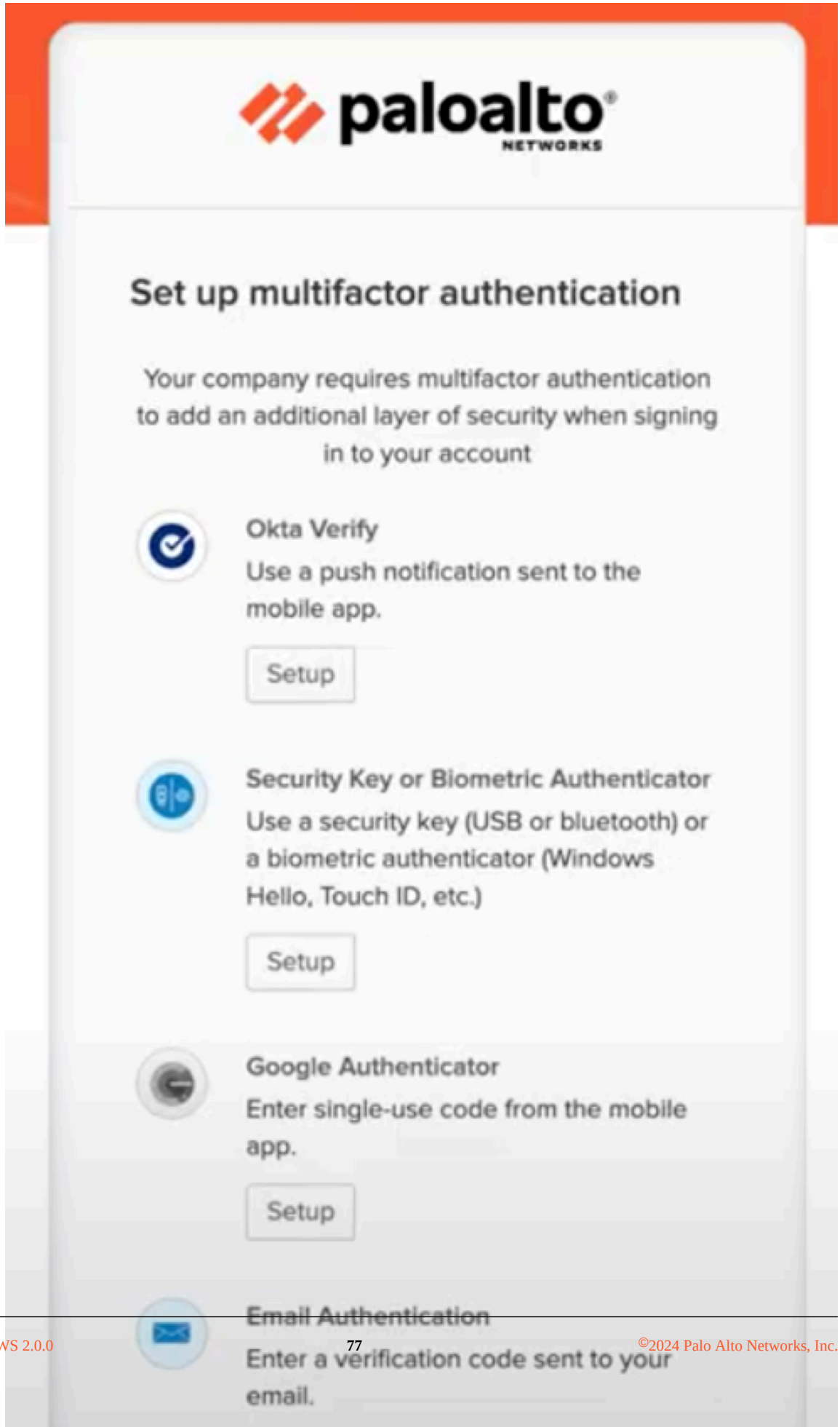
   Der Link ist 7 Tage lang aktiv. Wenn Sie innerhalb von 7 Tagen nicht auf den Link klicken, müssen Sie die Aktivierungs-E-Mail erneut anfordern.



5. Geben Sie Ihr neues Passwort ein und geben Sie es dann noch einmal ein.
6. Klicken Sie auf **Create My Account (Mein Konto erstellen)**.



7. Konfigurieren Sie Ihre Multifaktor-Authentifizierung (MFA).

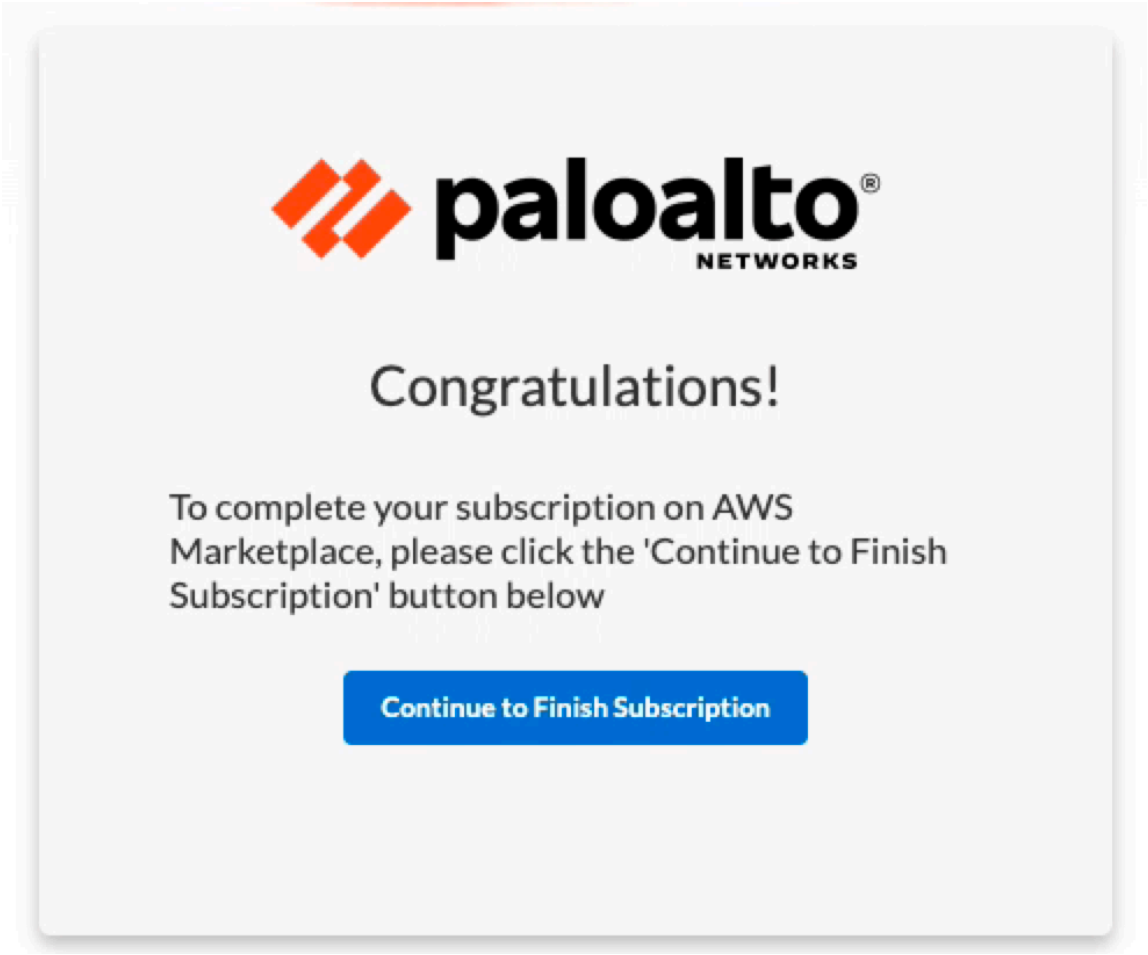


> *Wenn Sie sich nicht bei MFA registriert haben, aber Ihr SSO-Passwort kennen, werden Sie bei Ihrer ersten Anmeldung bei einer der Anwendungen aufgefordert, sich bei MFA zu registrieren. Um MFA zurückzusetzen, erstellen Sie ein Support-Ticket.*

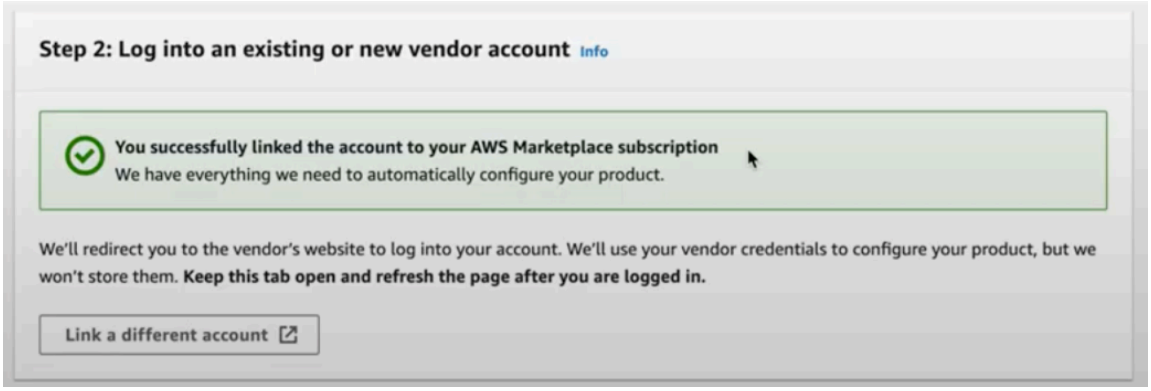
8. Wählen Sie eine der MFA-Methoden aus und klicken Sie auf **Setup (Einrichten)**.
9. Schließen Sie den MFA-Verifizierungsprozess ab. Wenn Sie beispielsweise auf die Schaltfläche „Setup“ (Einrichten) für die E-Mail-Authentifizierung klicken, werden Sie aufgefordert, auf die Schaltfläche **Send me the code (Senden Sie mir den Code)** zu klicken. Nach dem Klicken erhalten Sie eine E-Mail mit dem Bestätigungscode. Geben Sie den Bestätigungscode ein und klicken Sie auf **Verify (Bestätigen)**. Alternativ können Sie den MFA-Verifizierungsprozess

mit Okta Verify, Security Key oder Biometric Authenticator bzw. dem Google Authenticator abschließen.

10. Melden Sie sich mit Ihrer registrierten E-Mail-Adresse und Ihrem Passwort beim Mandanten an und klicken Sie auf **Continue to Finish Subscription (Fortfahren, um das Abonnement abzuschließen)**.



11. Auf der Schnellstartseite wird jetzt angezeigt, dass Sie Ihr Konto erfolgreich mit dem AWS Marketplace-Abonnement verknüpft haben.



1. Wenn Sie ein bestehender Benutzer sind und sich nicht für SSO registriert haben, aber einen neuen Mandanten mit derselben E-Mail-ID erstellen möchten, erhalten Sie nach der Anmeldung beim Mandanten eine Aktivierungs-E-Mail. Befolgen Sie die Schritte 6d bis 6k, um Ihren Mandanten zu registrieren.

   Wenn Sie ein bestehender Benutzer von Cloud NGFW, aber kein Mandantenadministrator sind, ist MFA derzeit nicht verfügbar. Sie werden sich weiterhin anmelden, ohne zur MFA-Registrierung aufgefordert zu werden.

2. Wenn Sie ein bestehender Benutzer sind, der sich für SSO registriert hat, und einen neuen Mandanten mit derselben E-Mail-ID erstellen möchten, werden Sie aufgefordert, einen Mandanten auszuwählen und auf **Continue (Weiter)** zu klicken.

STEP 7 | Klicken Sie auf **Launch Template (Vorlage aufrufen)**, wählen Sie die CFT-Region aus und erstellen Sie Rollen und Berechtigungen für Ihren Mandanten.

Cloud NGFW öffnet die AWS CloudFormation-Vorlage (CloudFormation Template, CFT)-Konsole, die dem AWS-Konto zugeordnet ist, das Sie in einer neuen Browser-Registerkarte angegeben haben. Wenn Sie einen Popup-Blocker installiert haben, wird die neue Registerkarte möglicherweise blockiert. Wählen Sie in diesem Fall in der Cloud NGFW-Konsole „AWS Accounts“ (AWS-Konten) aus und suchen Sie das soeben hinzugefügte AWS-Konto. Klicken Sie in der Spalte **Status** auf **Pending (Ausstehend)**.

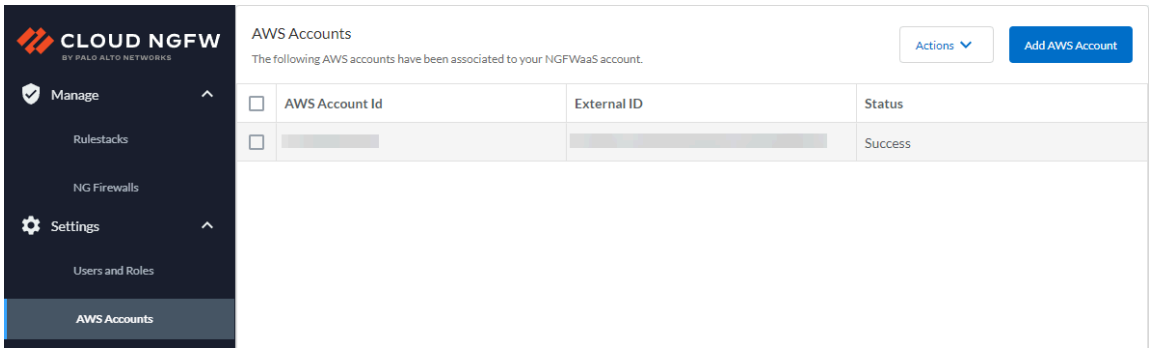
STEP 8 | Aktivieren Sie im Abschnitt „Capabilities“ (Fähigkeiten) unten in der CFT-Konsole das Kontrollkästchen **I acknowledge that AWS CloudFormation might create IAM resources (Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt)**.

STEP 9 | Klicken Sie auf **Create Stack (Stapel erstellen)**. Die mit dem Abonnement verknüpfte CFT (z. B. PaloAltoNetworksCrossAccountRoleSetup) wird angezeigt.

STEP 10 | Klicken Sie auf **Launch your product (Ihr Produkt starten)**.

1. Geben Sie Ihre E-Mail-Adresse und Ihr Passwort ein und klicken Sie dann auf **Log In (Anmelden)**.
2. Wählen Sie **AWS Accounts (AWS-Konten)** aus.
3. Stellen Sie sicher, dass sich der **Status** in **Success (Erfolg)** geändert hat.

*Der Onboarding-Status verbleibt auf **Pending (Ausstehend)**, bis AWS den Start der CFT abgeschlossen hat.*

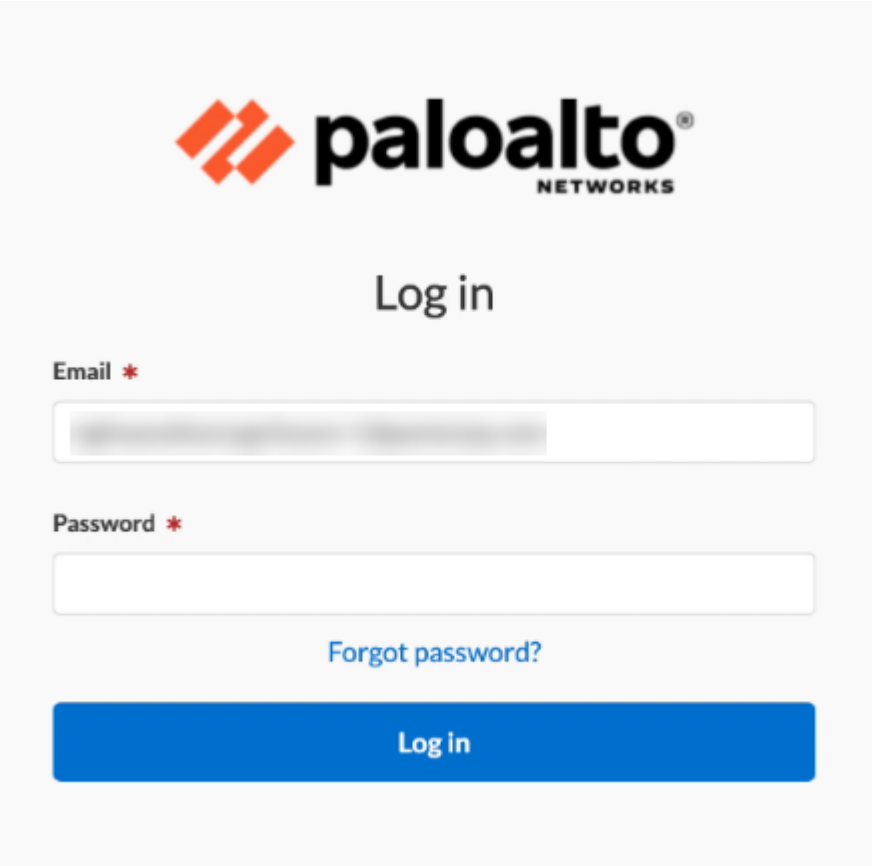


SAML 2.0 kann als Identitätsanbieter für Cloud NGFW für AWS verwendet werden. Weitere Informationen finden Sie unter Integration von Identitätsanbietern von Drittanbietern über allgemeine Dienste verwalten *und* So aktivieren Sie einen Identitätsanbieter (IDP) von Drittanbietern.

Ihren aktuellen Cloud NGFW-Zugriff mit SSO und MFA absichern

Verwenden Sie die Informationen in diesem Abschnitt, um einen vorhandenen Cognito-Benutzer zu SSO zu migrieren. Wenn Sie ein bestehender Benutzer von Cloud NGFW für AWS sind, müssen Sie sich für einen bestehenden Mandanten für zusätzliche Sicherheitsmaßnahmen wie SSO und MFA registrieren (indem Sie die Benutzer-E-Mail mit SSO+MFA aktivieren), um sich anzumelden und auf bestehende Mandanten zuzugreifen.

STEP 1 | Geben Sie die **E-Mail**-Adresse ein, mit der Sie sich bei AWS Cloud NGFW registriert haben, und klicken Sie auf **Log in (Anmelden)**.



STEP 2 | Geben Sie das Passwort ein und klicken Sie auf **Log in (Anmelden)**.

STEP 3 | Sie werden aufgefordert, sich für Palo Alto Networks Single Sign-On (SSO) zu registrieren.

STEP 4 | Klicken Sie auf **Continue (Weiter)**, um mit der SSO-Registrierung fortzufahren. Alternativ können Sie auf **Register Later (Später registrieren)** klicken, um mit Ihren vorherigen

Anmeldeinformationen fortzufahren. Sie werden jedoch bei jedem Anmeldeversuch aufgefordert, sich für SSO zu registrieren.

STEP 5 | Sie erhalten eine E-Mail mit Anweisungen zur Registrierung für SSO. Folgen Sie den Anweisungen und schließen Sie die Registrierung für SSO und MFA wie oben beschrieben ab.

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

STEP 7 | Bei Ihrer nächsten Anmeldung werden Sie mit der Schaltfläche **Enable and Log Out (Aktivieren und Abmelden)** aufgefordert, sich erneut per SSO anzumelden.

STEP 8 | Geben Sie Ihre **E-Mail**-Adresse ein und klicken Sie auf „Log in“ (Anmelden). Sie werden zur SSO-Anmeldeseite weitergeleitet.

STEP 9 | Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Next (Weiter)**.

STEP 10 | Geben Sie das Passwort ein und klicken Sie auf **Log In (Anmelden)**.

STEP 11 | Schließen Sie den MFA-Verifizierungsprozess ab. Sie können jetzt auf die Cloud NGFW-Mandantenseite zugreifen, nachdem Sie sich mit Ihren SSO-Anmeldeinformationen angemeldet haben.

Ihrem Mandanten Cloud NGFW für AWS Credits hinzufügen

Nachdem Sie Ihr PAYG-Abonnement eingerichtet haben, können Sie Ihr Cloud NGFW-Abonnement optional in einen Cloud NGFW-SaaS-Vertrag umwandeln.

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

STEP 2 | Suchen Sie die Liste „Cloud NGFW Contract Credits“ im AWS Marketplace.

STEP 3 | Nachdem Sie die Produktübersichtsinformationen gelesen haben, klicken Sie auf **View purchase options (Kaufoptionen anzeigen)**, um fortzufahren.

STEP 4 | Konfigurieren Sie Ihren Softwarevertrag.

1. Legen Sie die Vertragsdauer fest: **12 months (12 Monate)**, **24 months (24 Monate)** oder **36 months (36 Monate)**.
2. Automatische Verlängerung konfigurieren: **Yes (Ja)** oder **No (Nein)**.

   Sie können Ihren SaaS-Vertrag so konfigurieren, dass er sich am Ende der ausgewählten Vertragslaufzeit automatisch verlängert.

   Wenn Sie sich gegen eine automatische Verlängerung entscheiden, wird Ihr Abonnement nach Ablauf Ihres Cloud NGFW für AWS Credits-Vertrags wieder zu einem standardmäßigen PAYG-Abonnement.

   Kündigen Sie das Cloud NGFW für AWS Credits-Abonnement während der Vertragslaufzeit nicht.
3. Geben Sie die Anzahl der Credits ein. Weitere Informationen finden Sie unter Cloud NGFW für AWS – Preise.
4. Klicken Sie auf **Create contract (Vertrag erstellen)**.

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

How long do you want your contract to run?

○ 12 months ○ 24 months ◉ 36 months

Renewal Settings

Auto Renew when this contract ends on - Sun Aug 03 2025?

◉ Yes
○ No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Contract Options

Cloud NGFW Credits [redacted] / Units 1

Cloud NGFW Credits (1unit = 100 Credits)

You may increase your contract at any time. Changes will be billed on a pro-rated basis. If you have opted in for automatic renewal, your contracts will automatically renew at the end of each term until you change your automatic renewal selection. You may change your automatic renewal selection at any time.

Create contract

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services

Total Contract Price [redacted]

Due Today
Auto Renew -Yes

Cloud NGFW Credits [redacted]

Additional Usage Fees

Pay-as-you-go monthly for additional usage
usage Additional usage costs listed below will apply each month if your usage exceeds your contract. Please contact the seller of this product if you have any questions.

Cloud NGFW Overages [redacted]

Purchase order

Purchase order - *Optional* Learn more

Add purchase order number

STEP 5 | Überprüfen Sie Ihre Vertragsoptionen für Cloud NGFW für AWS Credits und klicken Sie auf **Pay Now (Jetzt bezahlen)**, um Ihren Vertragskauf abzuschließen.

STEP 6 | Klicken Sie auf **Set up your account (Konto einrichten)**, um Ihren Cloud NGFW für AWS Credits-Vertrag abzuschließen.

STEP 7 | Nachdem Sie sich bei der Cloud NGFW-Konsole angemeldet haben, können Sie Ihren Abonnementtyp überprüfen und Ihre Credit-Nutzung überwachen.

1. Melden Sie sich bei der Cloud NGFW-Konsole an.
2. Wählen Sie **Settings (Einstellungen)** > **Subscription Management (Abonnementverwaltung)**.

Multi-Mandanten-Benutzer eines einzelnen Benutzers, der auf mehreren Mandanten unterstützt wird

Cloud NGFW für AWS unterstützt einzelne Anmeldeinformationen für mehrere Mandanten. Wenn Sie sich bei der Cloud NGFW-Konsole anmelden, werden die Anmeldeinformationen verwendet, um den Benutzer dem entsprechenden Mandanten zuzuordnen. Wenn Sie dieselben Anmeldeinformationen für mehrere Mandanten verwenden, werden Sie auf der Anmeldeseite aufgefordert, den Mandanten auszuwählen, den Sie konfigurieren möchten.

Wählen Sie nach der Anmeldung bei Cloud NGFW im Dropdown-Menü den entsprechenden Mandanten aus und klicken Sie dann auf **Continue (Weiter)**.

Die folgende Tabelle veranschaulicht Anwendungsfälle für Szenarien mit mehreren Mandanten:

Anwendungsfall	Schritte
Benutzer A hat sich bereits bei Mandant A registriert und wird zu Mandant B eingeladen.	Sie erhalten keine Aktivierungs-E-Mail.
Benutzer A hat sich bereits bei Mandant A registriert und abonniert über das AWS Marketplace-Abonnement einen neuen Mandanten.	Sie erhalten keine Aktivierungs-E-Mail.

Mehrere AWS-Konten hinzufügen

Sie können mehrere AWS-Konten auf demselben Mandanten einbinden. Nach der Einbindung können Sie Firewall-Ressourcen in mehreren Konten erstellen. Darüber hinaus haben Sie die Möglichkeit, Cloud NGFW-Endpunkte für die Firewall-Ressource in jedem AWS-Konto über eingebundene Konten hinweg bereitzustellen.

Ihr AWS-Kontoabonnement lässt sich für ein verbessertes Abonnementerlebnis in den AWS Marketplace-Dienst integrieren. Diese Integration erfolgt, wenn Sie einen Cloud NGFW-Mandanten erstellen. Dabei wird Ihr AWS-Konto mit dem Cloud NGFW-Mandanten verknüpft.

Dem Mandanten können mehrere AWS-Kontoabonnements hinzugefügt werden. Cloud NGFW unterstützt bis zu 200 Konten.

Sie können mehrere AWS-Konten (ohne neue Abonnementanforderungen) über die Cloud NGFW-Konsole in den Mandanten einbinden und Firewall-Ressourcen in allen eingebundenen AWS-Konten im Mandanten erstellen.

Um die Benutzerfreundlichkeit zu verbessern, ist im Mandanten nur ein Abrechnungskonto vorhanden. Bei Kündigung des Abrechnungskontos in AWS Marketplace wird automatisch das nächste Abrechnungskonto für den Mandanten ausgewählt. Es werden zusätzliche Kontostatusänderungen eingeführt, um den Lebenszyklus des AWS-Kontos im Mandanten besser verwalten zu können. Wenn das Abonnement für das letzte AWS-Konto vom Mandanten gekündigt wird, wird eine Bereinigung der Mandantenressourcen ausgelöst, sofern mit dem Mandanten kein aktiver Vertrag verknüpft ist.

Pro Mandant werden zehn ausstehende Konten unterstützt.

Zusätzlich zur Unterstützung von Multi-Account Tenant unterstützt Cloud NGFW ein Multi-VPC-Firewall-Ressourcenmodell. Mit Multi-VPC-Unterstützung können Sie Ihre Cloud NGFW aktivieren, um den Datenverkehr in mehreren AWS-VPCs abzusichern. Sie zahlen für die Nutzung von Cloud NGFW für jede AWS-Verfügbarkeitszone, für die die NGFW zur Absicherung des Datenverkehrs bereitgestellt wird.

Im Abschnitt **Endpoint Management (Endpunktverwaltung)** auf der Seite **Create Firewall (Firewall erstellen)** können Sie verwalten, wie Endpunkte für die NGFW in diesen Verfügbarkeitszonen erstellt werden. Sie zahlen AWS für jeden VPC-Endpunkt (Gateway Load Balancer), den Sie für die NGFW erstellen.

Beachten Sie bei der Verwendung von Multi-VPC-Firewall-Ressourcen Folgendes:

- Multi-VPC-Firewalls werden nur im kundenverwalteten Modus unterstützt.

- Endpunkte für eine Multi-VPC-Firewall-Ressource können in jeder VPC aller erfolgreich eingebundenen Konten vorhanden sein. Für eine Multi-VPC-Firewall-Ressource werden 50 Endpunkte unterstützt.
- Wenn Sie die Multi-VPC-Funktion für eine Firewall-Ressource deaktivieren, kann ein Endpunkt nur in der Anker-VPC (und im Anker-Konto) vorhanden sein. Der Anker stellt eine stabile Verbindung zur Verfügbarkeitszone dar. Anker-VPC und Ankerkonto beziehen sich auf die VPC und das Konto, die zum Zeitpunkt der Erstellung der Firewall-Ressource zugeordnet waren. Die Kommunikation mit der VPC schlägt fehl, wenn ein Endpunkt außerhalb des Ankerkontos und der VPC vorhanden ist.
- Wenn Sie ein Konto vom Mandanten entfernen, müssen alle Endpunkte von Multi-VPC-Firewalls aus dem Konto entfernt werden. Der Aufruf schlägt fehl, wenn ein Endpunkt in einem Konto vorhanden ist, das aus dem Mandanten entfernt wurde.
- Wenn Sie für eine Firewall-Ressource Endpunkte über Konten hinweg erstellen, sollten die Endpunkte in einer der Zonen-IDs erstellt werden, die den in der Firewallkonfiguration definierten Zonen zugeordnet sind.
- Zonen-ID-Namen werden in AWS anders behandelt. Verwenden Sie für separate Konten dieselbe Zonen-ID, um sicherzustellen, dass der Endpunkt in der richtigen Zone angezeigt wird.
- Während die Konto-ID für ein einzelnes Konto optional ist, ist die Verwendung der Konto-ID für mehrere Konten obligatorisch.

Der Zonenname (z. B. us-east-la) hat bei verschiedenen Konten eine jeweils andere Zuordnung zur Zonen-ID (z. B. use1-az4).

Sie können dem Cloud NGFW-Mandanten kontoübergreifende Rollen aus Ihrem AWS-Konto hinzufügen, indem Sie das erweiterte Abonnementerlebnis von AWS Marketplace nutzen. Dieser Vorgang erfordert das Hinzufügen zusätzlicher IAM-Berechtigungen und die Bereitstellung von Ressourcen. Sie können die Rollen-ARNs auch manuell über die Cloud NGFW-Konsole hinzufügen. Die kontoübergreifende Rollenverwaltung wird für das inkrementelle Hinzufügen der Rollen unterstützt.

Das Aktualisieren von CloudFormation-Vorlagen wird unterstützt.

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

Für bereits eingebundene AWS-Konten können Sie mithilfe von Multi-Account Tenant weitere Konten hinzufügen. Rufen Sie zunächst die AWS Marketplace-Abonnementseite für Ihr Palo Alto Networks NGFW-Abonnement auf.

STEP 1 | Rufen Sie in AWS Marketplace Ihr Abonnement auf.

STEP 2 | Stellen Sie in Schritt 1 sicher, dass Ihr Abonnement über die erforderlichen AWS-Administratorberechtigungen verfügt.

STEP 3 | Verknüpfen Sie in Schritt 2 ein neues oder bestehendes Anbieterkonto. Klicken Sie auf **Login or create vendor account (Anmelden oder Anbieterkonto erstellen)**, um auf ein vorhandenes Cloud NGFW-Konto zuzugreifen, Ihren Mandanten zu verknüpfen und die Kommunikation mit dem AWS-Dienst zu ermöglichen. Die Anmeldeseite von **Palo Alto Networks Cloud NGFW** wird angezeigt.

STEP 4 | Klicken Sie im Bildschirm **Welcome (Willkommen)** auf **Login with an Existing Account (Mit einem vorhandenen Konto anmelden)**.

STEP 5 | Geben Sie Ihre Anmeldeinformationen für den Cloud NGFW-Mandanten ein. Nach der Anmeldung zeigt AWS Marketplace an, dass Sie Ihr Anbieterkonto erfolgreich verknüpft haben.

Wenn für Ihr Konto keine CloudFormation-Vorlage (CloudFormation Template, CFT) vorhanden ist oder Sie eine vorhandene CFT konfigurieren müssen, finden Sie am Ende dieses Artikels Informationen zum manuellen Hinzufügen einer CloudFormation-Vorlage.

STEP 6 | Wenn eine CFT vorhanden ist, fahren Sie mit Schritt 4 fort und starten Sie die Cloud NGFW-Konsole, um die Konfiguration fortzusetzen. Klicken Sie auf **Launch Product (Produkt starten)**.

STEP 7 | Melden Sie sich bei der Cloud NGFW-Konsole an.

STEP 8 | Wählen Sie **AWS Accounts (AWS-Konten)** aus.

STEP 9 | Wählen Sie die **AWS-Konto-ID** aus, für die Sie das Konto als Multi-Account Tenant hinzufügen möchten.

STEP 10 | Klicken Sie auf **Add AWS Account (AWS-Konto hinzufügen)**.

STEP 11 | Geben Sie den Namen der **AWS-Konto-ID** für das Konto ein, das Sie dem bestehenden Konto hinzufügen möchten.

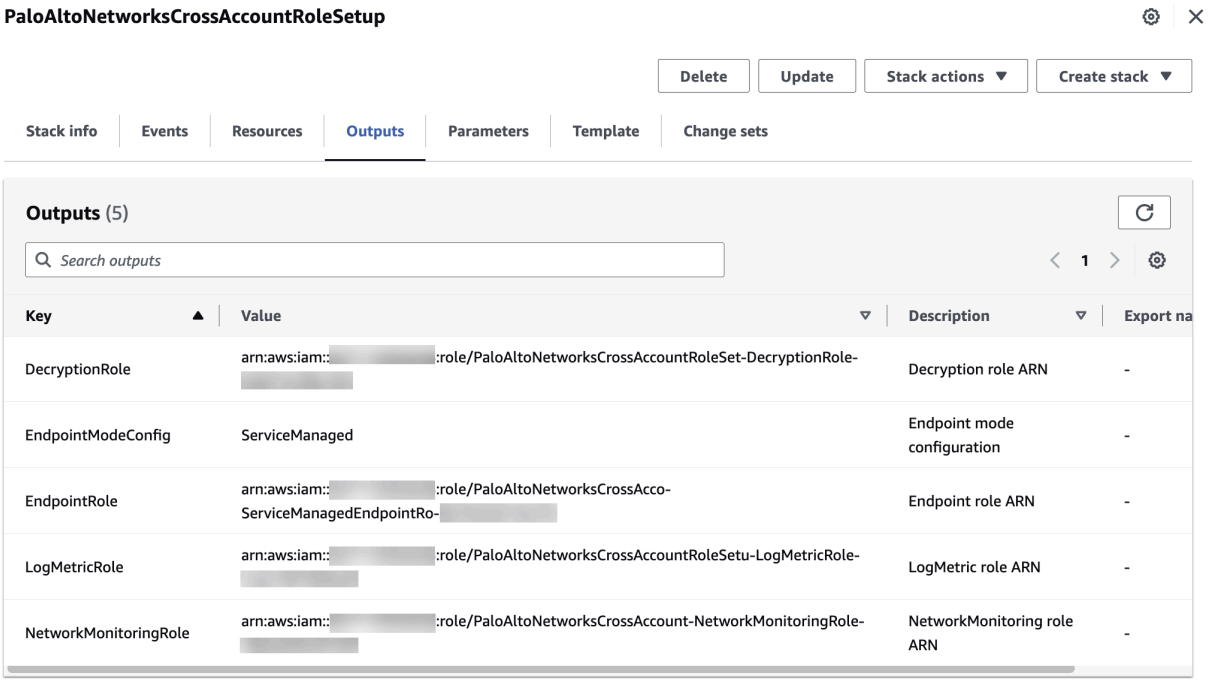
STEP 12 | Melden Sie sich bei Ihrem AWS-Konto an.

STEP 13 | Erstellen Sie mit der AWS-Konsole einen Stapel. Klicken Sie dazu auf **Create Stack on AWS (Stapel in AWS erstellen)** oder verwenden Sie alternativ die Befehlszeilenschnittstelle von AWS.

STEP 14 | Wählen Sie **I acknowledge that AWS CloudFormation might create IAM resources with custom names (Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt)** aus.

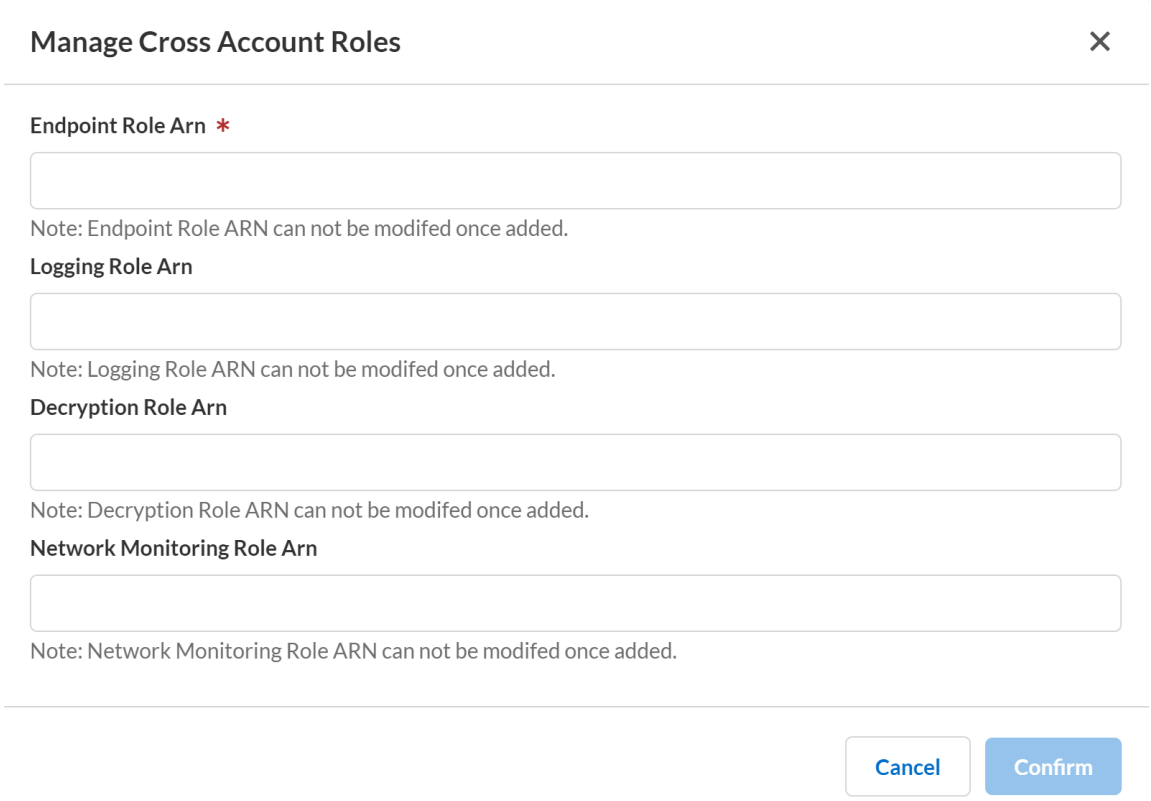
STEP 15 | Klicken Sie auf **Create Stack (Stapel erstellen)**.

STEP 16 | Sobald der Status **CREATE_COMPLETE (ERSTELLEN ABGESCHLOSSEN)** anzeigt wird, kopieren Sie den Rollen-ARN-**Wert** aus der Registerkarte **Outputs (Ausgaben)** in die AWS-Konsole.



STEP 17 | Fügen Sie die Rollen-ARN-Werte zur Cloud NGFW-Mandantenkonsole hinzu.

1. Kehren Sie zur Cloud NGFW-Mandantenkonsole zurück.
2. Wählen Sie in der Cloud NGFW-Mandantenkonsole die Option **Settings (Einstellungen)** > **AWS Accounts (AWS-Konten)** aus.
3. Wählen Sie das Optionsfeld des hinzuzufügenden AWS-Kontos aus und wählen Sie aus der Dropdown-Liste **Actions (Aktionen)** die Option **Manage Cross Account Roles (Kontoübergreifende Rollen verwalten)** aus.
4. Fügen Sie die Rollen-ARN-Werte aus dem vorherigen Schritt in die entsprechenden Felder ein.
5. Klicken Sie auf **Confirm (Bestätigen)**.



CloudFormation-Vorlage manuell hinzufügen

In einigen Fällen müssen Sie einem Konto eine CloudFormation-Vorlage (CloudFormation Template, CFT) möglicherweise manuell hinzufügen.

STEP 1 | Wählen Sie in der Cloud NGFW-Konsole das AWS-Konto aus, das Sie konfigurieren möchten.

STEP 2 | Klicken Sie unter **Account Property (Kontoeigenschaft)** auf **Check Details (Details prüfen)**. Dieser Bildschirm enthält Details, die Sie für die CFT verwenden.

STEP 3 | Der Bildschirm **Account Property Details (Kontoeigenschaftsdetails)** enthält die erforderlichen Informationen zum manuellen Erstellen einer neuen CFT. Um Ihre Sicherheit zu verbessern,

generieren Sie ein neues Token für die neue CFT. Klicken Sie auf **Generate Update Token (Update-Token generieren)**.

STEP 4 | Verwenden Sie die aktualisierten Token-Informationen zusammen mit den anderen Informationen im Bildschirm **Account Property Details (Kontoeigenschaftsdetails)** (externe ID, Cloud NGFW-Konto-ID und SNS-Thema-ARN), um die CFT manuell in der AWS-Konsole zu konfigurieren.

STEP 5 | Zur Unterstützung der Funktion Multi-Account Tenant wurden der Seite „AWS CFT Stack“ für Ihr Abonnement einige Funktionen hinzugefügt. Suchen Sie Ihr Abonnement in der AWS-Konsole und verwenden Sie die Informationen auf der Registerkarte **Events (Ereignisse)**, um den Status eines CFT-Stapels zu überwachen.

STEP 6 | Verwenden Sie die Registerkarte **Outputs (Ausgaben)**, um Informationen anzuzeigen, die Sie verwenden werden, z. B. die Schlüssel **EndpointRole** und **LogMetricRole** für die manuelle Konfiguration von Multi-Account Tenant für ein vorhandenes AWS-Konto in der Cloud NGFW-Konsole. Kopieren Sie diese Informationen, damit Sie sie später verwenden können.

STEP 7 | Wählen Sie in der Cloud NGFW-Konsole **AWS Accounts (AWS-Konten)** aus. Wählen Sie das Konto aus, das Sie konfigurieren möchten, und wählen Sie dann im Dropdown-Menü die Option **Manage Cross Account Rules (Kontenübergreifende Regeln verwalten)** aus.

STEP 8 | Geben Sie im Bildschirm **Account Property Details (Kontoeigenschaftsdetails)** den **Endpunktregel-ARN**, **Protokollierungsregel-ARN** und den **Netzwerküberwachungsrollen-ARN** ein. Sie finden diese Informationen im Feld **Endpoint Rules (Endpunktregeln)** auf der Registerkarte **Outputs (Ausgaben)** in der AWS-Konsole (**CloudFormation > Stacks (Stapel)**). Klicken Sie anschließend auf **Create (Erstellen)**.

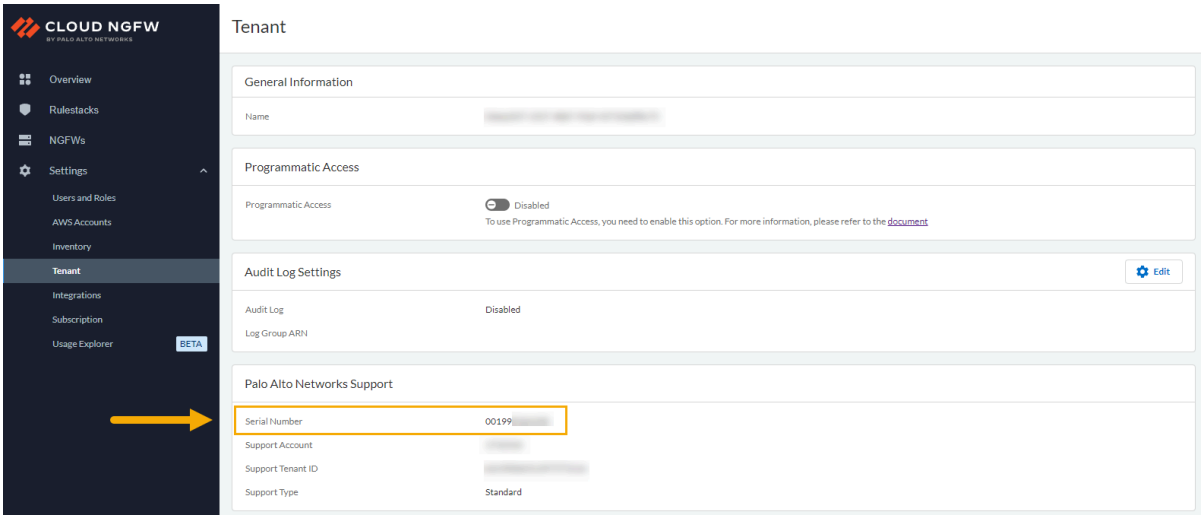
Nachdem Sie die ARN-Informationen im Bildschirm **Account Details (Kontodetails)** aktualisiert haben, wird auf der Seite **Cloud NGFW AWS Accounts (Cloud NGFW AWS-Konten)** angezeigt, dass die Kontoinformationen erfolgreich aktualisiert wurden.

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.



Kontoübergreifende Rollen-CFT-Berechtigungen für Cloud NGFW

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" } ] }
```


Benutzer zu Cloud NGFW für AWS einladen

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, indem Sie die E-Mail-Adresse des Benutzers angeben und eine oder mehrere Cloud NGFW-Rollen zuweisen, sendet der Cloud NGFW-Mandant dem Benutzer eine E-Mail mit einem Registrierungslink und einem temporären Passwort. Nach der ersten Anmeldung wird der neue Benutzer aufgefordert, ein neues Passwort zu erstellen. 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 • Benutzer einladen und Rollen zuweisen • NGFW erstellen • Globale und lokale Regelstapel erstellen/verwalten
Mandantenadministrator	• AWS-Konten hinzufügen • Benutzer einladen und Rollen zuweisen
Mandanten-Reader	• Alle Firewall-Ressourcen und ihre Einstellungen lesen • Alle globalen und lokalen Regelstapel lesen • Alle Mandantenbenutzer und Mandanteneinstellungen lesen
Globaler Firewall-Administrator	• NGFW erstellen • Globale und lokale Regelstapel erstellen
Administrator für globalen Regelstapel	Globalen Regelstapel erstellen
Lokaler Firewall-Administrator	• NGFW erstellen • Lokalen Regelstapel mit NGFWs verknüpfen *Lokale Firewall-Administratoren können nur innerhalb eines bestimmten AWS-Kontos NGFWs erstellen und Regelstapel zuordnen.*
Administrator für lokale Regelstapel	• Lokale Regelstapel erstellen • Lokale Regelstapel mit NGFWs verknüpfen

Cloud NGFW-Rolle	Berechtigungen
	Jedem Administrator für lokale Regelstapel ist eine Konto-ID zugeordnet. 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.

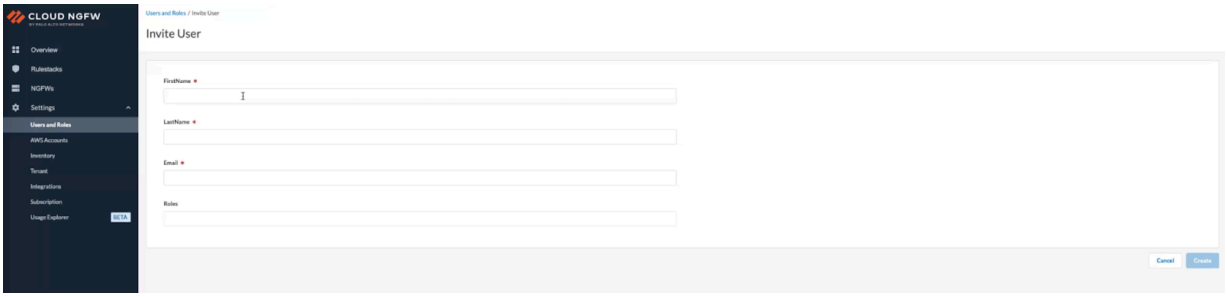
STEP 1 | Melden Sie sich beim Cloud NGFW-Mandanten an.

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

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 zu ändernden 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 zu löschenden 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. Sie müssen sich mit dem neuen Passwort erneut anmelden.

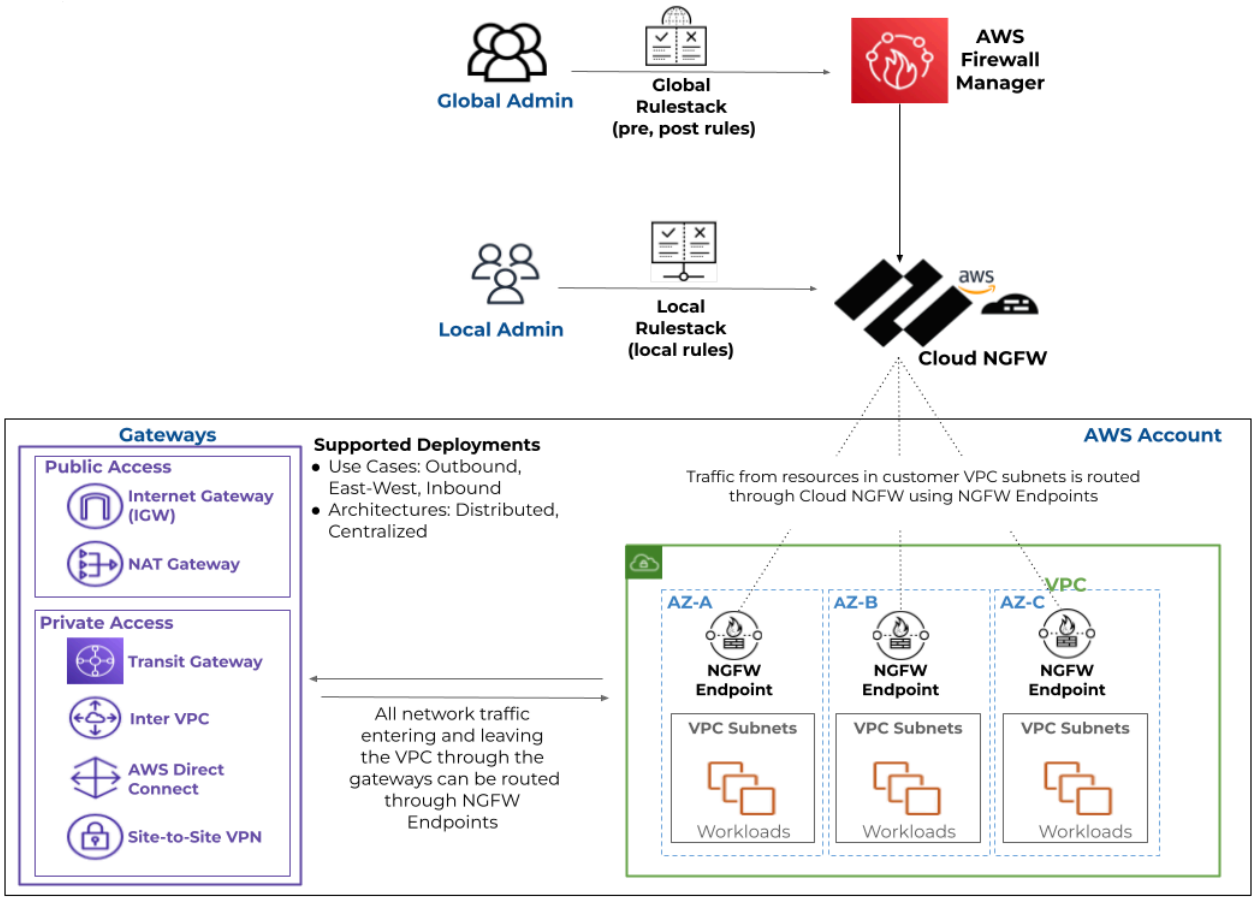
STEP 5 | Klicken Sie auf **Save (Speichern)**.

Cloud NGFW für AWS mit AWS Firewall Manager bereitstellen

AWS Firewall Manager (FMS) ist ein Dienst, mit dem Sie Regeln für AWS Web Application Firewalls, Security Groups und AWS Network Firewalls für alle Mitgliedskonten der AWS-Organisation zentral verwalten können. Sie können AWS Firewall Manager jetzt verwenden, um Cloud NGFW-Ressourcen zentral bereitzustellen und Regeln für VPCs in verschiedenen AWS-Konten Ihrer AWS-Organisation zu verwalten. Das AWS Firewall Manager-Dashboard ermöglicht Ihnen außerdem, Konformitätsbenachrichtigungen anzuzeigen und darauf zu reagieren.

AWS Firewall Manager bietet einen Workflow, mit dem Sie Cloud NGFW als FMS-Richtlinie bereitstellen, einen Bereitstellungsmodus und eine Region auswählen, einen globalen Regelstapel erstellen, NGFW-Endpunkte konfigurieren und den Umfang von Cloud NGFW in Ihrer Organisation definieren können.

Weitere Informationen finden Sie in der Dokumentation zu AWS Firewall Manager.



Cloud NGFW unterstützt VPC-Ressourcen nur innerhalb des Geltungsbereichs der FMS-Richtlinie.

STEP 1 | Cloud NGFW für AWS abonnieren. Das AWS-Konto, das Sie zum Abonnieren des Cloud NGFW-Diensts verwenden, muss mit dem AWS Firewall Manager-Administratorkonto identisch sein.

Als IAM-Benutzer im AWS Firewall Manager-Konto abonnieren Sie zunächst den Cloud NGFW-Dienst über den AWS Marketplace. Kehren Sie nach der Ersteinrichtung zum FMS-Dashboard in der AWS-Konsole zurück. Mit diesem Verfahren wird ein Cloud NGFW-Mandant erstellt und Ihnen (dem FMS-Administrator) werden automatisch die Rollen „TenantAdmin“ (Mandantenadministrator) und „GlobalFirewallAdmin“ (Globaler Firewall-Administrator) zugewiesen.

STEP 2 | Verknüpfen Sie den Cloud NGFW-Dienst von Palo Alto mit Firewall Manager.

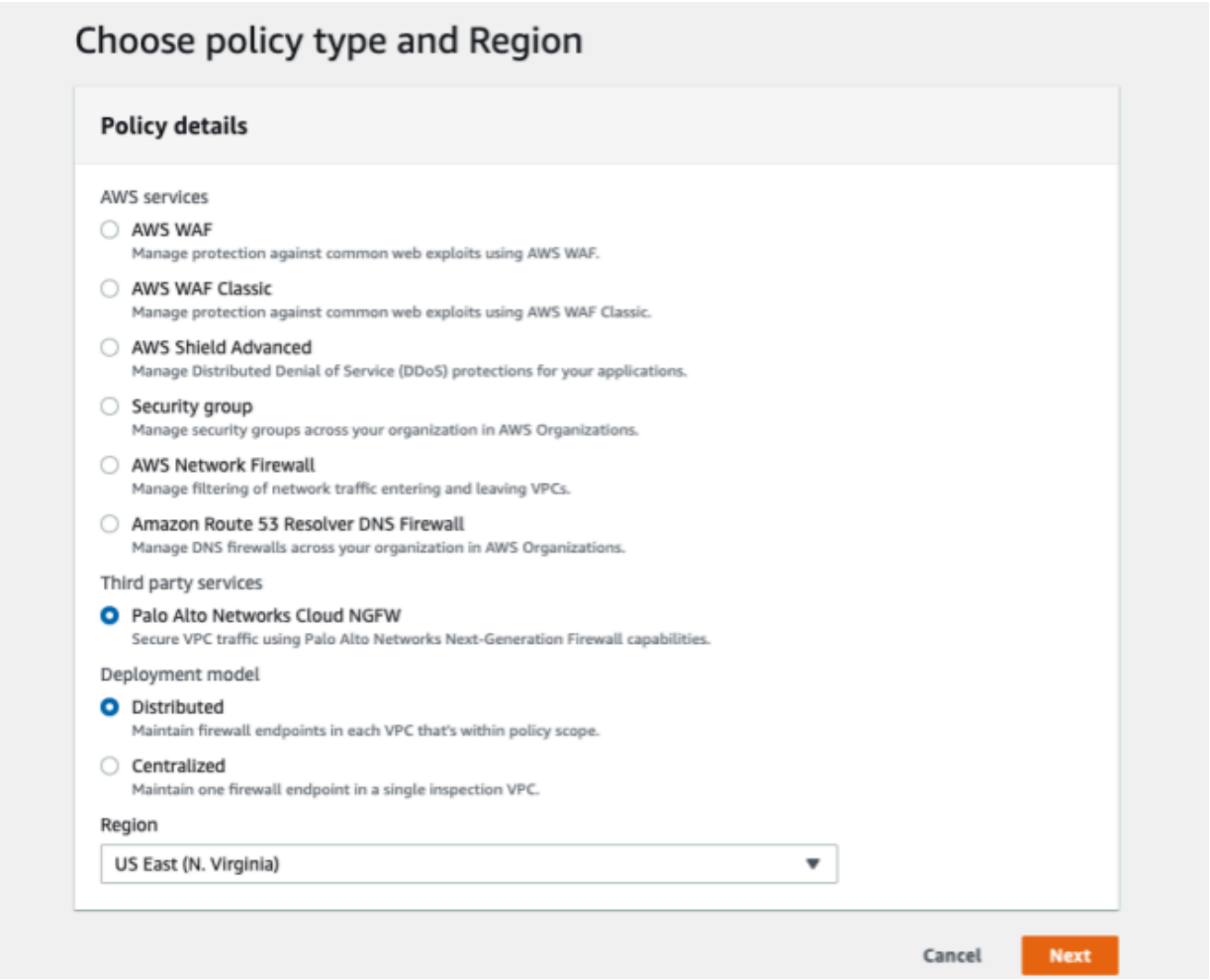
1. Melden Sie sich bei der AWS-Konsole an und wählen Sie **Services (Dienste)** > **AWS Firewall Manager** > **Settings (Einstellungen)** aus.
2. Wählen Sie unter „Third Party Firewall Association Status“ (Verknüpfungsstatus für Firewalls von Drittanbietern) die Option „Palo Alto Networks Cloud NGFW“ aus.
3. Klicken Sie auf **Associate (Verknüpfen)**.

STEP 3 | Wählen Sie **Security Policies (Sicherheitsrichtlinien)** > **Create Policy (Richtlinie erstellen)** aus.

STEP 4 | Wählen Sie den Richtlinientyp und die Region aus.

1. Wählen Sie unter „Third Party Services“ (Dienste von Drittanbietern) die Option **Palo Alto Networks Cloud NGFW** aus.
2. Wählen Sie unter **Deployment Mode (Bereitstellungsmodus)** Ihren Bereitstellungsmodus aus: „Distributed“ (Verteilt) oder „Centralized“ (Zentralisiert).
3. Wählen Sie die **Region** aus.

STEP 5 | Klicken Sie auf **Next (Weiter)**.



STEP 6 | Beschreiben Sie die FMS-Richtlinie für Cloud NGFW für AWS.

Geben Sie einen beschreibenden Namen für Ihre FMS-Richtlinie an, konfigurieren Sie einen globalen Regelstapel oder weisen Sie der FMS-Richtlinie einen globalen Regelstapel zu und konfigurieren Sie Protokolleinstellungen. FMS zeigt alle vorhandenen globalen Regelstapel (falls verfügbar) und einen Link an, der Sie zur Cloud NGFW-Konsole führt, um einen globalen Regelstapel zu erstellen. Da der abonnierende Benutzer (FMS-Administrator) ein Administrator

für den „GlobalRuleStackAdmin“ (globalen Regelstapel) ist, müssen Sie keine Änderungen an den Benutzerrollen vornehmen.

1. Geben Sie einen beschreibenden **Richtliniennamen** ein.
2. Wählen oder erstellen Sie eine **Third Party Firewall Policy Configuration (Richtlinienkonfiguration für Firewalls von Drittanbietern)**.

   In der FMS-Konsole bezieht sich die Richtlinienkonfiguration für Firewalls von Drittanbietern auf einen globalen Regelstapel im Kontext von Cloud NGFW. Wenn Sie bereits einen oder mehrere globale Regelstapel erstellt haben, werden diese hier aufgelistet. Wenn Sie noch keinen globalen Regelstapel erstellt haben, können Sie dies tun, indem Sie auf **Create Firewall Policy (Firewallrichtlinie erstellen)** klicken. Dadurch werden Sie zur Cloud NGFW-Konsole weitergeleitet. Informationen zu Regelstapeln und zur Regelstapelkonfiguration finden Sie unter Informationen zu Regelstapeln und Regeln in Cloud NGFW für AWS.
3. Erstellen Sie einen globalen Regelstapel.

   1. Geben Sie einen beschreibenden **Namen** für Ihren Regelstapel ein.

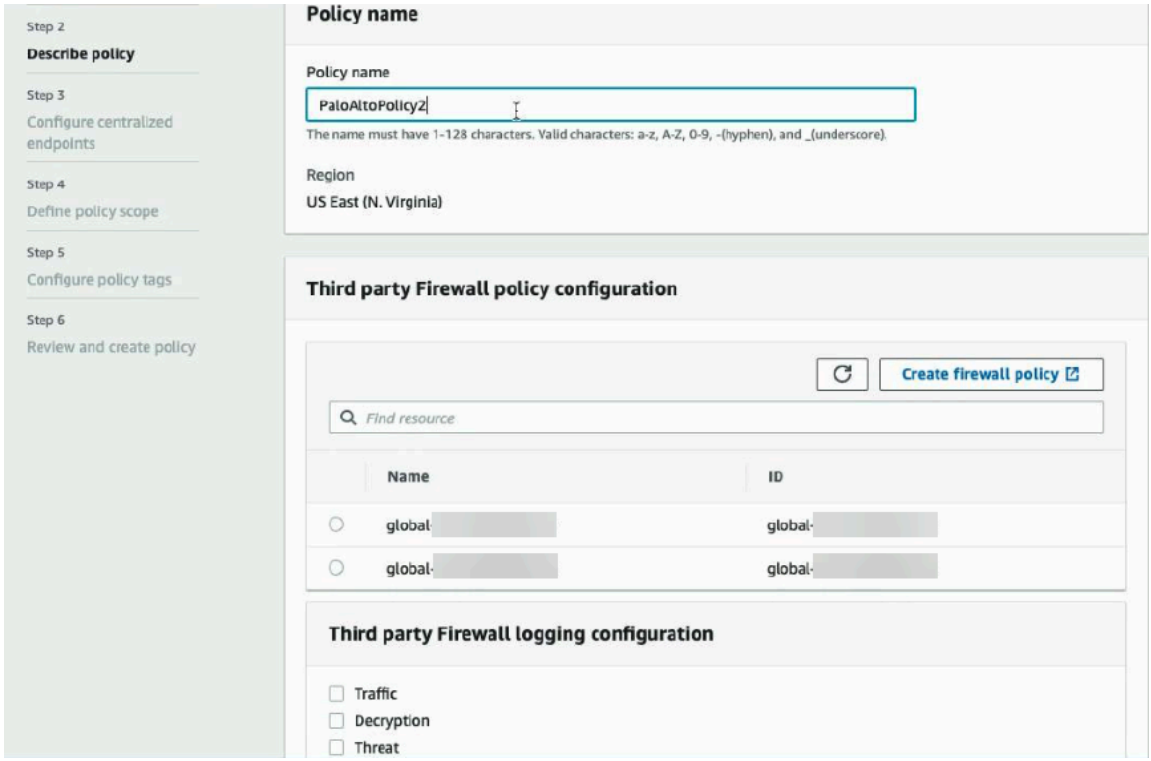
   2. (optional) Geben Sie eine **Beschreibung** für Ihren Regelstapel ein.

   3. Klicken Sie auf **Save (Speichern)**.

   4. Kehren Sie zur FMS-Konsole zurück.
4. Konfigurieren Sie die Protokollierung.

   Sie können Datenverkehr, Entschlüsselung und/oder Threat-Protokolle auswählen. Für jeden Protokolltyp müssen Sie ein Ziel (S3-Bucket, CloudWatch-Protokollgruppe oder Kinesis Firehose-Bereitstellungsstream) aus der Dropdown-Liste angeben. In der Dropdown-Liste werden zuvor konfigurierte Ziele in Ihrer AWS-Umgebung angezeigt.

5. Klicken Sie auf **Next (Weiter)**.



STEP 7 | Konfigurieren Sie NGFW-Endpunkte.

Cloud NGFW erstellt Endpunkte in Ihren Verfügbarkeitszonen, die gesichert werden müssen. Diese NGFW-Endpunkte fangen den Datenverkehr ab und leiten ihn zur Prüfung und Durchsetzung an Cloud NGFW weiter. Anzahl und Speicherort von NGFW-Endpunkten unterscheiden sich je nach Bereitstellungsmodus (verteilt oder zentralisiert).

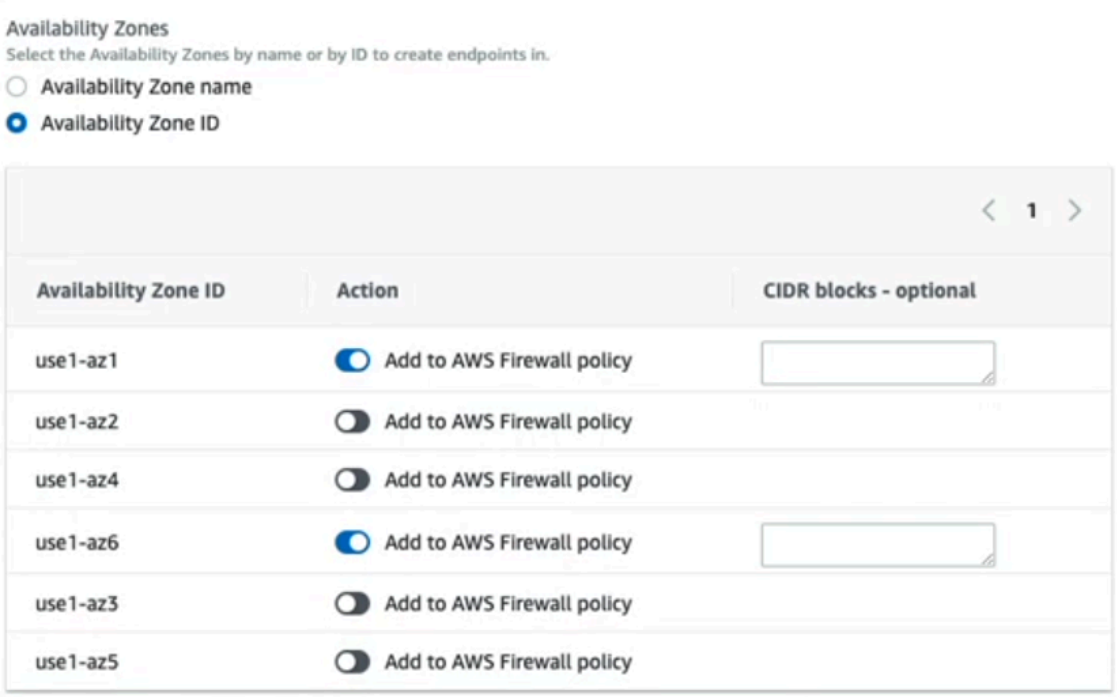
Sie wählen die NGFW-Endpunktstandorte aus, indem Sie Namen oder IDs von Verfügbarkeitszonen festlegen. Beachten Sie, dass die Namen der Verfügbarkeitszonen zwischen AWS-Konten

unterschiedlich sein können, die IDs der Verfügbarkeitszonen jedoch in allen AWS-Konten konsistent sind.

1. Wählen Sie den **Namen der Verfügbarkeitszone** oder die **ID der Verfügbarkeitszone** aus. Diese Auswahl bestimmt, welche Optionen (Namen oder IDs) in der FMS-Konsole aufgelistet sind.
2. Klicken Sie in der Spalte „Action“ (Aktion) auf den Schieberegler, um der FMS-Richtlinie der Cloud NFGW eine Verfügbarkeitszone hinzuzufügen.
3. (optional) Fügen Sie CIDR-Blöcke (Classless Inter-Domain Routing) hinzu, um die von den NGFW-Endpunkten verwendeten Subnetze anzugeben.

   Sie können für jede ausgewählte Verfügbarkeitszone einen CIDR-Block angeben oder eine Liste von CIDR-Blöcken erstellen, die der FMS den ausgewählten Verfügbarkeitszonen zuweisen soll. Jeder CIDR-Block muss ein /28-CIDR-Block sein.

   Wenn Sie keine CIDR-Blöcke angeben, versucht der FMS mit allen Möglichkeiten, nicht zugewiesene CIDR-Blöcke in Ihrer VPC zu finden, damit Subnetze für die NGFW-Endpunkte erstellt werden. Wenn in Ihrer VPC keine CIDR-Blöcke verfügbar sind, zeigt der FMS den Fehler „Nicht konform“ an.
4. Klicken Sie auf **Next (Weiter)**.



STEP 8 | Definieren Sie den Geltungsbereich der FMS-Richtlinie für Cloud NGFW.

Der Geltungsbereich definiert die AWS-Konten oder Organisationseinheiten und Ressourcen, die von der FMS-Richtlinie für Cloud NGFW abgedeckt werden. Sie können die FMS-Richtlinien für Cloud

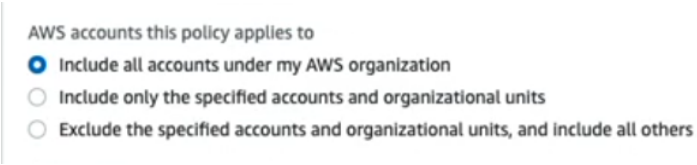
NGFW auf alle AWS-Konten und VPCs in Ihrer Organisation anwenden oder eine Teilmenge von Konten und/oder VPCs angeben.

Wenn Sie Ihrer Organisation ein neues AWS-Konto oder eine neue VPC hinzufügen, bestimmt der FMS, ob Ihre Cloud NGFW-Richtlinie auf dieses Konto bzw. diese VPC angewendet werden soll. Sie können die Cloud NGFW-Richtlinie beispielsweise auf alle Konten mit Ausnahme einer kleinen, ausgeschlossenen Teilmenge anwenden. Wenn ein neues Konto Ihrer Organisation beitritt und es nicht in der Ausschlussliste enthalten ist, wird die Cloud NGFW-Richtlinie angewendet.

1. Geben Sie die Konten an, die in die FMS-Richtlinie für Cloud NGFW eingeschlossen oder ausgeschlossen werden sollen.

   Sie können zwischen den folgenden Optionen wählen: **Include all accounts under my AWS organization (Alle Konten unter meiner AWS-Organisation einschließen)** **Include on the specified accounts and organizational units (Angegebene Konten und Organisationseinheiten einschließen)** oder **Exclude specific accounts and organizational units, and include all others (Bestimmte Konten und Organisationseinheiten ausschließen und alle anderen einschließen)**.

   Wenn Sie eine Teilmenge von Konten und Organisationseinheiten einschließen oder ausschließen, zeigt die FMS-Konsole ein Feld an, in dem Sie diese Konten und Organisationseinheiten angeben können. Klicken Sie auf **Edit List (Liste bearbeiten)**, um Ihre Einschluss- oder Ausschlussliste zu erstellen.

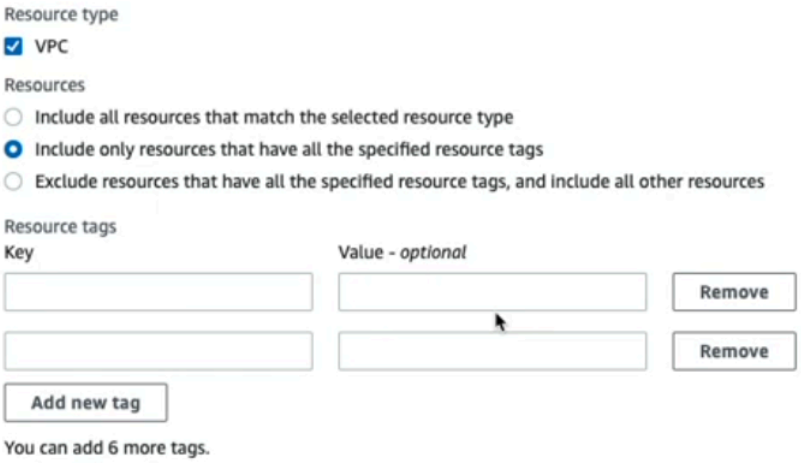
   

2. Geben Sie die VPC an, die in die FMS-Richtlinie für Cloud NGFW eingeschlossen oder ausgeschlossen werden soll.

   Ähnlich wie bei den Konten und Organisationseinheiten haben Sie folgende Auswahlmöglichkeiten: **Include all resources that match the selected type (Alle Ressourcen einschließen, die dem ausgewählten Typ entsprechen)**, **Include only resources that have all the specified resource tags (Nur Ressourcen einschließen, die alle angegebenen Ressourcentags aufweisen)** oder **Exclude resources that have all the specified resource tags,**

and include all others (Ressourcen ausschließen, die alle angegebenen Ressourcentags aufweisen, und alle anderen einschließen).

Wenn Sie eine Teilmenge von VPCs einschließen oder ausschließen, zeigt die FMS-Konsole Optionen für eine Liste von bis zu acht Ressourcentags und Werten an.



3. Unter **Third Party Firewall Customer IAM Role (IAM-Rolle für Kunden einer Firewall von Drittanbietern)** können Sie eine Kopie der CloudFormation-Vorlage (CFT) für IAM-Rollen in Cloud NGFW herunterladen.
4. Klicken Sie auf **Next (Weiter)**.
5. (optional) Konfigurieren Sie Richtlinientags.

   Sie können Tags (bestehend aus einem Schlüssel und einem optionalen Wert) anwenden, um das Suchen und Filtern Ihrer über den FMS erstellten Cloud NGFW-Ressource zu erleichtern.
6. Klicken Sie auf **Next (Weiter)**.
7. Überprüfen Sie die Konfiguration Ihrer Cloud NGFW-Richtlinie.
8. Klicken Sie auf **Create Policy (Richtlinie erstellen)**, um Cloud NGFW bereitzustellen.

Programmgesteuerten Zugriff aktivieren

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.

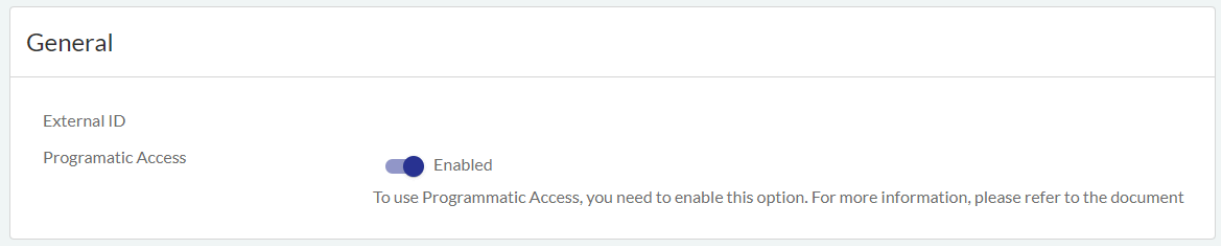
Da der programmgesteuerte Zugriff sehr effektiv ist, stellt Cloud NGFW keinen weiteren Zugriffsschlüssel oder geheimen Schlüssel zum Signieren von Autorisierungsanforderungen bereit. Stattdessen können Sie die IAM-Rolle in Ihrem AWS-Konto verwenden, um auf die Cloud NGFW-APIs zuzugreifen, und dann konfigurieren, 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

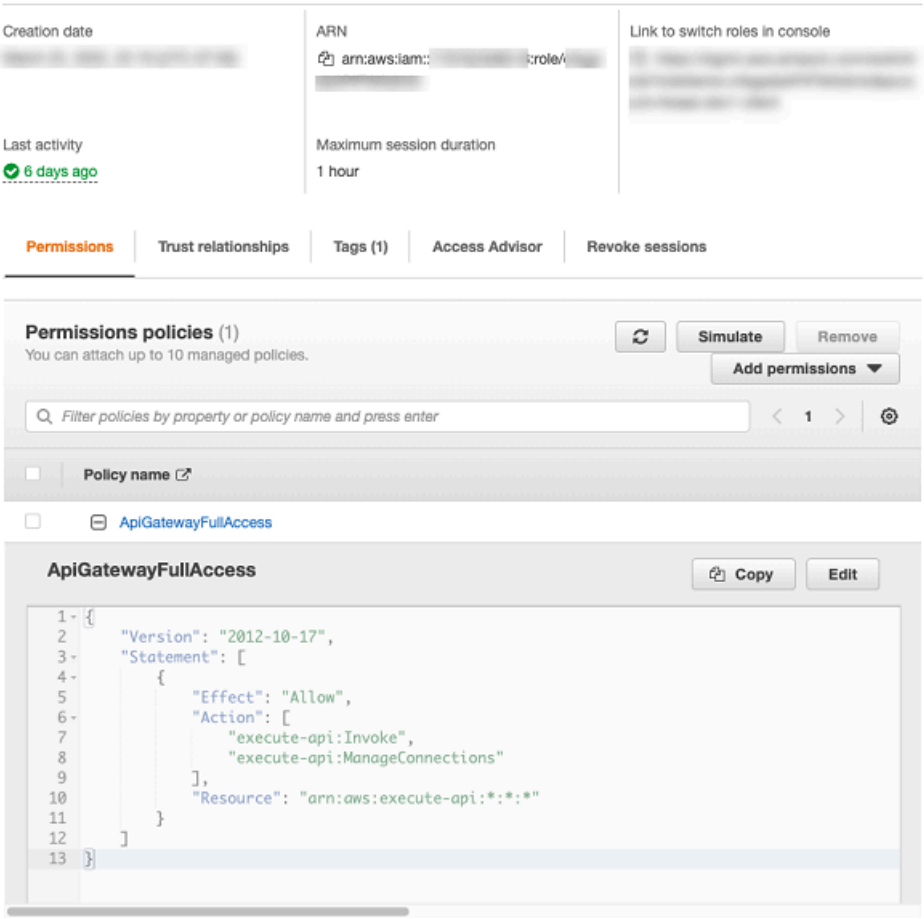
- Wählen Sie in der **Cloud NGFW Tenant (Cloud NGFW-Mandanten)**-Konsole die Option **Tenant (Mandant)** aus.
- Klicken Sie unter **General (Allgemein)** auf den Schieberegler **Programmatic Access (Programmgesteuerter Zugriff)**.
- Klicken Sie zur Bestätigung auf **Enable (Aktivieren)**.



STEP 2 | Melden Sie sich bei der AWS Management Console an und erstellen Sie eine IAM-Rolle.

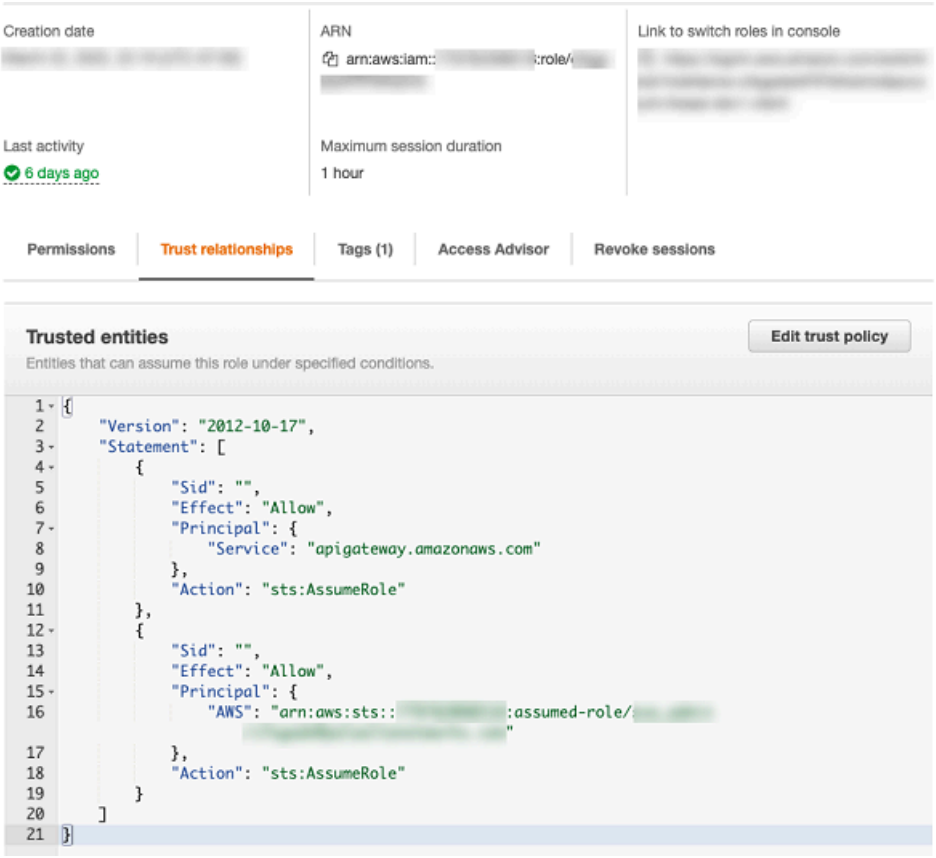
Nachfolgend ist die Berechtigungsrichtlinie aufgeführt, die zum Aktivieren des vollständigen Zugriffs auf das API-Gateway erforderlich ist.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Action": "execute-api:Invoke", "Resource": "arn:aws:execute-
api:*:*:*" } ] }
```



STEP 3 | Aktivieren Sie die Berechtigung für das API-Gateway zum Aufrufen von APIs.

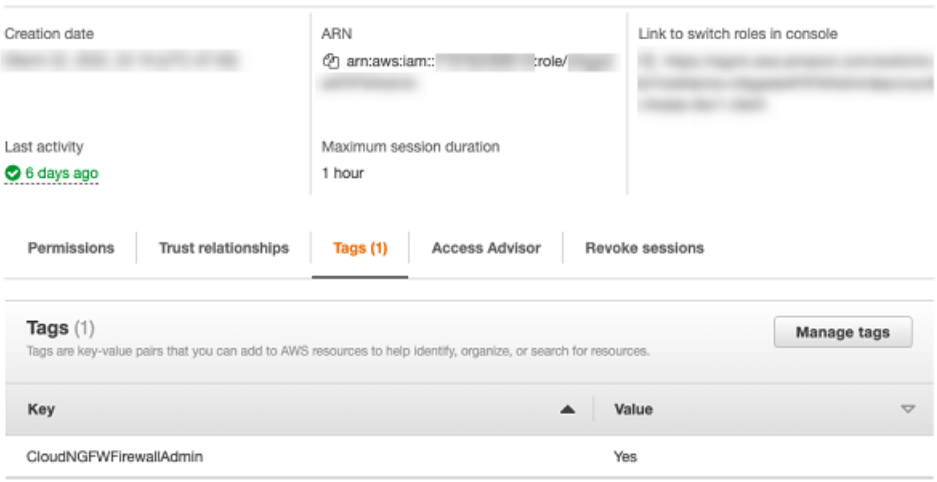
Übernehmen Sie Rollen unter den in den Vertrauensbeziehungen genannten Bedingungen.



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
Erstellen und Verwalten globaler Regelstapel	**`CloudNGFWGlobalRulestackAdmin`**	Ja

Verwendung	TagKey	TagValue
AWS-Konto einbinden	`CloudNGFWGAccountAdmin`	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

Hashicorp Terraform ist ein Open-Source-Infrastructure-as-Code (IaC)-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 Plugins interagieren mit den Providern wie AWS, um die Wiederverwendung zu erleichtern, indem sie wiederholbare Schritte für den Aufbau und die Wartung der Cloud-Infrastruktur erstellen und so einfache Ergänzungen zu Ihrer CI/CD-Pipeline gewährleisten.

Palo Alto Networks fügt den Provider „cloudngfwaws“ hinzu, um den Aufbau der Sicherheitsinfrastruktur zu automatisieren und die Netzwerksicherheit 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 in AWS mit Terraform zu erfahren und die Terraform-Referenzinformationen anzuzeigen.

Sie können den Terraform-Provider in Ihrer Konfiguration für Folgendes 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: Terraform-Provider 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 config file:

```
{ "host": "api.us-east-1.aws.cloudngfw.paloaltonetworks.com",
 "region": "us-east-1", "arn": "arn:aws:iam::123456789:role/MyRole" }
```


Cloud NGFW-Ressourcen für Ihre AWS CFT bereitstellen

Die Cloud NGFW bietet Flexibilität bei der Bereitstellung von Ressourcen für Ihre AWS CloudFormation-Vorlage (CFT), indem Sie Ihre eigenen Ressourcen erstellen können.

Sie müssen den programmatischen Zugriff aktivieren, bevor Sie CloudFormation Registry mit der Cloud NGFW verwenden können.

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.
	JSON
	`„RuleStackName“: String,`
	YAML
	`RuleStackName: String`

RuleStack	Geben Sie eine **Beschreibung** für Ihren Regelstapel ein. Die Beschreibung beinhaltet: **JSON** `{ "Scope" : String, "Profiles" : RuleStackProfiles, "Description" : String "Deploy" : String }`

Element	Beschreibung
	YAML `Scope: String Profiles: RuleStackProfiles Description: String Deploy: String`

RuleStackProfiles	Geben Sie **Profile** für den angegebenen Regelstapel an. Profile beinhalten:
	JSON
	`{ "AntiSpywareProfile" : String, "AntiVirusProfile" : String, "VulnerabilityProfile" : String, "URLFilteringProfile" : String, "FileBlockingProfile" : String, "OutboundTrustCertificate" : String, "OutboundUntrustCertificate" : String }`
	YAML
	`AntiSpywareProfile: String AntiVirusProfile: String VulnerabilityProfile: String URLFilteringProfile: String FileBlockingProfile: String OutboundTrustCertificate: String OutboundUntrustCertificate: String`

Regel	Richten Sie **Regeln** für den Regelstapel ein. Regeln beinhalten: **JSON** `{ "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, ...] }` **YAML** `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`

Element	Beschreibung

RuleSource	Legen Sie die Sammlung von Regeln mithilfe von **RuleSource** fest. RuleSource beinhaltet:
	
	JSON
	`{ "Cidrs" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }`
	
	YAML
	`cidrs: - String PrefixLists: - String Countries: - String Feeds: - String`

RuleDestination	Legen Sie **RuleDestination** für den Webdienst fest, der die Bestätigungs-URL und eine oder mehrere Datenerfassungs-URLs unterstützt. RuleDestination beinhaltet:
	
	JSON
	`{ "Cidrs" : [ String, ... ], "FqdnLists" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }`
	
	YAML
	`Cidrs: - String FqdnLists: - String PrefixLists: - String Countries: - String Feeds: - String`

Tag	Geben Sie ein **Tag** für den Regelstapel an. Ein Tag beinhaltet:
	
	JSON
	`{ "Key" : String, "Value" : String }`
	
	YAML
	`Key: String Value: String`

UrlCategory	Verwenden Sie **UrlCategory**, um Kriterien in Authentifizierungs-, Entschlüsselungs-, QoS- und Sicherheitsrichtlinienregeln abzugleichen. UrlCategory beinhaltet: **JSON** `{ "URLCategoryNames" : [ String, ... ], "Feeds" : [ String, ... ] }`

Element	Beschreibung
	YAML `URLCategoryNames: - String Feeds: - String`

SecurityObjects	Legen Sie die **SecurityObjects** für den Regelstapel fest. SecurityObjects beinhalten:
	JSON
	`{ "PrefixList" : PrefixList, "FqdnLists" : FqdnList, "CustomUrlCategories" : CustomUrlCategory, "IntelligentFeeds" : IntelligentFeed, "CertificateLists" : CertificateList }`
	YAML
	`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:
	JSON
	`{ "FileBlocking" : FileBlocking }`
	YAML
	`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: **JSON** `{ "Name" : String, "PrefixList" : [ String, ... ], "AuditComment" : String, "Description" : String }`

Element	Beschreibung
	YAML `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:
	JSON
	`{ "Name" : String, "Description" : String, "FqdnList" : [ String, ... ], "AuditComment" : String }`
	YAML
	`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: • 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. • 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. CustomURLCategories beinhalten: **JSON** `{ "URLTargets" : [ String, ... ], "Name" : String, "Description" : String, "Action" : String, "AuditComment" : String }`

Element	Beschreibung
	YAML `URLTargets: - String Name: String Description: String Action: String AuditComment: String`

IntelligentFeeds	Verwenden Sie **IntelligentFeeds**, um die aktuellsten Bedrohungsdaten kontinuierlich bereitzustellen. IntelligentFeeds beinhalten:
	JSON
	`{ "Name" : String, "Description" : String, "Certificate" : String, "FeedURL" : String, "Type" : String, "Frequency" : String, "Time" : Integer, "AuditComment" : String }`
	YAML
	`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:
	JSON
	`{ "Name" : String, "Description" : String, "CertificateSignerArn" : String, "CertificateSelfSigned" : Boolean, "AuditComment" : String }`
	YAML
	`Name: String Description: String CertificateSignerArn: String 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/Download haben. FileBlocking beinhaltet:

Element	Beschreibung

	JSON
	`{ "Direction" : String, "FileType" : String, "Description" : String, "Action" : String, "AuditComment" : String }`
	YAML
	`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

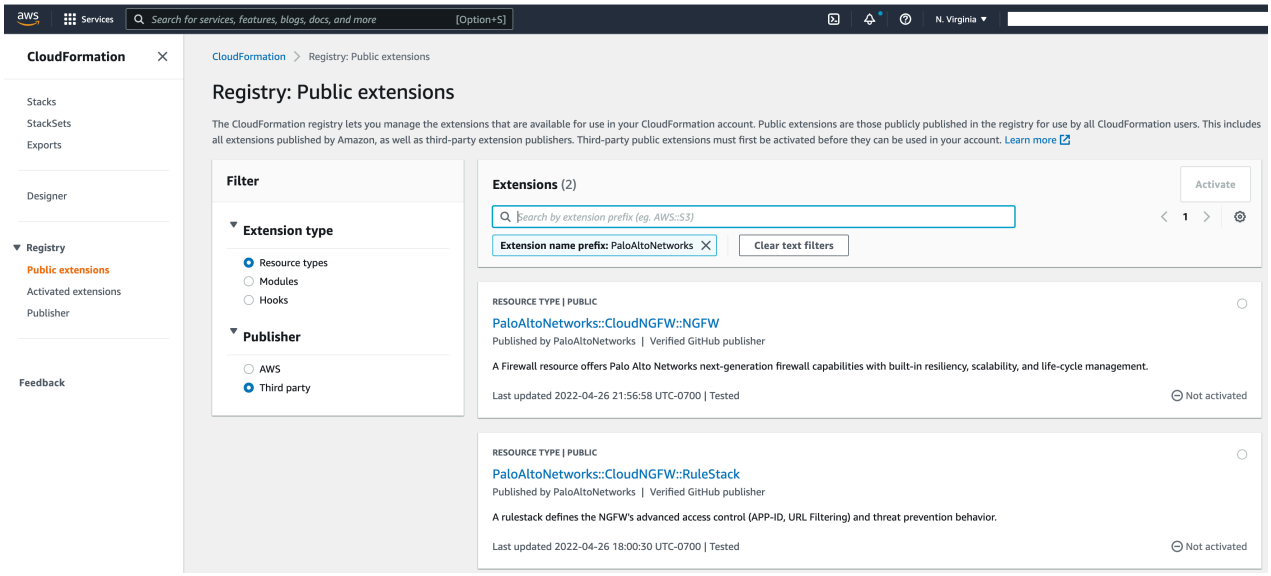
```
Type: PaloAltoNetworks::CloudNGFW::NGFWProperties: AppIdVersion:
 String AutomaticUpgradeAppIdVersion: Boolean Description:
 String EndpointMode: String FirewallName: String RuleStackName:
 String RuleStackName: String SubnetMappings: - String Tags: -
 Map VpcId: String UpdateToken: String LogDestinationConfigs:
 - LogProfileConfig CloudWatchMetricNamespace: String
 ProgrammaticAccessToken: String
```

Element	Beschreibung

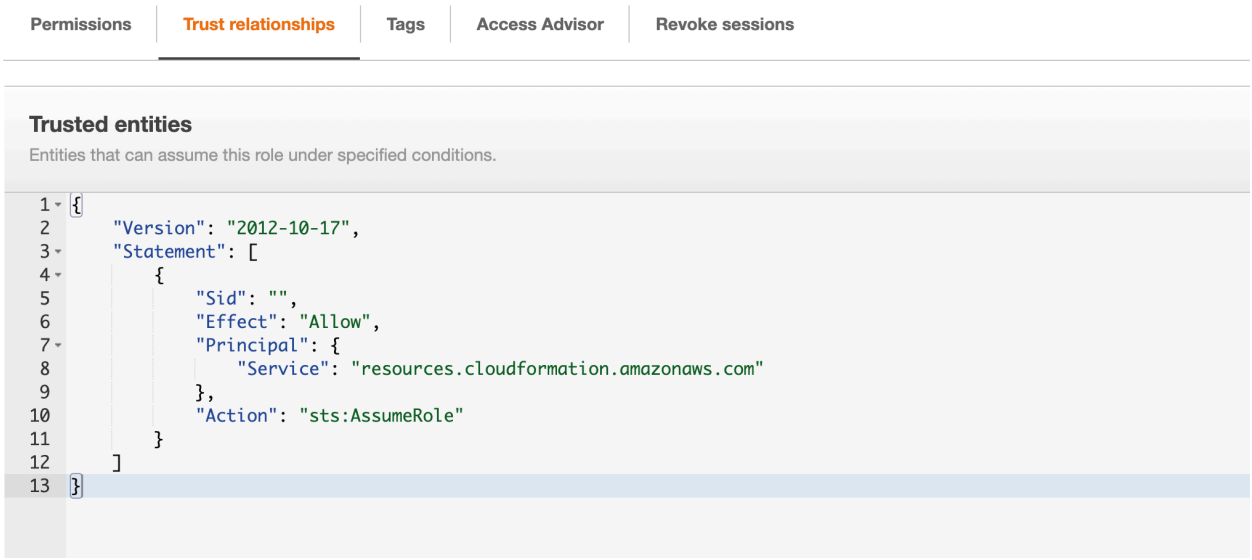
LogProfileConfig	Verwenden Sie **LogProfileConfig**, um Einträge für Änderungen an der Firewall-Konfiguration anzuzeigen.
	JSON
	`{ "LogDestination" : String, "LogDestinationType" : String, "LogType" : String}`
	YAML
	`LogDestination: String LogDestinationType: String LogType: String`

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 Cloud Formation-Vorlagen zu verwenden:



Aktivieren Sie nach dem Einrichten der Vertrauensbeziehung die Erweiterungen:

Um Protokolle in AWS CloudWatch zu versenden, konfigurieren Sie die Protokollierung (siehe Protokollierung in Cloud NGFW für AWS konfigurieren).

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" ] } } }
```


Automatisierte Einbindung von Konten konfigurieren

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.
- Um die Funktion für die automatisierte Einbindung von Konten verwenden zu können, müssen Sie lediglich ein Konto manuell einbinden.

> *Sie müssen eine Rolle mit Anwendungsberechtigungen der CloudFormation-Vorlage (CloudFormation Template, CFT) in jedem der Konten erstellen, das Sie einbinden möchten.*

Eine aktualisierte Terraform-Vorlage wird zum Aufrufen der LinkAccount-API verwendet, die Parameter abruft, die zum Erstellen von Rollen-ARNs [für Ihre eingebundenen AWS-Konten] verwendet werden. Die Terraform-Vorlage greift auf die API zu, indem sie über programmgesteuerten Zugriff verfügbar gemacht wird, was die Erstellung einer neuen Rolle erfordert: **AccountAdmin**.

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. Weitere Informationen finden Sie unter Programmgesteuerten Zugriff aktivieren.

> *Die von der Vorlage bereitgestellten Aspekte der Rollenerstellung sind identisch. Sie wurde jedoch so geändert, dass sie die Ressourcen und Rollen zur Unterstützung der automatisierten Einbindung von Konten einschließt.*

So konfigurieren Sie die automatisierte Einbindung von Konten:

STEP 1 | Erstellen Sie für alle derzeit eingebundenen Konten die Rolle **AccountAdmin** für den programmgesteuerten Zugriff.

STEP 2 | Erstellen Sie eine Rolle zum Ausführen der CloudFormation-Vorlage (CloudFormation Template, CFT) zur kontoübergreifenden Rolleneinrichtung in jedem Konto, das Sie einbinden möchten. Die Rolle muss das folgende Vertrauensverhältnis aufweisen:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::018147215560:user/sosrinath"
},
"Action": "sts:AssumeRole"
}
]
}
```

Für die Rolle sollte folgende **Berechtigungsrichtlinie** definiert sein, die die Option „Create Inline policy“ (Inline-Richtlinie erstellen) in IAM verwendet:

```
{
"Version": "2012-10-17",
"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"
}
]
}
```

STEP 3 | Verwenden Sie den Terraform-Provider **cloudngfwaws**, um auf Ressourcen zur Verwaltung von Cloud NGFW für AWS zuzugreifen. Die CFT-Rolle, die im vorherigen Schritt erstellt wurde, sollte als Wert der Variablen „cft_role_name“ in der Modulschemadefinition **account_onboarding** angegeben werden.

STEP 4 | 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.

Eingebundenes Konto löschen

Verwenden Sie Terraform **destroy**. Weitere Informationen hierzu finden Sie in der Terraform-Dokumentation.

Auflisten eines eingebundenen Kontos

Verwenden Sie Terraform **list**. Weitere Informationen hierzu finden Sie in der Terraform-Dokumentation.

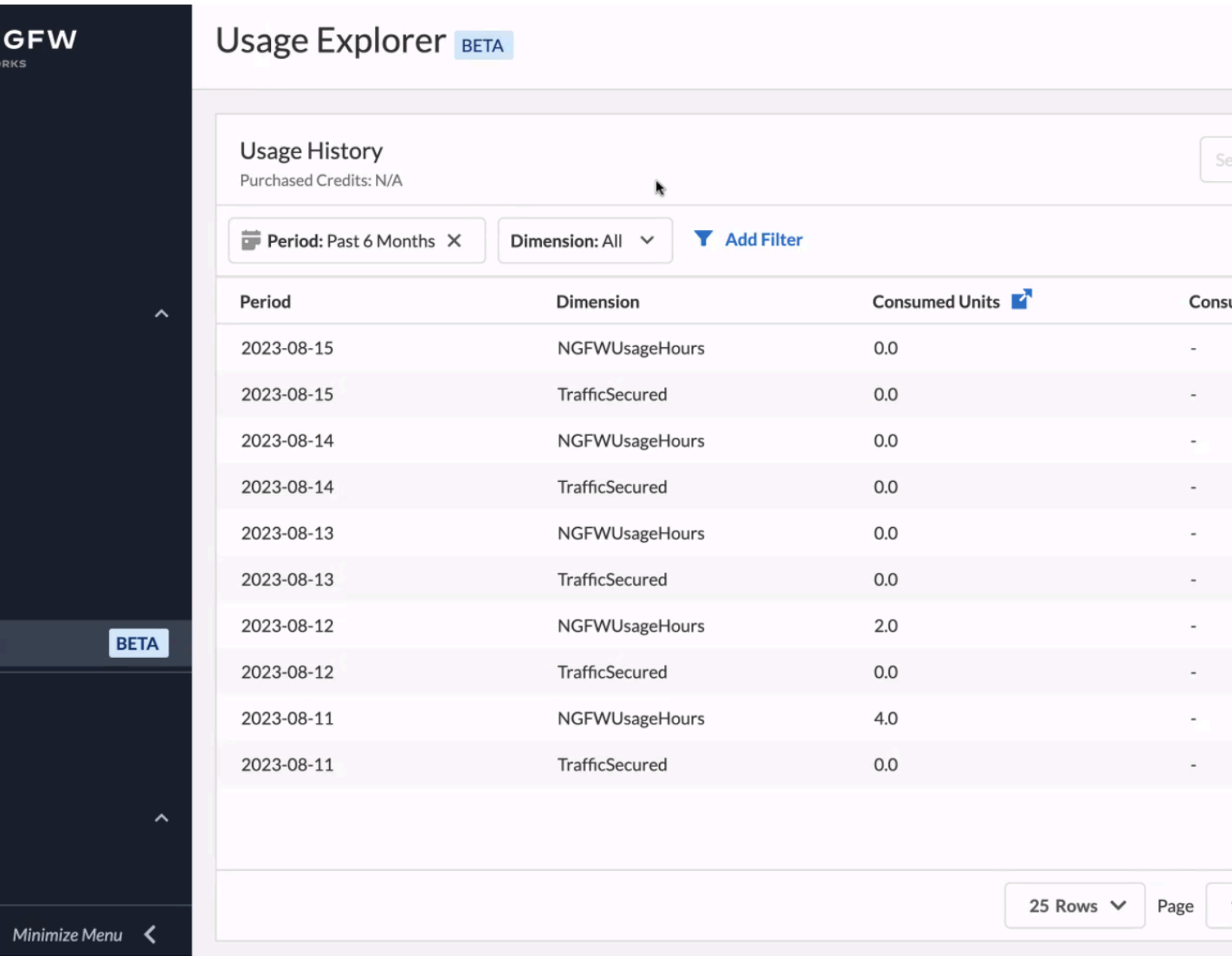
Usage Explorer

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. Wähle Sie in der Konsole die Option **Usage Explorer** aus.



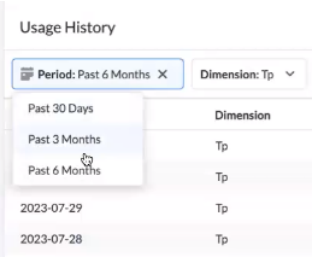
Der Usage Explorer enthält Optionen zum Anzeigen des Verbrauchs über einen bestimmten Zeitraum und ermöglicht es Ihnen, eine CSV-Datei herunterzuladen, um relevante Daten für zukünftige Überprüfungen zu erfassen. Der tägliche Verbrauchsverlauf wird in einer Tabelle bereitgestellt, die die folgenden Felder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

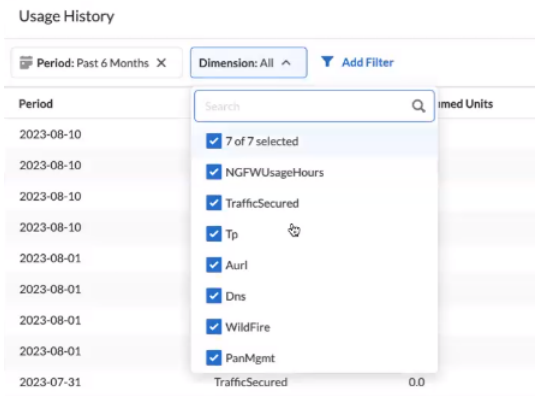
*Sie können nur nach unterstützten Dimensionen filtern. Die Option **Add filter (Filter hinzufügen)** funktioniert derzeit nicht in dieser Vorschauversion.*

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:

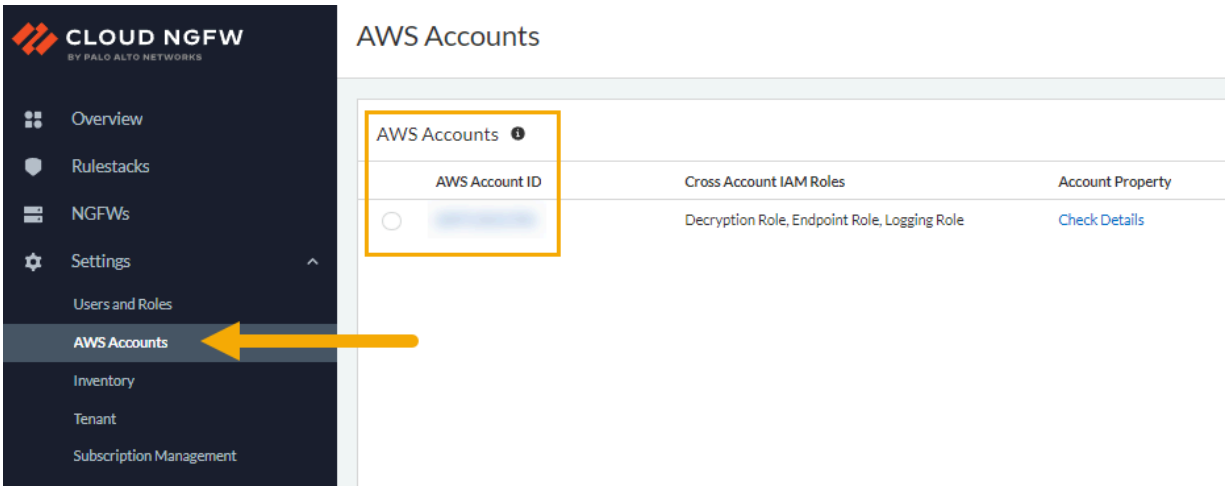


Die Anzeige von Usage Explorer unterscheidet sich je nach Modell des Cloud NGFW-Mandantenabonnements (entweder PAYG oder als Vertrag).

Supportfall erstellen

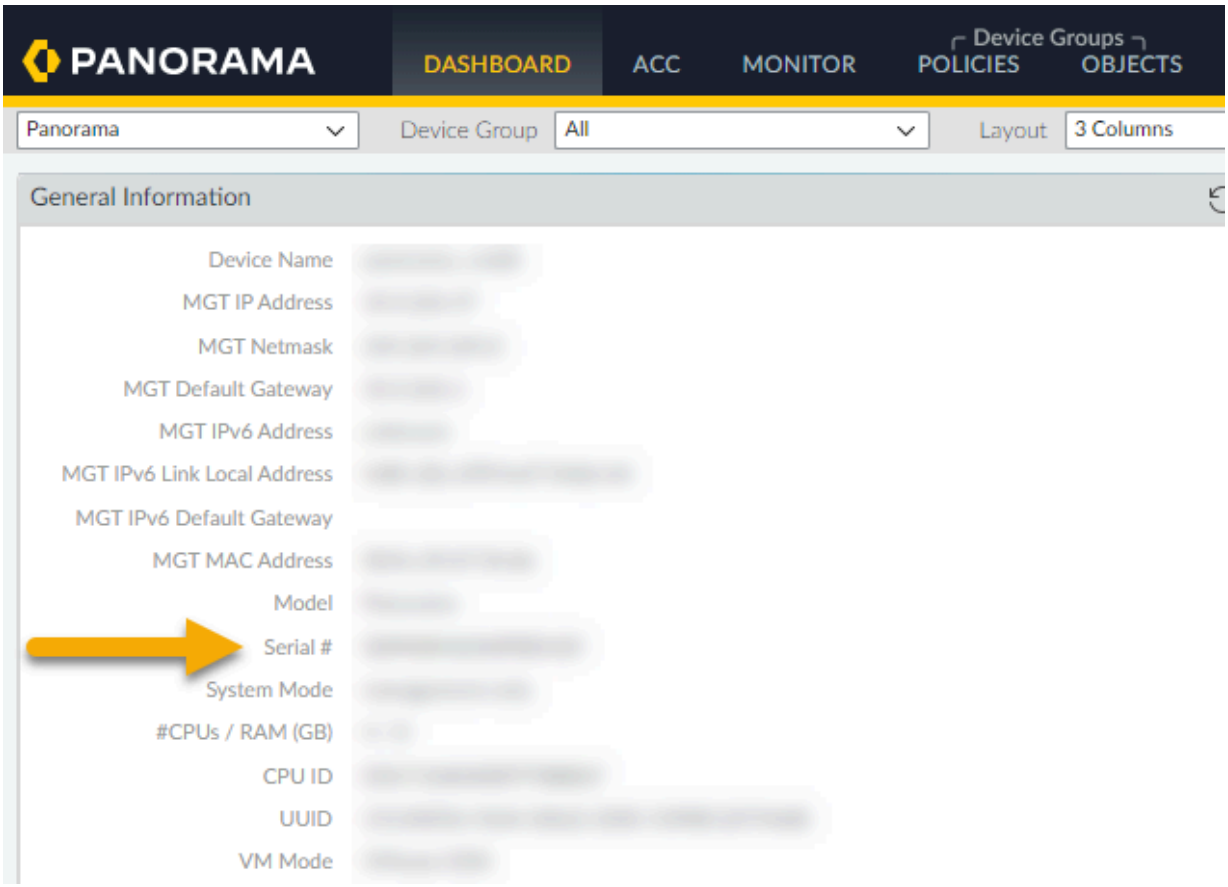
So erstellen Sie einen Supportfall mithilfe der Cloud NGFW-Konsole:

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

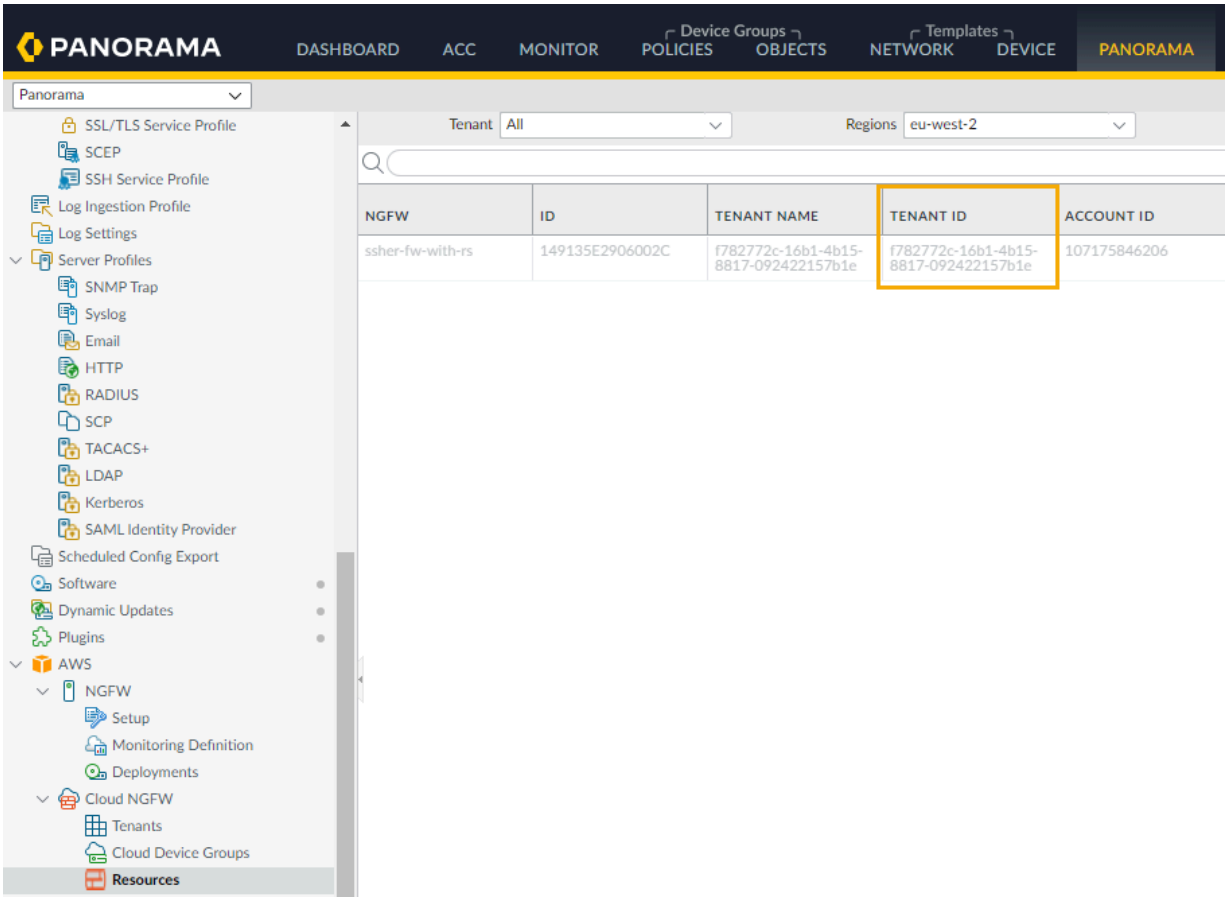


STEP 2 | Verwenden Sie bei Bedarf die Panorama-Konsole, um zusätzliche Informationen für den Supportfall zu ermitteln, beispielsweise die Mandanten-ID oder die Panorama-Seriennummer.

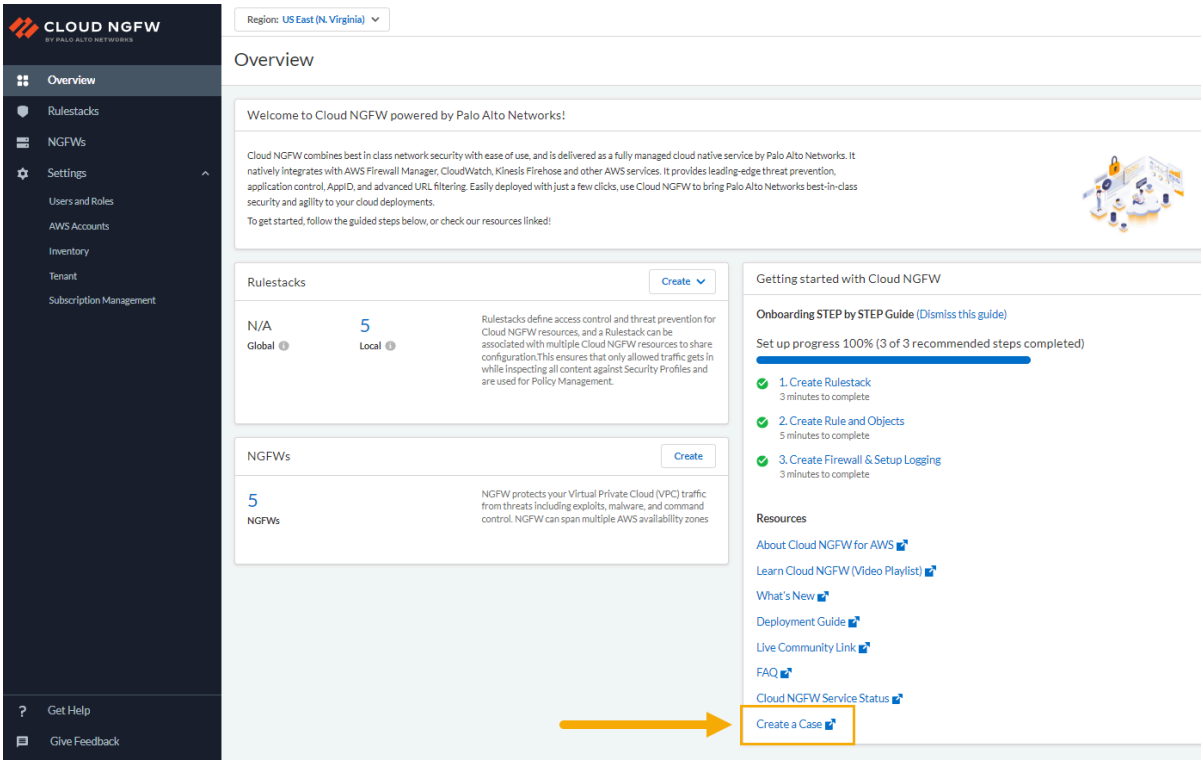
Suchen Sie die **Panorama-Seriennummer** mithilfe des **Dashboards**:



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)**.



Regelstapel und Regeln in Cloud NGFW für AWS

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

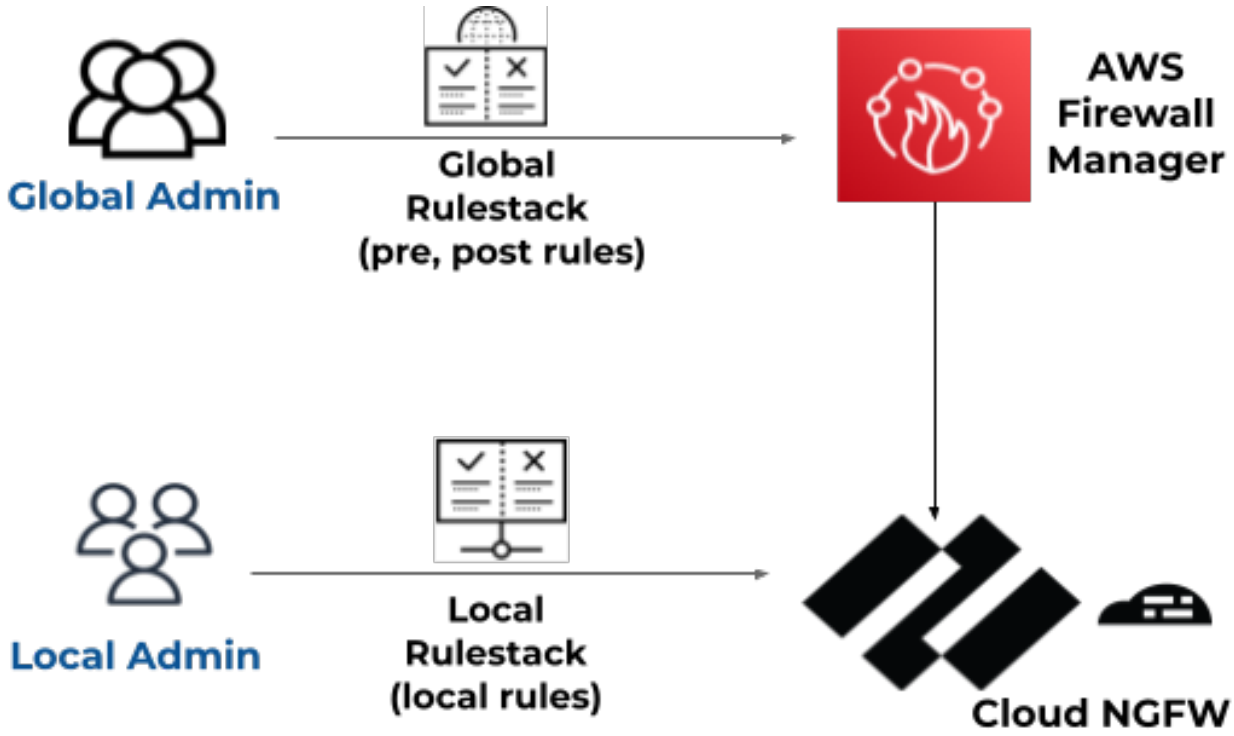
Die Cloud NGFW-Mandantenkonsole unterstützt nur die Erstellung lokaler Regelstapel.

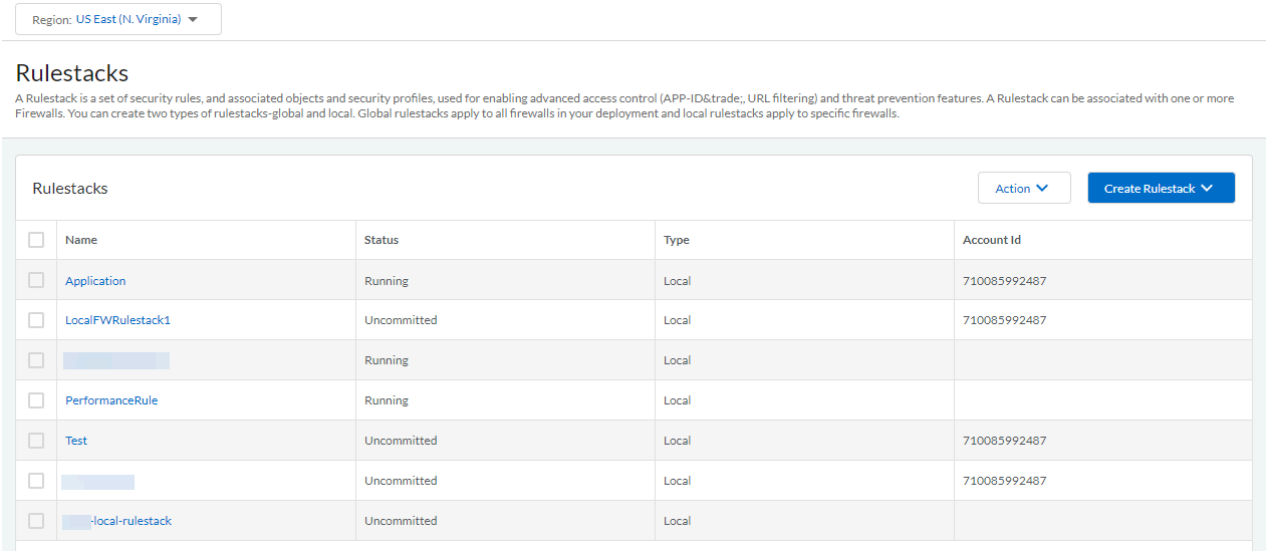
Informationen zu Regelstapeln und Regeln in Cloud NGFW für AWS

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 ihr einen globalen Regelstapel zuordnen. 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 und zuerst ausgewertet werden.
  - **Nach-Regeln**: Regeln, die am Ende der Regelreihenfolge hinzugefügt und nach den Vor-Regeln und den in einem lokalen Regelstapel definierten Regeln ausgewertet werden. Dieser Regelstapel wird auf eine einzelne NGFW angewendet.

Wenn Sie 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 kann ein globaler Regelstapel und ein lokaler Regelstapel angewendet werden.

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 dem Regelstapel zugeordnet ist. Alle Änderungen am Regelstapel müssen von einem Benutzer mit LRA-Berechtigungen im Regelstapel-Konto vorgenommen werden.

Zertifikate von jedem eingebundenen Konto können einem Regelstapel zugeordnet werden.

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

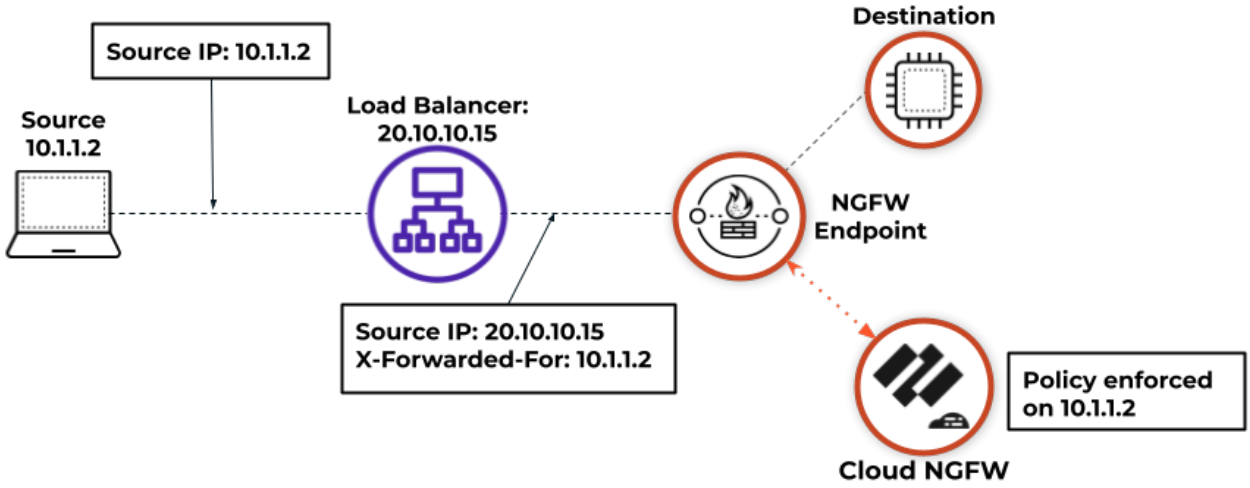
- Regelstapel in Cloud NGFW für AWS erstellen
- Sicherheitsprofile in Cloud NGFW für AWS
- Sicherheitsregelobjekte in Cloud NGFW für AWS
- Sicherheitsregeln in Cloud NGFW für AWS erstellen

X-Forwarded-For in Cloud NGFW für AWS

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.



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. Der Regelstapel wird nur auf NGFWs angewendet, die diesem AWS-Konto zugeordnet 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.

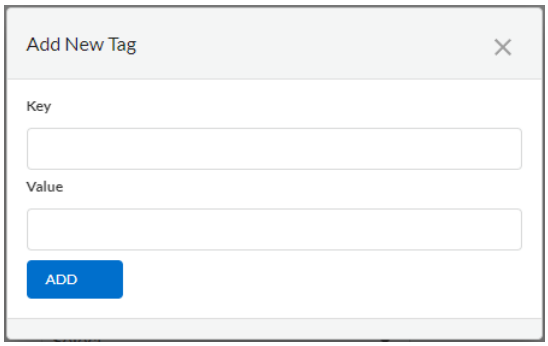
STEP 3 | Geben Sie einen beschreibenden **Namen** für Ihren Regelstapel ein.

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.

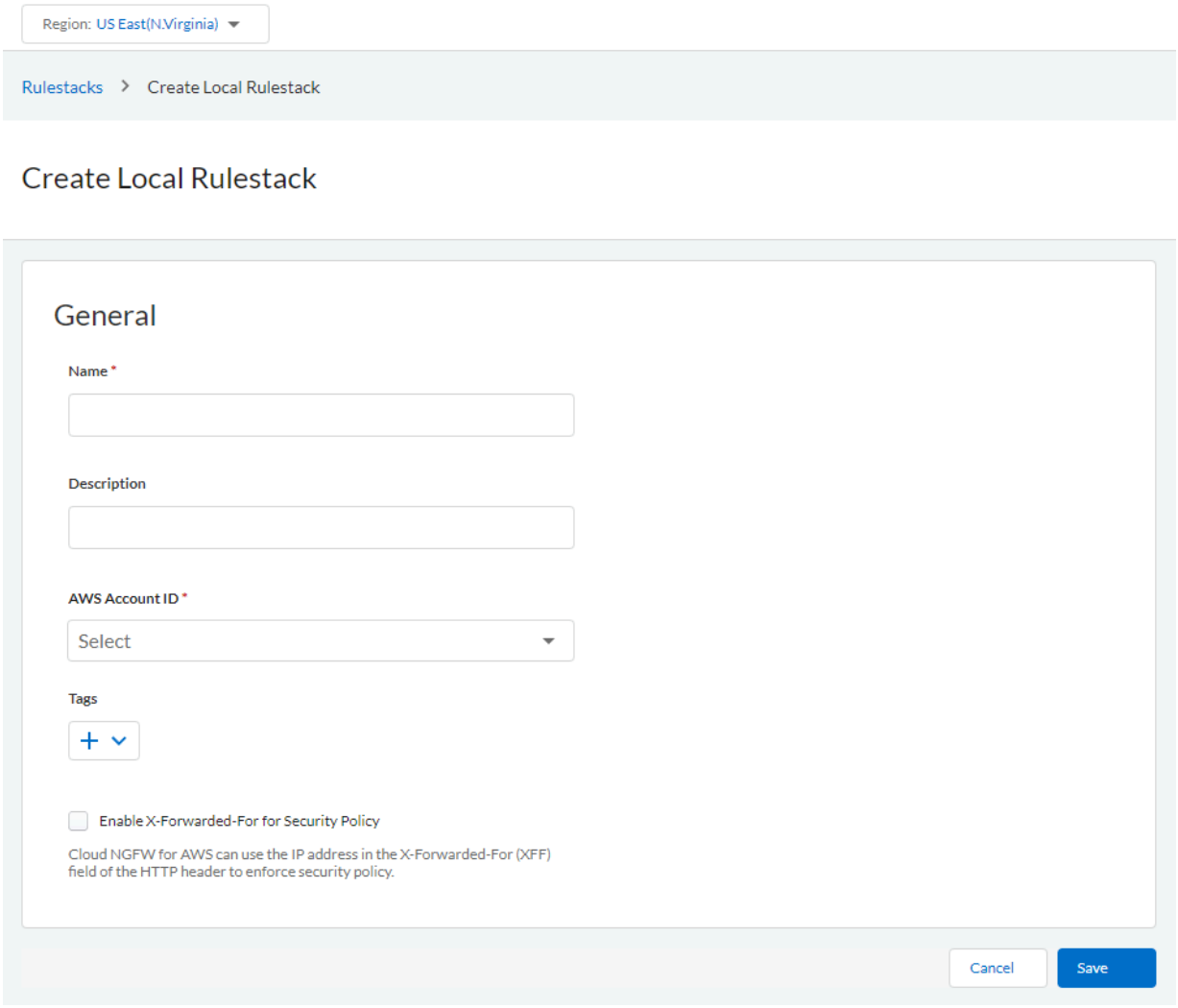
1. Klicken Sie auf das Symbol + und wählen Sie **Add New (Neu hinzufügen)** aus.
2. Geben Sie einen **Schlüssel** und einen **Wert** ein.
3. Klicken Sie auf **Add (Hinzufügen)**.



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

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

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



Sicherheitsregelobjekte in Cloud NGFW für AWS

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.

- **Präfix-** und **FQDN-Listen**: Mit Präfix- und FQDN-Listen können Sie bestimmte Quell- oder Ziel-IP-Adressen oder FQDNs gruppieren, die dieselbe Richtliniendurchsetzung benötigen. 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. 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.
- **Benutzerdefinierte URL-Kategorie**: Mit einer benutzerdefinierten URL-Kategorie können Sie Ausnahmen für die Durchsetzung einer URL-Kategorie angeben und eine benutzerdefinierte URL-Kategorie basierend auf mehreren vorhandenen Kategorien erstellen.
- **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 unten beschrieben wird.

- **Zertifikat**: Ein Zertifikatsobjekt ist ein Verweis auf ein TLS-Zertifikat, das im AWS Secrets Manager in Ihrem AWS-Konto gespeichert ist.

Präfixliste in Cloud NGFW für AWS erstellen

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)**.

FQDN-Liste in Cloud NGFW für AWS erstellen

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)**.

Benutzerdefinierte URL-Kategorie in Cloud NGFW für AWS erstellen

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. Beispiel: • **`*.paloaltonetworks.com`** stimmt mit www.paloaltonetworks.com und www.paloaltonetworks.com.uk überein. • **`*.paloaltonetworks.com/`** stimmt mit www.paloaltonetworks.com überein, aber nicht mit www.paloaltonetworks.com.uk.
^	Verwenden Sie dieses Zeichen, um eine variable Unterdomäne anzugeben. Beispiel: **`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 support.tools.company.com tools.company.com docs.company.com
^.company.com	tools.company.com docs.company.com
^.^.company.com	eng.tools.company.com support.tools.company.com
Beispielsatz 2	
mail.google.*	mail.google.com mail.google.co.uk mail.google.example.org
mail.google.^	mail.google.com mail.google.info
mail.google.^.^	mail.google.co.uk mail.google.example.info
Beispielsatz 3	
site.*.com	site.yourname.com site.abc.xyz.com
site.^.com	site.company.com site.example.com
site.^.^.com	site.a.b.com
site.com/*	site.com/photos site.com/blog/latest beliebiges Unterverzeichnis von site.com

Intelligenten Feed in Cloud NGFW für AWS konfigurieren

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.

- **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 Benutzerdefinierte URL-Kategorie in Cloud NGFW für AWS erstellen.

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)**.

Zertifikat zu Cloud NGFW für AWS hinzufügen

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

- Zertifikat als Schlüssel/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**.
- Sie müssen das CA-Stammzertifikat und das/die CA-Zwischenzertifikat(e) in den Truststore des Clients importieren.
- 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-----
```

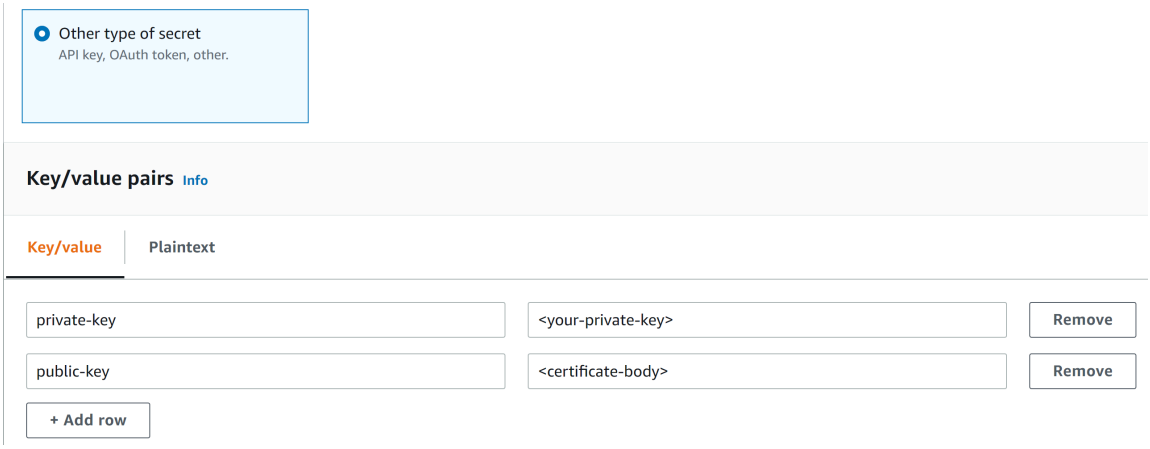
Nicht unterstütztes PKCS1-Format:

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

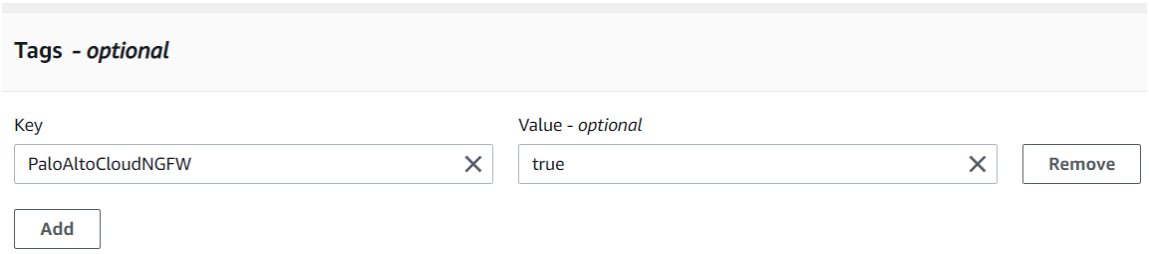
Führen Sie die folgenden Schritte aus, um ein Zertifikat hinzuzufügen, das mit Cloud NGFW für AWS verwendet werden soll.

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/value pairs (Schlüssel/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.

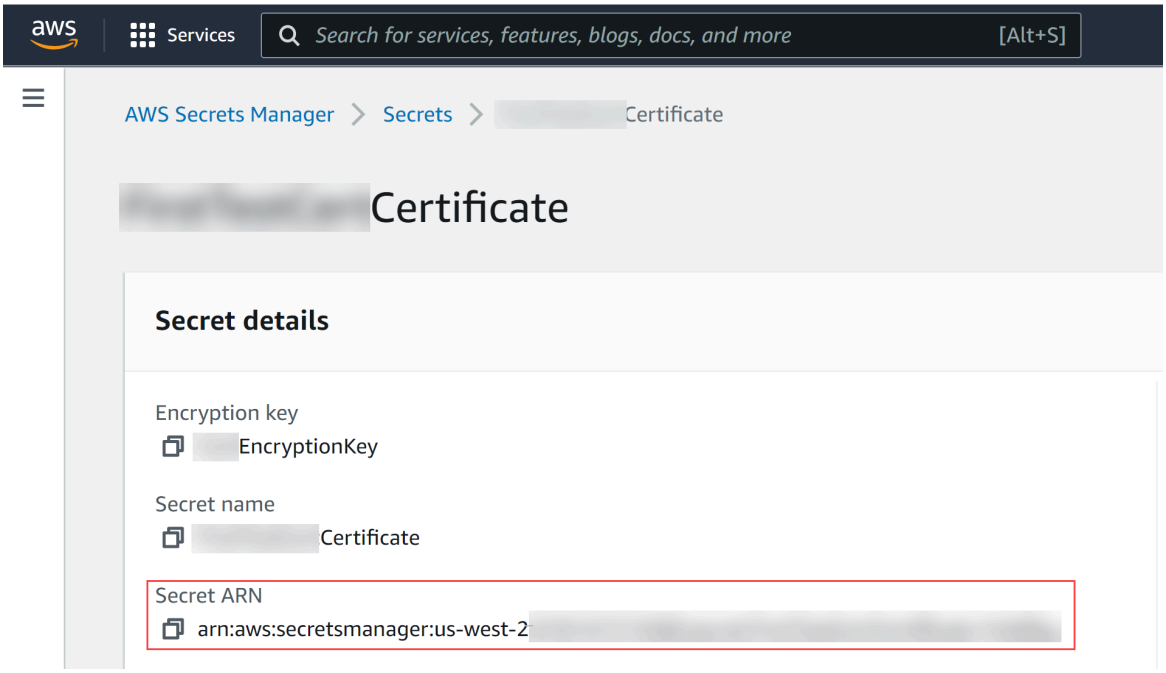
STEP 3 | Wählen Sie **Objects (Objekte)** > **Certificate List (Zertifikatsliste)** > **Add Certificate (Zertifikat hinzufügen)** aus.

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 das 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)**.

Sicherheitsregeln in Cloud NGFW für AWS erstellen

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 von mindestens 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 von mindestens 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.

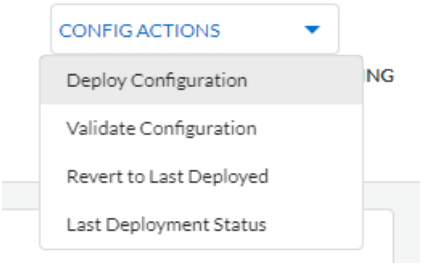
   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von Port und Protokoll ausgewertet. Durch die Angabe eines Ports und Protokolls wird der Datenverkehr anhand der Regel ausgewertet, wenn der Datenverkehr mit dem angegebenen Port und Protokoll übereinstimmt.
2. Wenn Sie sich für „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.



Regelnutzung in Cloud NGFW für AWS

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

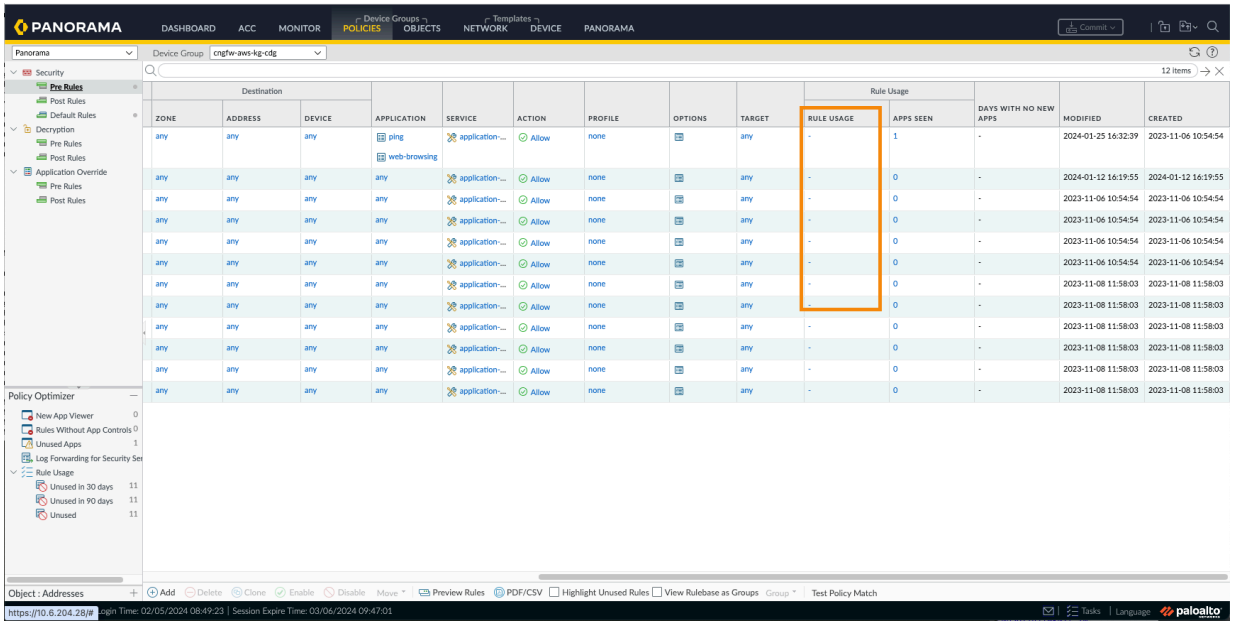
Nachdem Sie in der Panorama-Konsole eine Cloud-Gerätegruppe einer Cloud NGFW-Ressource zugeordnet und Richtlinien für die Cloud-Gerätegruppe konfiguriert haben, führen Sie die folgenden Schritte aus, um die Anzahl der Regeltreffer für eine Cloud-Gerätegruppe in Panorama anzuzeigen:

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.

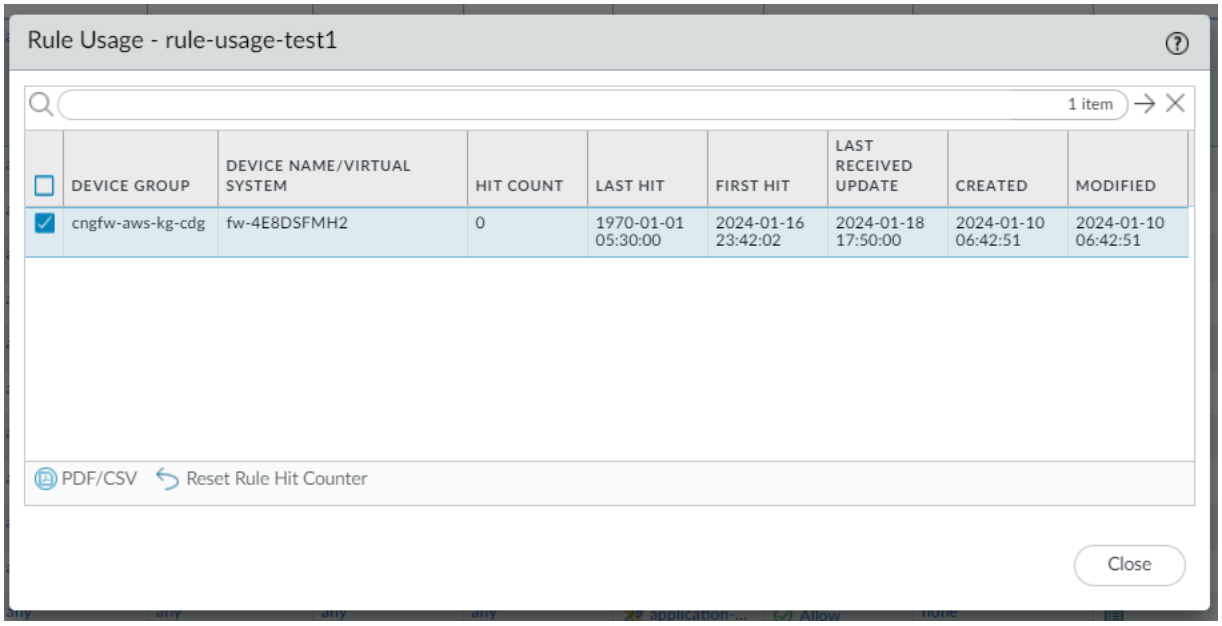
1. Wählen Sie **Policies (Richtlinien)** aus.
2. Wählen Sie im Abschnitt **Device Group (Gerätegruppe)** mithilfe der Dropdown-Liste die Cloud-Gerätegruppe aus.

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.



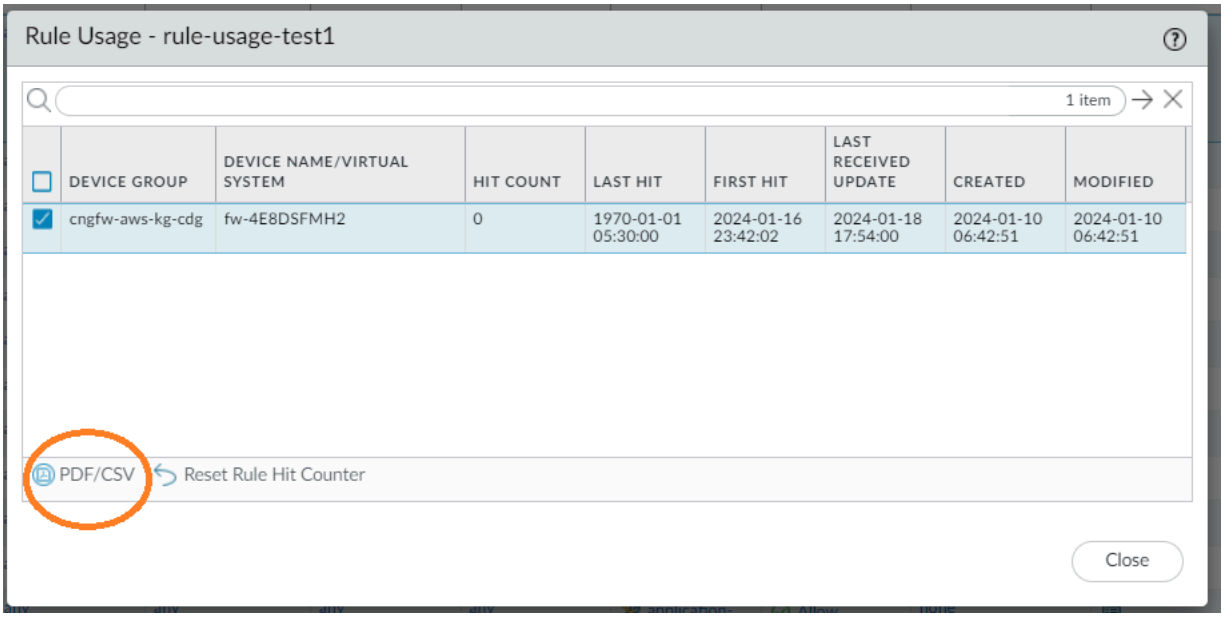
In der Spalte **Hit Count (Trefferanzahl)** wird nun die Anzahl der Treffer angezeigt.



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.

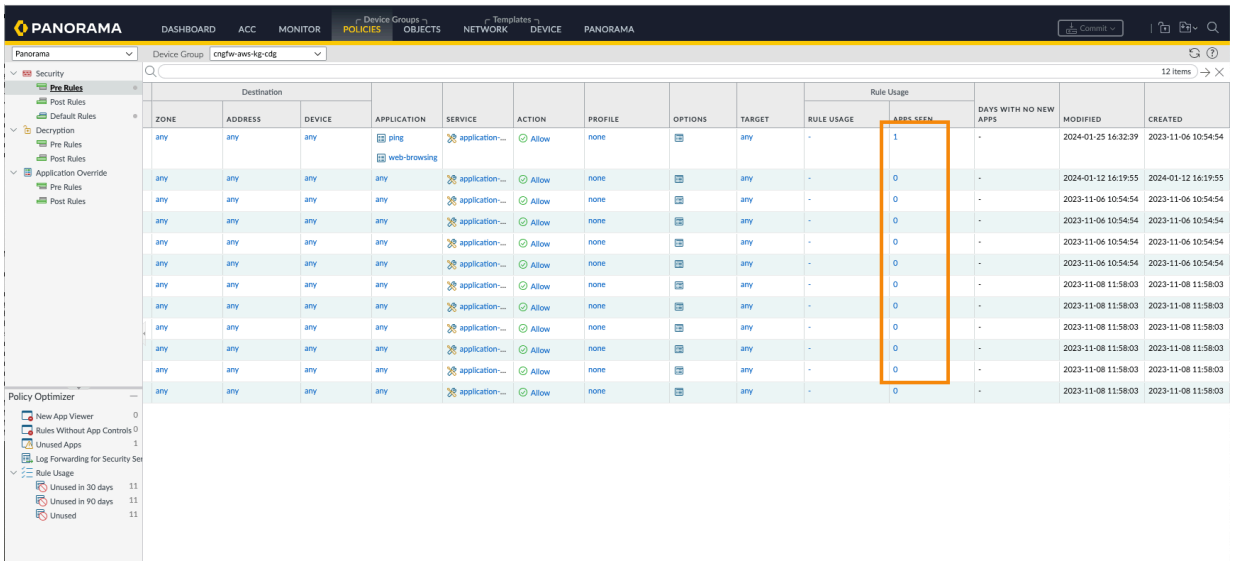


Regelnutzung – Erkannte Apps und Richtlinienoptimierer

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.

Sicherheitsprofile in Cloud NGFW für AWS

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 soll, und es blockiert Bedrohungen wie Viren, Malware, Spyware und DDOS-Angriffe.

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

Schweregrad der Signatur	Aktion
Mittel	Beide zurücksetzen
Informativ	Standard
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. Ein einzelner FTP-Anmeldefehler deutet beispielsweise 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

Bedrohungskategorie	Beschreibung
	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 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. 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-

Bedrohungskategorie	Beschreibung
	Website verleitet Benutzer dazu, Anmelde-Informationen einzugeben, die ein Angreifer dann abgreifen kann, um Zugriff auf das Netzwerk zu erhalten.
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 sie 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. *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

Bedrohungskategorie	Beschreibung
	koordinierte Aktion auszuführen (wie zum Beispiel einen DoS-Angriff zu starten).
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 Formularjacking, Phishing und Betrug) Erkennt den Zugriff auf kompromittierte Websites, bei denen festgestellt wurde, dass bösartiger JavaScript-Code injiziert wurde, um vertrauliche Benutzerinformationen (z. B. Name, Adresse, E-Mail, Kreditkartennummer, CVV, Ablaufdatum) aus Zahlungsformularen der Checkout-Seiten von E-Commerce-Websites abzugreifen.
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

Bedrohungskategorie	Beschreibung
	Forschung und Entwicklung. Die Verwendung oder der Besitz dieser Tools ist in manchen Ländern illegal, unabhängig von der Nutzungsabsicht.
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.
post-exploitation	Erkennt Aktivitäten, die auf einen vorangegangenen Exploit-Angriff hinweisen. In dieser Phase versuchen die Angreifer, den Wert des kompromittierten Systems zu bewerten. 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. 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) Antivirus-Profile schützen vor Viren, 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,

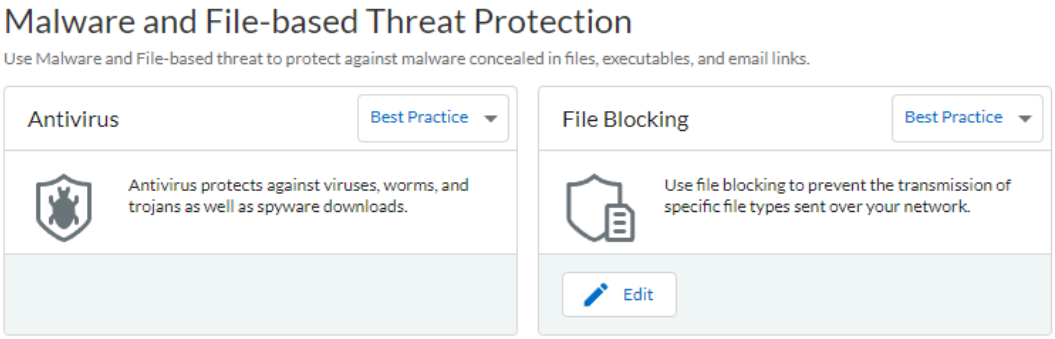
ohne die Leistung der Firewall erheblich zu beeinträchtigen. Dieses Profil scannt ausführbare Dateien, PDF-Dateien, HTML und JavaScript auf Malware, auch in komprimierten Dateien und Datencodierungsschemata.

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 (Datei-Blockade)** – Ein Datei-Blockade-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: • 7z • bat • cab • chm • class • cpl • dll • exe • flash • hip • hta • msi • Multi-Level-Encoding • ocx • PE • pif • rar • scr • tar • torrent	Beliebige	Beides (Hochladen und Herunterladen)	Blockieren

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

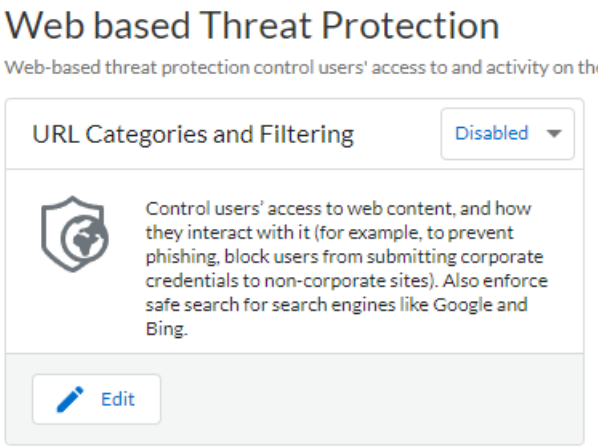
In der folgenden Tabelle sind alle möglichen Signaturen für die Kategorie „Antivirus“ aufgeführt. Diese Signaturen werden in Ihren NGFWs kontinuierlich aktualisiert.

Bedrohungskategorie	Beschreibung
Antivirus-Signaturen	
apk	Bösartige Android-Anwendungsdateien (APK).
MacOSX	Bösartige MacOSX-Dateien, einschließlich: • Apple Disk Image (DMG)-Dateien. • Mach-Objektdateien (Mach-O) sind ausführbare Dateien, Bibliotheken und Objektcode. • 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: • Objektcode. • Schriftarten (FONs). • Systemdateien (SYS). • Treiberdateien (DRV). • Elemente der Windows-Systemsteuerung (CPLs). • DLLs (Dynamic-Link-Bibliotheken).

Bedrohungskategorie	Beschreibung
	• OCXs (Bibliotheken für benutzerdefinierte OLE-Steuerelemente oder ActiveX-Steuerelemente). • Windows-Bildschirmschonerdateien (SCRs). • Extensible Firmware Interface (EFI)-Dateien, die zwischen einem Betriebssystem und der Firmware ausgeführt werden, um Geräteaktualisierungen und Startvorgänge zu erleichtern. • 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.

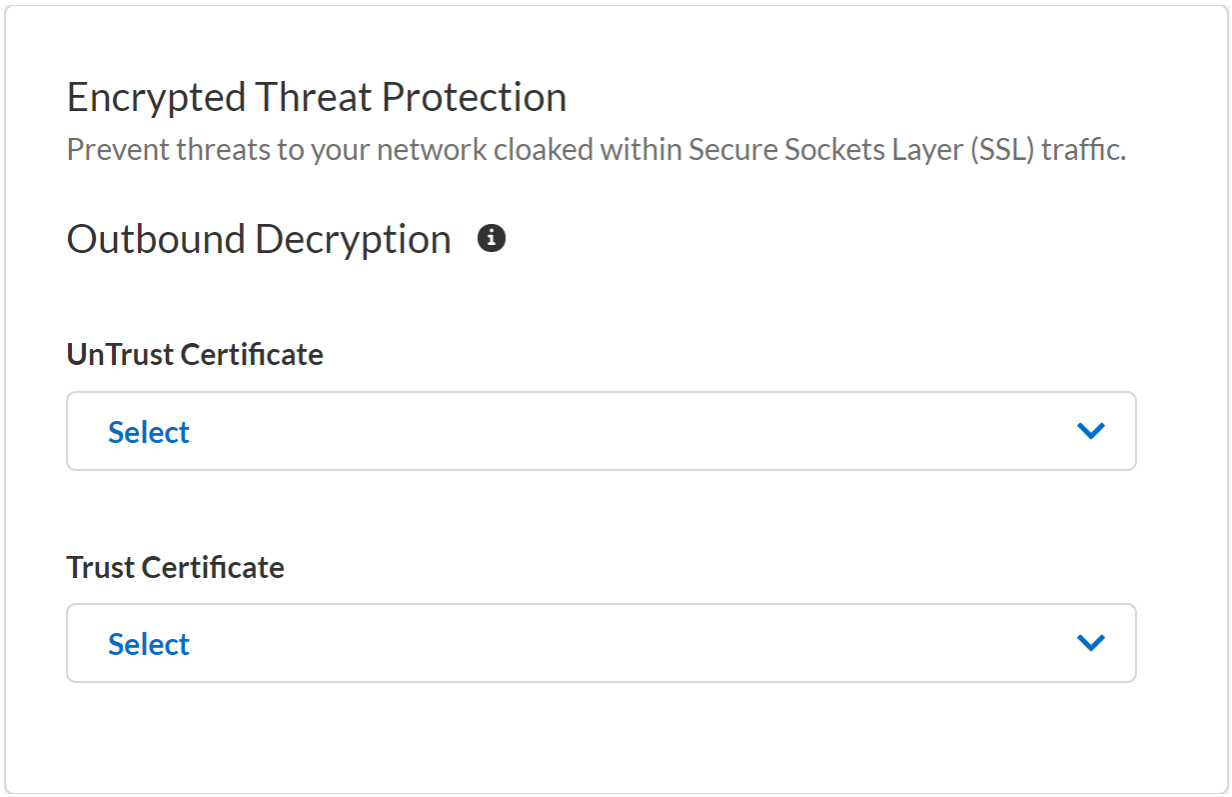
URL-Kategorien	Websitezugriff	Übermittlung von Anmeldeinformationen
Bösartige und missbräuchliche Kategorien:	Blockieren	Blockieren

URL-Kategorien	Websitezugriff	Übermittlung von Anmeldeinformationen
• adult • command-and-control • copyright-infringement • dynamic-dns • extremism • malware • parked • phishing • proxy-avoidance-and-anonymizers • 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

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.
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

URL-Kategorie	Beschreibung
	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/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 Anmelde-Informationen, Kreditkarteninformationen (absichtlich oder unabsichtlich), Kontonummern, PINs und aller Informationen, die als personenbezogene Daten gelten. Betrug mit technischem Support und Scareware gehört ebenfalls zur Phishing-Kategorie.
Verdächtig	
Unzureichender Inhalt	Websites und Dienste, die Testseiten ohne Inhalt präsentieren, API-Zugriff bieten, der nicht für die Anzeige durch Endbenutzer bestimmt ist, oder eine Authentifizierung erfordern, ohne andere Inhalte anzuzeigen, die auf eine andere Kategorisierung hindeuten. Sollte keine Websites umfassen, die Fernzugriff ermöglichen, wie z. B. webbasierte VPN-Lösungen, webbasierte E-Mail-Dienste oder bekannte Phishing-Seiten.
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, Anmelde-

URL-Kategorie	Beschreibung
	Informationen oder persönliche Identifikationsinformationen 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/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 Drogen-Utensilien, 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 wie Video-/Telefonanrufe, Begleitdienste, 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.

URL-Kategorie	Beschreibung
	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 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/-tools, Comics, darstellende Künste, Museen, Kunstgalerien oder Bibliotheken. Umfasst

URL-Kategorie	Beschreibung
	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/Handel von Brettspielen oder verwandte Veröffentlichungen/Medien anbieten. Umfasst 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.

URL-Kategorie	Beschreibung
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.
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

URL-Kategorie	Beschreibung
	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.
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 Immobilienvermietung, -verkauf und damit verbundene Tipps oder Informationen. Umfasst Websites für Immobilienmakler und -firmen,

URL-Kategorie	Beschreibung
	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.
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.

URL-Kategorie	Beschreibung
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, Portfoliomanagement, 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-/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 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/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.

URL-Kategorie	Beschreibung
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.

Websitezugriff für URLs in Cloud NGFW für AWS einrichten

Ein Sicherheitsprofil für die URL Filterung schützt vor webbasierten Bedrohungen und ermöglicht es Ihnen, genau zu kontrollieren, auf welche Webressourcen Ihre VPC-Workloads zugreifen können.

Wenn der Datenverkehr durch Ihre NGFW geleitet wird, um eine URL zu erreichen, lässt die NGFW diesen Datenverkehr basierend auf der Aktion zu, die Sie für die entsprechende URL-Kategorie festgelegt haben. Folgende Websitezugriffsaktionen können Sie festlegen:

- **Alert (Benachrichtigen)** – Wählen Sie „Alert“ (Benachrichtigen) aus, um Einblick in die Websites zu erhalten, auf die Benutzer zugreifen. Datenverkehr, der dieser Kategorie entspricht, ist zulässig, aber ein URL Filterungsprotokoll wird generiert, um aufzuzeichnen, wann ein Benutzer auf eine Website in dieser Kategorie zugreift.
- **Allow (Zulassen)** – Datenverkehr, der für diese Kategorie bestimmt ist, ist zulässig. Darüber hinaus wird zulässiger Datenverkehr nicht protokolliert.
- **Block (Blockieren)** – Verweigert den Zugriff auf Datenverkehr, der dieser Kategorie entspricht, und aktiviert die Protokollierung des blockierten Datenverkehrs.

Um die URL Filterung in Ihrer Bereitstellung optimal zu nutzen, sollten Sie zunächst Zulassungsregeln für die Anwendungen erstellen, die für Ihre Geschäftstätigkeit wichtig sind. Überprüfen Sie dann die URL-Kategorien, die für bösartige Inhalte stehen – wir empfehlen Ihnen, diese vollständig zu blockieren.

Wenn Sie die URL Filterung zum ersten Mal bereitstellen, empfehlen wir, mit einer grundlegenden Einrichtung zu beginnen, die uns Einblick in Webaktivitätsmuster gibt und gleichzeitig bestätigte schädliche Inhalte blockiert. Sie können als Erstes Kategorien blockieren, die als schädlich bekannt sind: Malware, Command-and-Control und Phishing. Legen Sie für andere Kategorien die Option „Alert“ (Benachrichtigen) fest, um einen Einblick in die Websites zu erhalten, auf die Ihre Benutzer zugreifen. Dann können Sie entscheiden, was Sie zulassen, einschränken und blockieren möchten.

Durch Benachrichtigungen für alle Webaktivitäten wird eine große Anzahl von Protokolldateien generiert. Daher sollten Sie später Ihre Websitezugriffsaktionen an Ihre Anforderungen anpassen.

Führen Sie die folgenden Schritte aus, um den Websitezugriff für benutzerdefinierte und vordefinierte URL-Kategorien festzulegen.

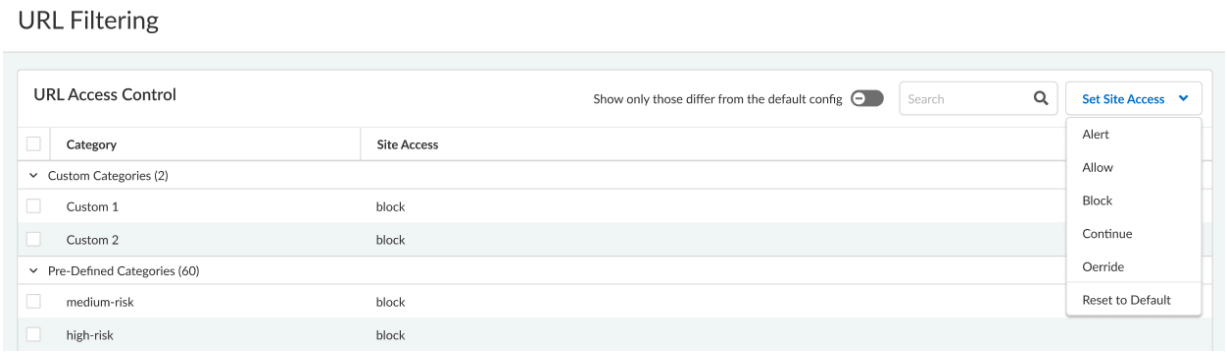
STEP 1 | Wählen Sie **Rulestacks (Regelstapel)** und einen zuvor erstellten Regelstapel aus, für den die URL Filterung konfiguriert werden soll.

STEP 2 | Wählen Sie **Security Profiles (Sicherheitsprofile)** > **Web-based Threat Protection (Schutz vor webbasierten Bedrohungen)** > **URL Categories & Filtering (URL-Kategorien und -Filterung)** > **Edit (Bearbeiten)** aus.

STEP 3 | Wählen Sie eine oder mehrere Kategorien aus der angezeigten Liste aus.

STEP 4 | Legen Sie mit **Set Site Access** den Websitezugriff für die ausgewählten Kategorien aus der Dropdownliste fest.

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



Dateiblockade in Cloud NGFW für AWS einrichten

Bei der Datei-Blockade 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/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 (Datei-Blockade)** > **Edit (Bearbeiten)** aus.

STEP 3 | Wählen Sie den Dateityp oder die Dateitypen 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.

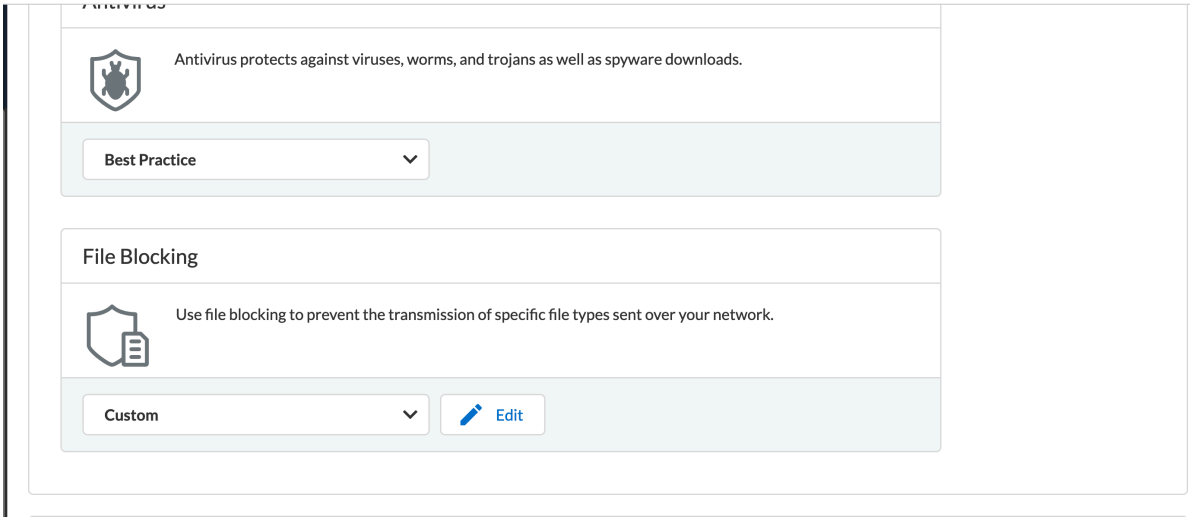
STEP 5 | Klicken Sie auf **Save (Speichern)**.

Ändern des Dateiblockade-Profils

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

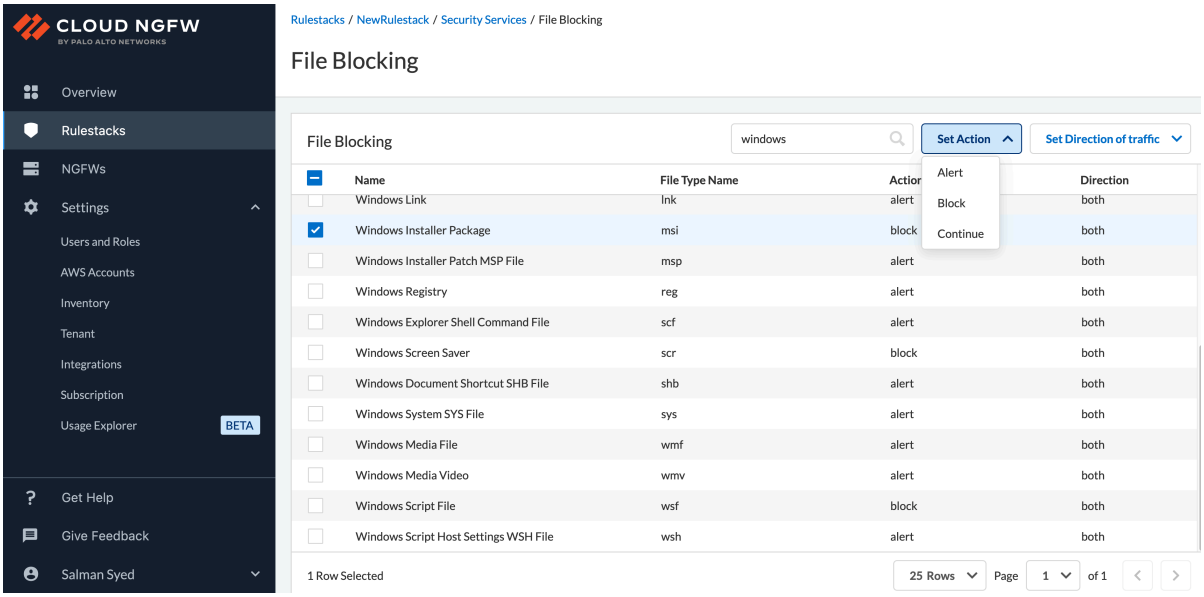
STEP 1 | Navigieren Sie im Bildschirm **Malware and File-based Threat Protection (Schutz vor Malware und dateibasierten Bedrohungen)** zu **File Blocking (Dateiblockade)**.

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

Bei der ausgehenden Entschlüsselung verhält sich Cloud NGFW wie ein SSL-Weiterleitungsproxy und verwendet die zugehörigen Zertifikate, um als vertrauenswürdiger Dritter (Man-in-the-Middle) 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 präsentiert die NGFW 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 Filterung und Datei-Blockaden. 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. Sie müssen die ausgehende TLS-Entschlüsselung während der Regelerstellung aktivieren.

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 Certificate (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 grundlegenden Einschränkungen muss auf TRUE gesetzt werden. Nachfolgend sehen Sie ein Beispiel für ein privates CA-Zertifikat.

```
Certificate: Data: Version: 3 (0x2) Serial Number: 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. Nachfolgend finden Sie ein Beispiel dazu, 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 Zertifikatsformat.

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

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 mit **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.*

Das Zertifikat und der private 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.

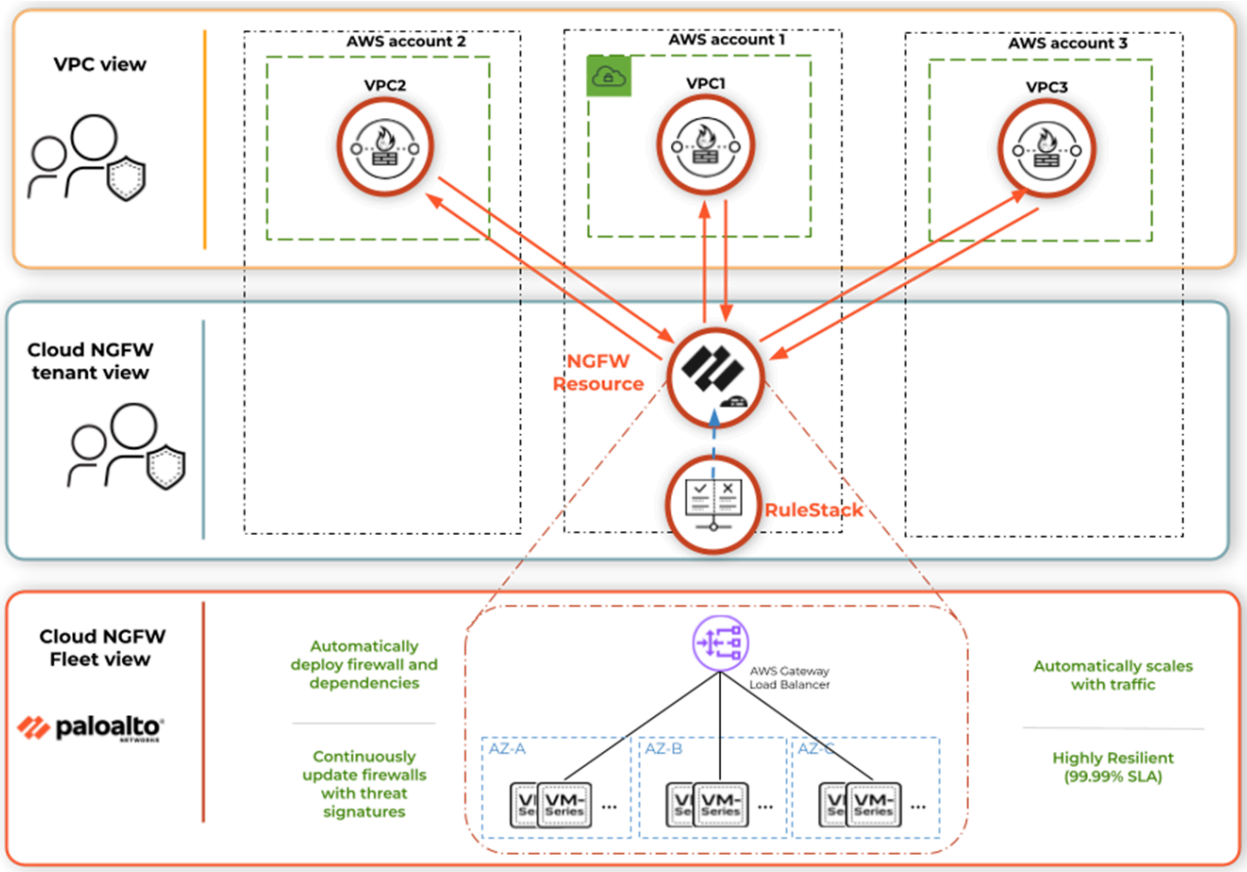
STEP 8 | Klicken Sie auf **Enabled (Aktiviert)**, um die Protokollierung zu aktivieren.

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.

Cloud NGFW-Ressource und NGFW-Endpunkte

Die NGFW ist eine Firewall-Ressource, die für die von Ihnen angegebene VPC vorgesehen ist und innovative Firewall-Funktionen bereitstellt. Beim Erstellen wird eine NGFW einer oder mehreren VPCs zugeordnet. NGFW-Endpunkte sind Konstrukte, die manuell oder automatisch in jeder Verfügbarkeitszone in den von Ihnen angegebenen VPCs erstellt werden. Die NGFW wendet Ihre Sicherheitsrichtlinie auf den Datenverkehr an, der von den NGFW-Endpunkten empfangen wird, und setzt diese Richtlinie durch. Beim Erstellen Ihrer NGFW müssen Sie mindestens eine VPC und einen lokalen Regelstapel angeben. Darüber hinaus müssen Sie angeben, wie und wo die zugehörigen NGFW-Endpunkte bereitgestellt werden.



NGFW-Endpunkte sind dafür verantwortlich, den Datenverkehr zur Prüfung und Durchsetzung an die NGFW weiterzuleiten. NGFW-Endpunkte fangen den Datenverkehr ab und leiten ihn zur Prüfung und Richtliniendurchsetzung an die NGFW weiter. Es gibt zwei Verwaltungsmodi, mit denen Endpunkte automatisch oder manuell erstellt werden können.

- Im **dienstverwalteten Modus** erstellt der Cloud NGFW-Mandant einen Endpunkt in jedem von Ihnen angegebenen Subnetz. Der NGFW-Dienst ruft eine Liste von Subnetzen in der von Ihnen angegebenen VPC ab und Sie wählen aus dieser Liste die Subnetze aus, die einen Endpunkt haben sollen.
- Im **kundenverwalteten Modus** wählen Sie vorhandene Verfügbarkeitszonen aus, die in Ihrer angegebenen VPC gesichert werden müssen, und erstellen dann manuell die NGFW-Endpunkte in vorhandenen Subnetzen in den ausgewählten Verfügbarkeitszonen. Nachdem die NGFW erstellt wurde, müssen Sie in der AWS-Konsole den Erstellungsprozess der NGFW-Endpunkte abschließen.

Nach dem Erstellen einer NGFW und von NGFW-Endpunkten müssen Sie Ihre AWS-Routing-Tabellen aktualisieren, um sicherzustellen, dass der Datenverkehr an die NGFW gesendet wird. Welche Routing-Tabellen aktualisiert werden und wie dies geschieht, hängt von Ihrer spezifischen Bereitstellung ab. Bereitstellungsbeispiele mit Routing-Tabellen, die Ihnen als Orientierungshilfe dienen, finden Sie unter Datenverkehr zu Cloud NGFW für AWS leiten.

- NGFW-Ressource in AWS erstellen
- NGFW-Endpunkte erstellen und anzeigen
- Datenverkehr zu Cloud NGFW für AWS leiten
- Protokollierung in Cloud NGFW für AWS konfigurieren
- Überwachungsprotokollierung in Cloud NGFW für AWS aktivieren
- Cloud NGFW-Ressource löschen

NGFW-Ressource in AWS erstellen

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.

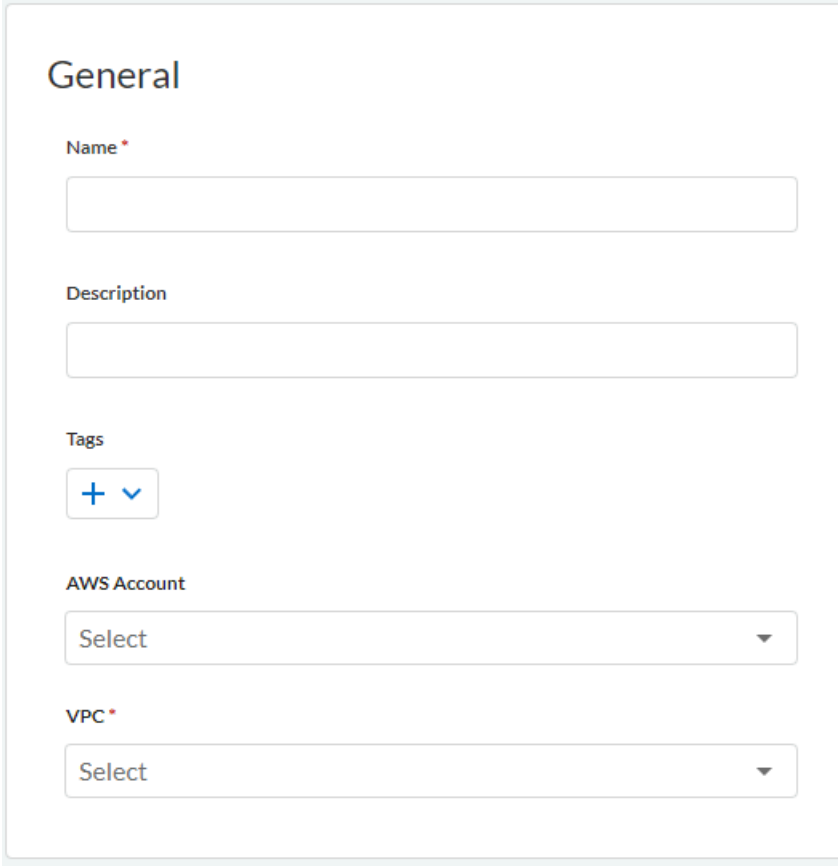
STEP 2 | Klicken Sie auf **Add Firewall (Firewall hinzufügen)**.

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

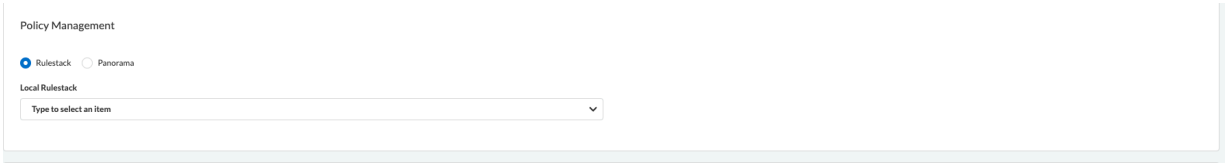
STEP 4 | (optional) Geben Sie eine **Beschreibung** ein.

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.

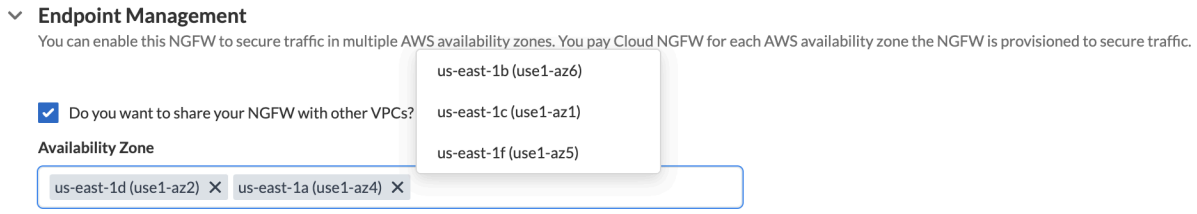


STEP 8 | Geben Sie AWS-Verfügbarkeitszonen oder Subnetze an. Sie müssen angeben, ob der Cloud NGFW-Mandant NGFW-Endpunkte bereitstellen wird (dienstverwalteter Modus) oder nicht (kundenverwalteter Modus).

- **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)**.

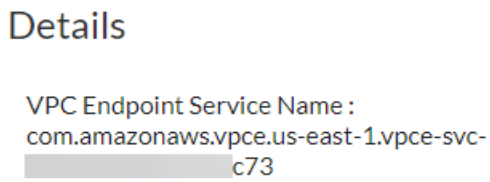
NGFW-Endpunkte erstellen und anzeigen

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 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.

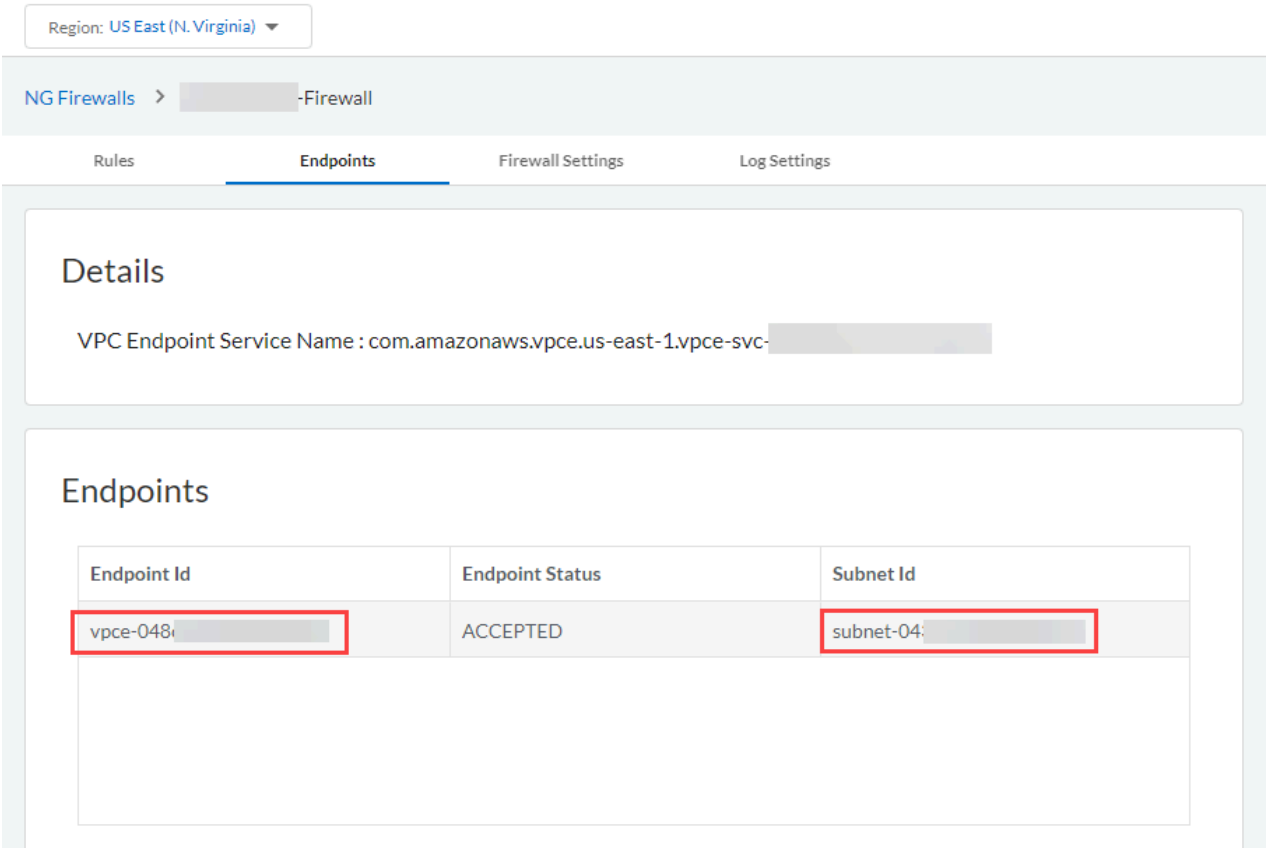
STEP 8 | Wählen Sie die Subnetze aus, in denen Sie NGFW-Endpunkte erstellen möchten.

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

Datenverkehr zu Cloud NGFW für AWS leiten

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

Zentralisierte Bereitstellungen in Cloud NGFW für AWS

Bei einer zentralisierten Bereitstellung werden Ihre Cloud NGFW-Komponenten in einer zentralisierten Sicherheits-VPC bereitgestellt. Der Datenverkehr muss immer durch ein AWS Transit Gateway (TGW)

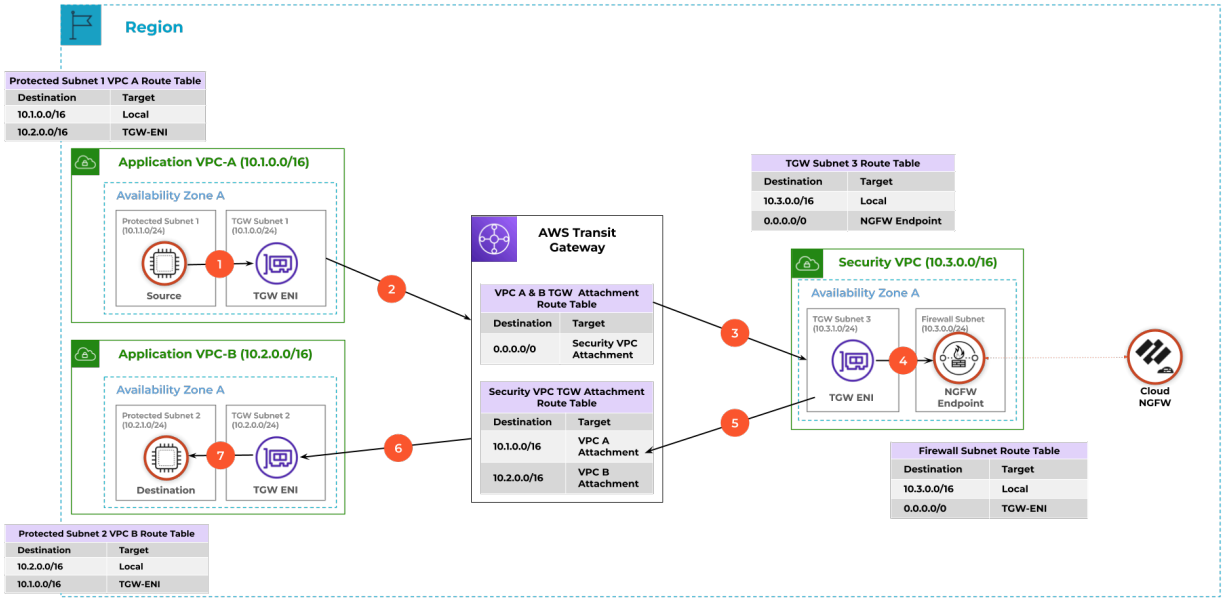
geleitet werden, das als Netzwerk-Hub fungiert und die Konnektivität zwischen VPCs sowie lokalen Netzwerken vereinfacht.

Weitere Beispiele für zentralisierte Bereitstellungen finden Sie unter Bereitstellungsarchitekturen in Cloud NGFW für AWS.

Zentralisierter Ost-West-Datenverkehr

1. Datenverkehr von der Quellinstanz wird an das TGW ENI gesendet.
2. Das TGW ENI leitet den Datenverkehr zum TGW.
3. Das TGW leitet den Datenverkehr an das TGW ENI der Sicherheits-VPC weiter.
4. Das TGW ENI sendet den Datenverkehr an den NGFW-Endpunkt und weiter an die NGFW zur Prüfung.
5. Wenn der Datenverkehr zulässig ist, sendet die NGFW ihn an den NGFW-Endpunkt zurück. Der Datenverkehr wird dann über den TGW-Endpunkt der Sicherheits-VPC an das TGW zurückgesendet.
6. Das TGW leitet den Datenverkehr an das TGW ENI in der Ziel-VPC weiter.

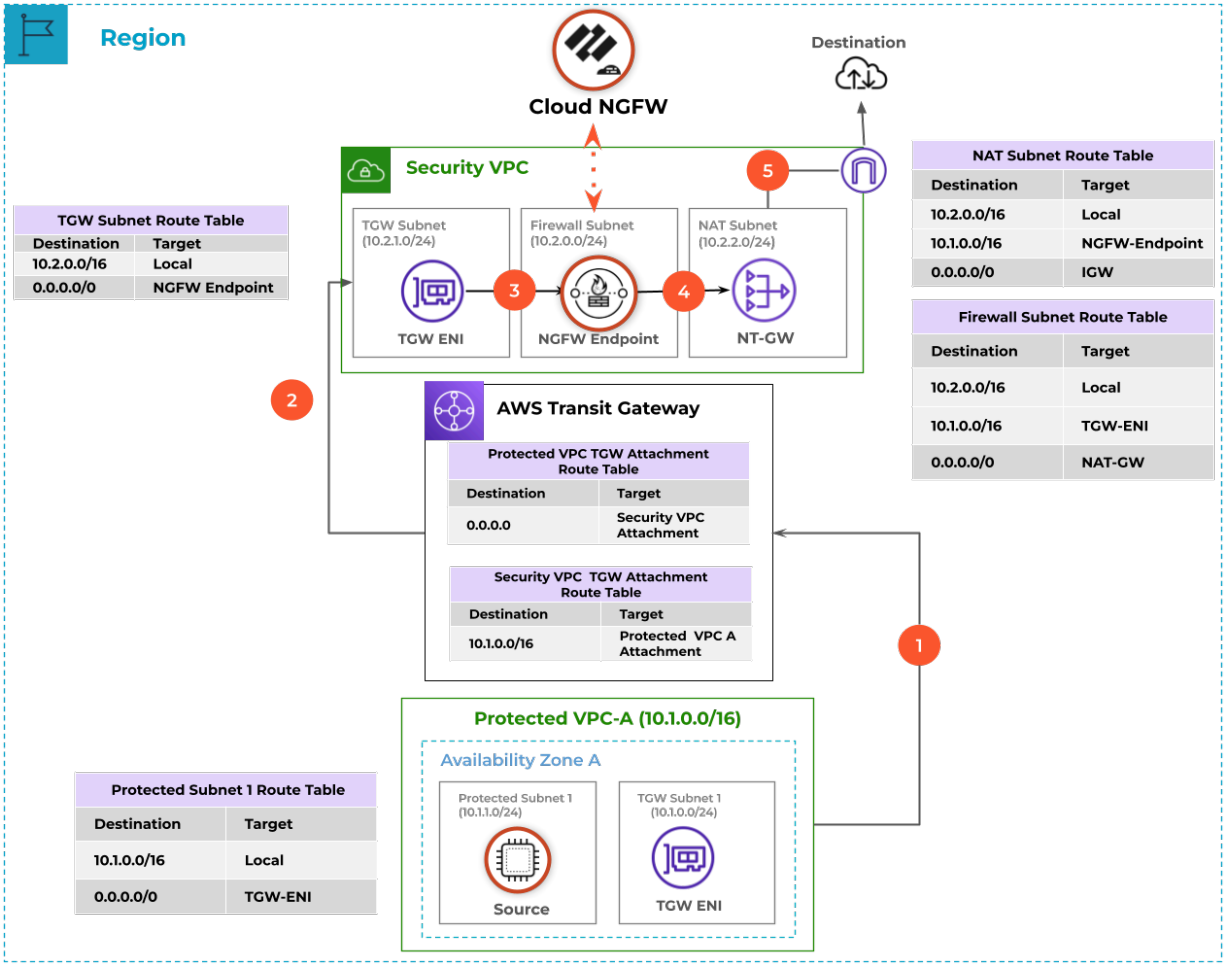
7. Dann sendet das TGW ENI den Datenverkehr an das Ziel.



Zentralisierter ausgehender Datenverkehr

1. Datenverkehr von der Quellinstanz wird an das TGW ENI und weiter an das TGW gesendet.
2. Das TGW leitet den Datenverkehr an das TGW ENI der Sicherheits-VPC weiter.
3. Das TGW ENI sendet den Datenverkehr an den NGFW-Endpunkt und weiter an die NGFW zur Prüfung.
4. Wenn der Datenverkehr zulässig ist, leitet der NGFW-Endpunkt ihn an das NAT-Gateway weiter.

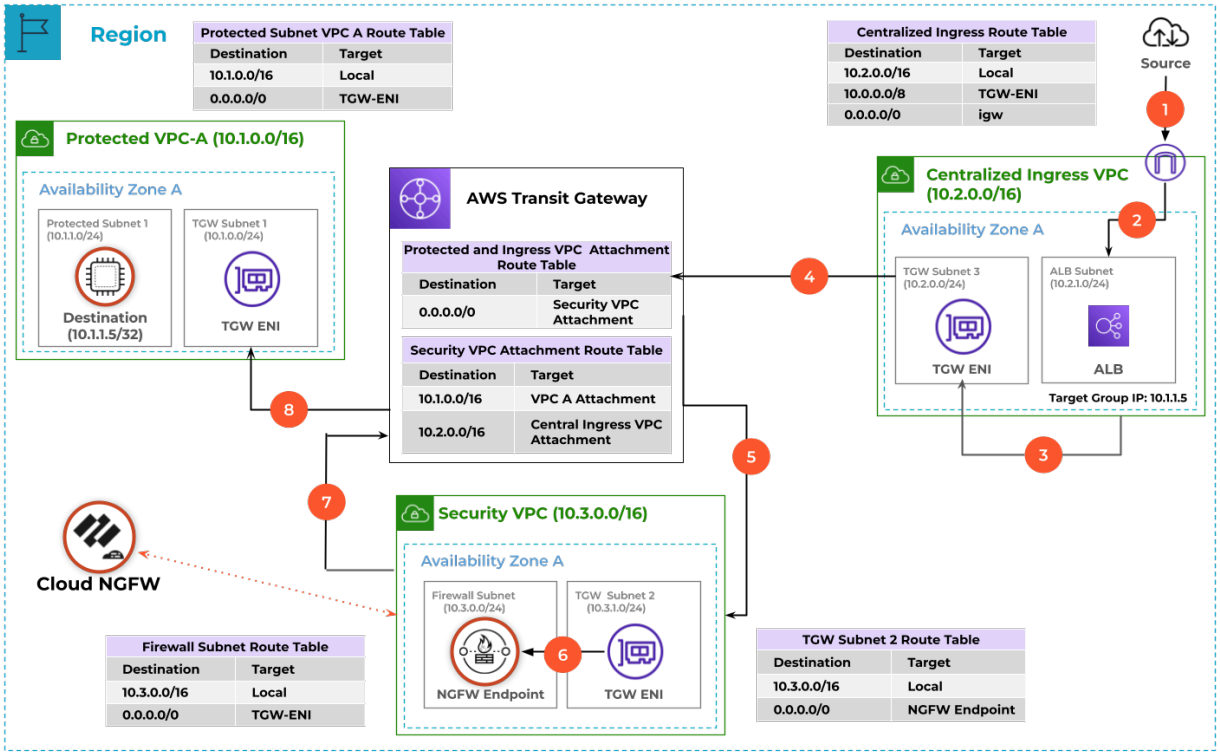
5. Das NAT-Gateway leitet den Datenverkehr an das IGW und dann weiter an das Ziel.



Zentralisierter eingehender Datenverkehr

1. Datenverkehr aus dem Internet kommt am Internetgateway an.
2. Das Internetgateway leitet den Datenverkehr an den Application Load Balancer (ALB) weiter.
3. Der ALB sendet dann den Datenverkehr an das TGW ENI der Eingangs-VPC.
4. Das TGW ENI sendet den Datenverkehr an das TGW.
5. Das TGW leitet den Datenverkehr an das TGW ENI der Sicherheits-VPC.
6. Das TGW ENI sendet den Datenverkehr an den NGFW-Endpunkt und weiter an die NGFW zur Prüfung.
7. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt ihn an das TGW.

8. Das TGW leitet den Datenverkehr dann an das TGW ENI der geschützten VPC und dann weiter an das Ziel.



Verteilte Bereitstellungen in Cloud NGFW für AWS

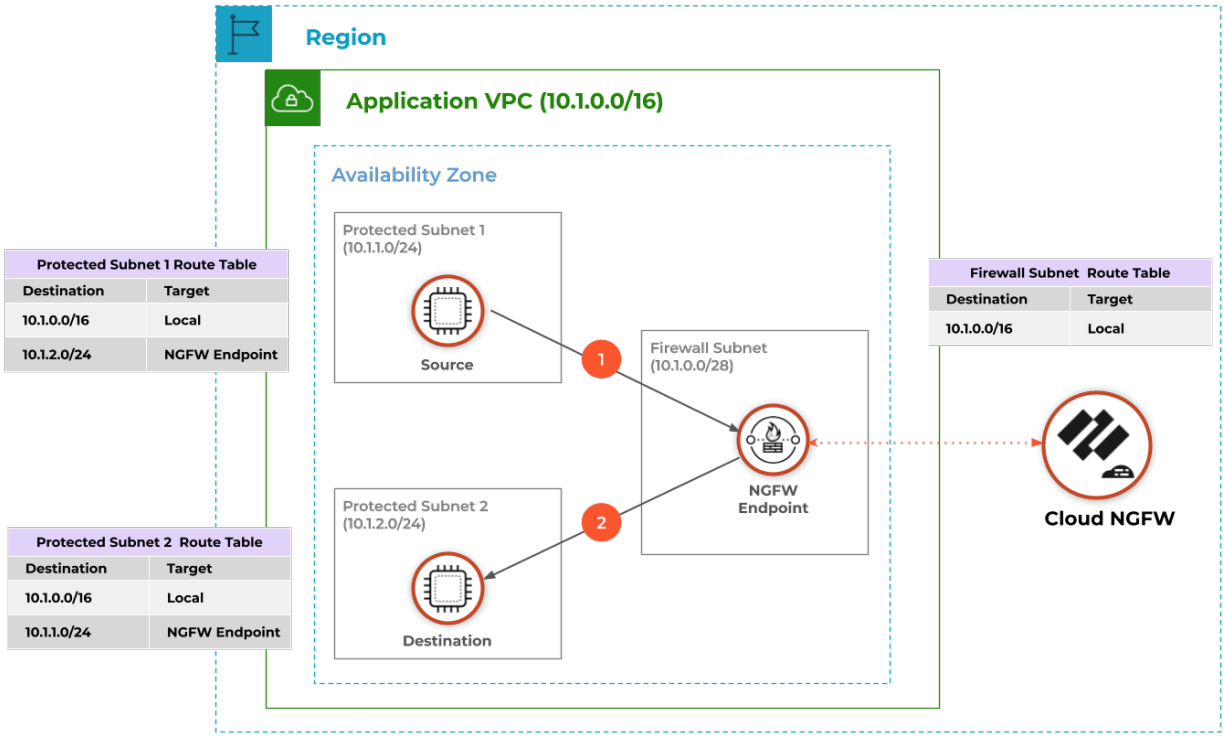
In einer verteilten Bereitstellung verfügt jede VPC, die geschützt werden muss, über eine eigene NGFW. Diese Bereitstellungsmethode ist weniger kompliziert und eine Fehlkonfiguration ist daher weniger wahrscheinlich.

Weitere Beispiele für verteilte Bereitstellungen finden Sie unter Bereitstellungsarchitekturen in Cloud NGFW für AWS.

Verteilter Ost-West-Datenverkehr (innerhalb der VPC)

1. Datenverkehr von der Quellinstanz wird zur Prüfung an den NGFW-Endpunkt und weiter an die NGFW geleitet.

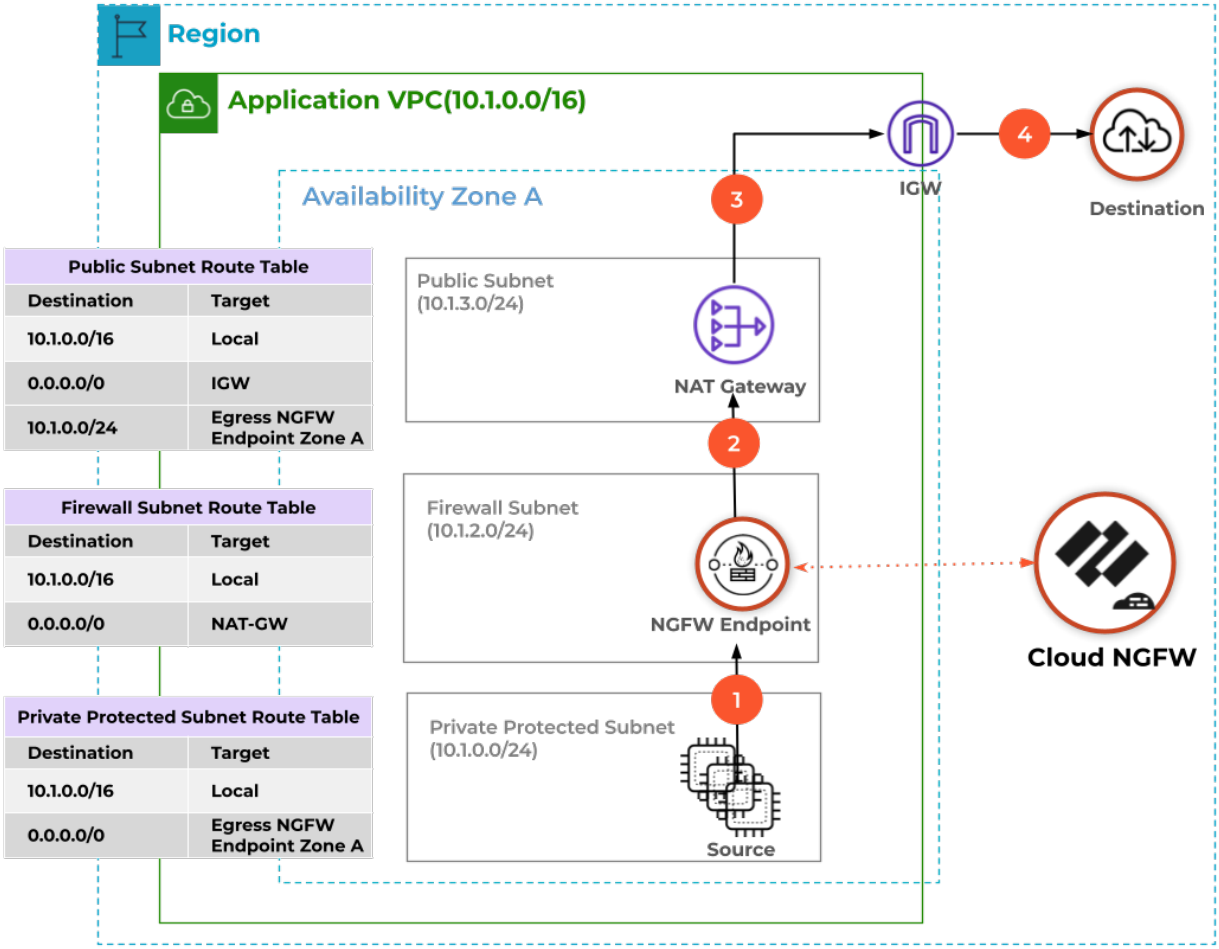
2. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt ihn an das Ziel.



Verteilter ausgehender Datenverkehr

1. Datenverkehr von der Quellinstanz wird zur Prüfung an den NGFW-Endpunkt und weiter an die NGFW geleitet.
2. Wenn der Datenverkehr zulässig ist, sendet der NGFW-Endpunkt den geprüften Datenverkehr an das NAT-Gateway.
3. Das NAT-Gateway sendet den Datenverkehr an das Internetgateway.

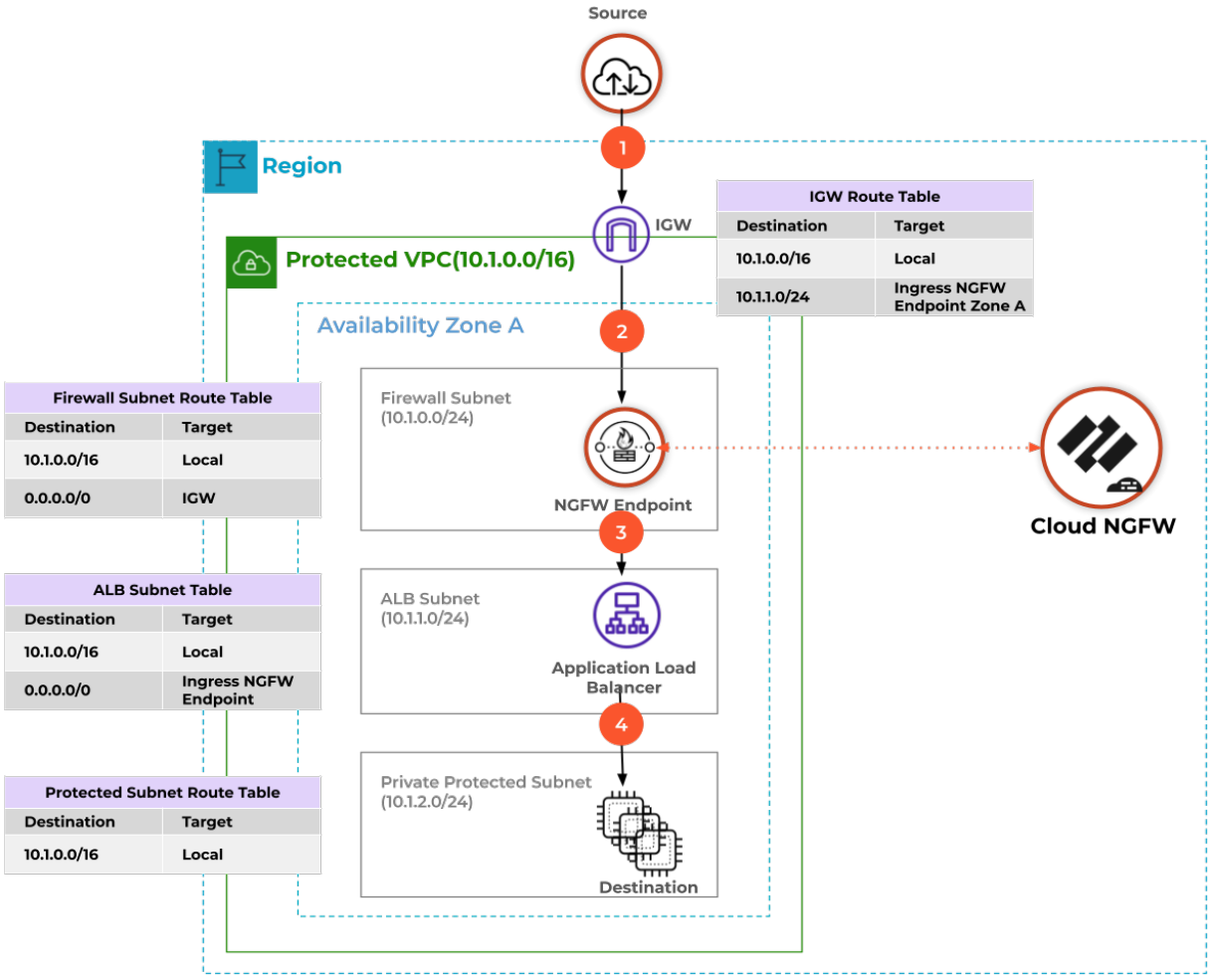
4. Der Datenverkehr wird ins Internet und an das Ziel weitergeleitet.



Verteilter eingehender Datenverkehr

1. Der Datenverkehr von der Quelle kommt am Internetgateway an.
2. Das Internetgateway leitet den Datenverkehr an den NGFW-Endpunkt und dann zur Prüfung an die NGFW weiter.
3. Wenn der Datenverkehr zulässig ist, leitet der NGFW-Endpunkt ihn an den Application Load Balancer weiter.

4. Der Application Load Balancer leitet den Datenverkehr an das Ziel weiter.



Protokollierung in Cloud NGFW für AWS konfigurieren

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 einer Spyware, Sicherheitslücke oder Virensignatur 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 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.

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. Virus 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 Exploit-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

Severity (Schweregrad)	Beschreibung
	auszunutzen sein, nicht zu erhöhten Rechten führen oder keinen großen 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 oder 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 den Cloud NGFW für AWS abonnieren, werden Sie aufgefordert, Ihren AWS CloudFormation-Vorlagenstapel 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.

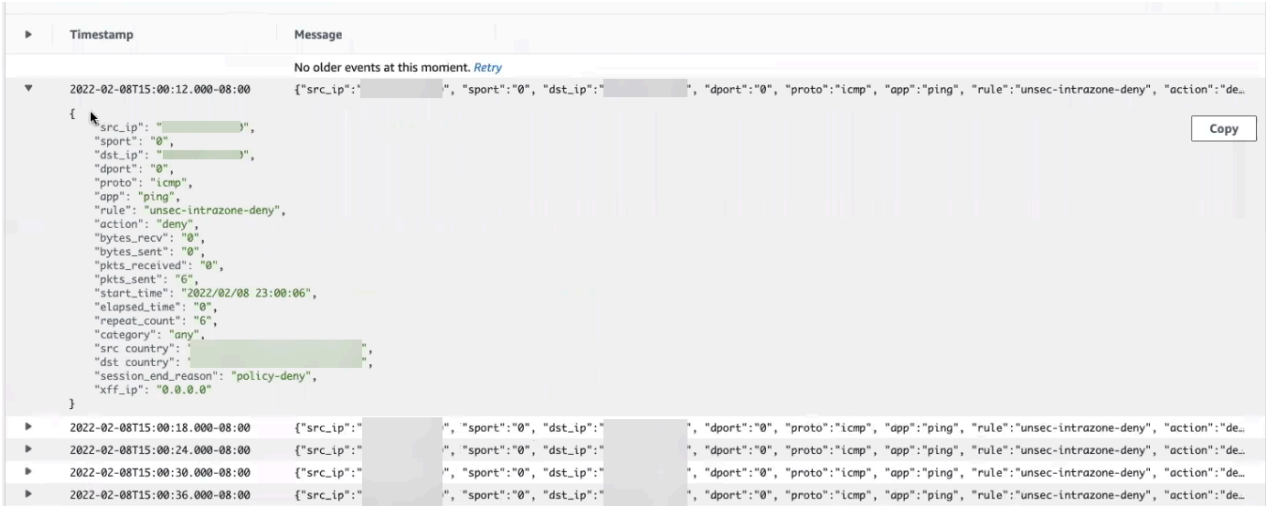
Wenn Sie die Protokolle an eine CloudWatch-Protokollgruppe senden, können Sie die Protokolleinträge direkt in der AWS CloudWatch-Konsole anzeigen. In der CloudWatch-Protokollgruppe, die Sie beim Konfigurieren der Protokollierung angeben, sehen Sie eine Liste der Protokollstreams. Der Protokollstreamname wird wie folgt angezeigt:

`/<aws-account-id>/<region>/<NGFW-name>/<random-string>/<log-type>.<year>.<month>.<day>.<hour>`

Beispiel: /account123/us-west-1/firewall-1/qadd232312345dea/TRAFFIC.2022.02.10.23

<random string> bezieht sich auf die einzelne NGFW-Ressource, die das Protokoll generiert hat.

Sie können auf den Streamnamen klicken, um Protokolleinträge einzublenden, die wie im folgenden Beispiel gezeigt 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)***. Die Namen der S3-Bucket-Protokolldateien haben das folgende Format:


```
<aws-account-id>-<region>-<NGFW-name>-<log-type>-<year>-<month>-<day>-
<hour>-<random-string>
```

<random string> bezieht sich auf die einzelne NGFW-Ressource, die das Protokoll generiert hat.

Anschließend können Sie die Datei herunterladen und mit einem JSON-Reader die Protokolle in einem besser lesbaren Format anzeigen. 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

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: • allow: Sitzung wurde von der Richtlinie zugelassen • deny: Sitzung wurde von der Richtlinie abgelehnt • reset both: Sitzung wurde beendet und ein TCP-Reset wird an beide Seiten der Verbindung gesendet • reset client: Sitzung wurde beendet und ein TCP-Reset wird an den Client gesendet • reset server: Sitzung wurde beendet und ein TCP-Reset wird an den Server gesendet
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.

Feldname	Beschreibung
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): • threat: Die Firewall hat eine Bedrohung erkannt, die mit einer Aktion zum Zurücksetzen, Löschen oder Blockieren (einer IP-Adresse) verbunden ist. • policy-deny: Die Sitzung stimmte mit einer Sicherheitsregel mit einer deny- oder drop-Aktion überein. • 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. • 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

Feldname	Beschreibung
	Protokollversion, Verschlüsselung oder einen SSH-Algorithmus verwendet. Dieser Grund für das Sitzungsende wird angezeigt, wenn die Sitzung eine schwerwiegende Fehlerwarnung des Typs „unsupported_extension“, „expected_message“ oder „handshake_failure“ erzeugt. • 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 Beendungsgründe „decrypt-cert-validation“ und „decrypt-unsupport-param“ aufgeführten Warnungen ausgegeben hat. • tcp-rst-from-client: Der Client hat ein TCP-Reset an den Server gesendet. • tcp-rst-from-server: Der Server hat ein TCP-Reset an den Client gesendet. • 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. • tcp-fin: Beide Hosts in der Verbindung haben eine TCP-FIN-Nachricht gesendet, um die Sitzung zu schließen. • tcp-reuse: Eine Sitzung wird wiederverwendet und die Firewall schließt die vorherige Sitzung. • decoder: Der Decoder erkennt eine neue Verbindung innerhalb des Protokolls (z. B. HTTP-Proxy) und beendet die vorherige Verbindung. • aged-out: Die Sitzung ist abgelaufen. • 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 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

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. • alert: Bedrohung oder URL erkannt, aber nicht blockiert • allow: Flood-Erkennungswarnung • deny: Mechanismus zur Flood-Erkennung aktiviert und Datenverkehr basierend auf der Konfiguration ablehnen • drop: Bedrohung erkannt und zugehörige Sitzung wurde gelöscht • reset-client: Bedrohung erkannt und ein TCP-RST wird an den Client gesendet • reset-server: Bedrohung erkannt und ein TCP-RST wird an den Server gesendet • reset-both: Bedrohung erkannt und ein TCP-RST wird sowohl an den Client als auch an den Server gesendet • block-url: URL-Anforderung wurde blockiert, da sie mit einer URL-Kategorie übereinstimmte, die als blockiert festgelegt war • block-ip: Bedrohung erkannt und Client-IP wird blockiert • random-drop: Flood erkannt und Paket wurde nach dem Zufallsprinzip verworfen

Feldname	Beschreibung
	• sinkhole: DNS-Sinkhole aktiviert • syncookie-sent: syncookie-Warnung • block-continue (nur URL-Untertyp): eine HTTP-Anforderung wird blockiert und auf eine continue-Seite mit einer Schaltfläche zur Bestätigung zum Fortfahren umgeleitet • continue (nur URL-Untertyp): Antwort auf eine continue-Seite der block-continue-URL, die angibt, dass eine block-continue-Anforderung fortgesetzt werden durfte • 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 • override-lockout (nur URL-Untertyp): zu viele fehlgeschlagene Admin-Überschreibungs-Passcodeversuche von der Quell-IP. IP ist jetzt von der block-override-Weiterleitungsseite blockiert • override (nur URL-Untertyp): Antwort auf eine block-override-Seite, auf der ein korrekter Passcode angegeben wird und die Anforderung zulässig ist • 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: • data: Datenmuster, das einem Datenfilterungsprofil entspricht. • file: Dateityp, der einem Dateiblockadeprofil entspricht. • flood: Flood, die über ein Zonen-Sicherheitsprofil erkannt wird. • packet: Paketbasierter Angriffsschutz, der durch ein Zonen-Sicherheitsprofil ausgelöst wird. • scan: Scan, der über ein Zonen-Sicherheitsprofil erkannt wird. • spyware: Spyware, die über ein Anti-Spyware-Profil erkannt wird. • url: URL-Filterungs-Protokoll. • ml-virus: Virus, der von WildFire Inline ML über ein Antivirus-Profil erkannt wird. • virus: Virus, der über ein Antivirus-Profil erkannt wird. • vulnerability: Sicherheitslücken-Exploit, der über ein Sicherheitslücken-Sicherheitsprofil erkannt wird. • 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

Feldname	Beschreibung
	protokollieren) im WildFire-Übermittlungsprotokoll protokolliert wird. • wildfire-virus: Virus, der über ein Antivirus-Profil erkannt wurde.
Bedrohungs-/Inhaltsname (threat_content_name)	Palo Alto Networks Kennung für bekannte und benutzerdefinierte Bedrohungen. Es ist eine Beschreibungszeichenfolge, gefolgt von einer numerischen 64-Bit-Kennung in Klammern für einige Untertypen: • 8000–8099: Scan-Erkennung • 8500–8599: Flood-Erkennung • 9999: URL-Filterungs-Protokoll • 10000–19999: Erkennung von Spyware-Telefonen • 20000–29999: Erkennung von Spyware-Downloads • 30000–44999: Erkennung von Sicherheitslücken-Exploits • 52000–52999: Erkennung von Dateitypen • 60000–69999: Erkennung von Datenfilterung *Bedrohungs-ID-Bereiche für Virenerkennung, 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.*
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: • 0: Richtung der Bedrohung ist Client-zu-Server • 1: Richtung der Bedrohung ist Server-zu-Client
Wiederholungsanzahl (repeatcnt)	Anzahl der Sitzungen mit derselben Quell-IP, Ziel-IP, Anwendung und demselben Inhalts-/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

Feldname	Beschreibung
	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

Feldname	Beschreibung
Generierte Zeit (time_generated oder cef-formatted-time_generated)	Uhrzeit, zu der das Protokoll auf der Datenebene generiert wurde.
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: • allow: Sitzung wurde von der Richtlinie zugelassen • deny: Sitzung wurde von der Richtlinie abgelehnt • reset both: Sitzung wurde beendet und ein TCP-Reset wird an beide Seiten der Verbindung gesendet • reset client: Sitzung wurde beendet und ein TCP-Reset wird an den Client gesendet • reset server: Sitzung wurde beendet und ein TCP-Reset wird an den Server gesendet

Feldname	Beschreibung
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.
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“.
Kettenstatus (chain_status)	Legt fest, ob der Kette vertraut wird. Werte sind: • Nicht geprüft • Nicht vertrauenswürdig • Vertrauenswürdig • Unvollständig

Cloud NGFW für AWS – CloudWatch-Metriken

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.

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.

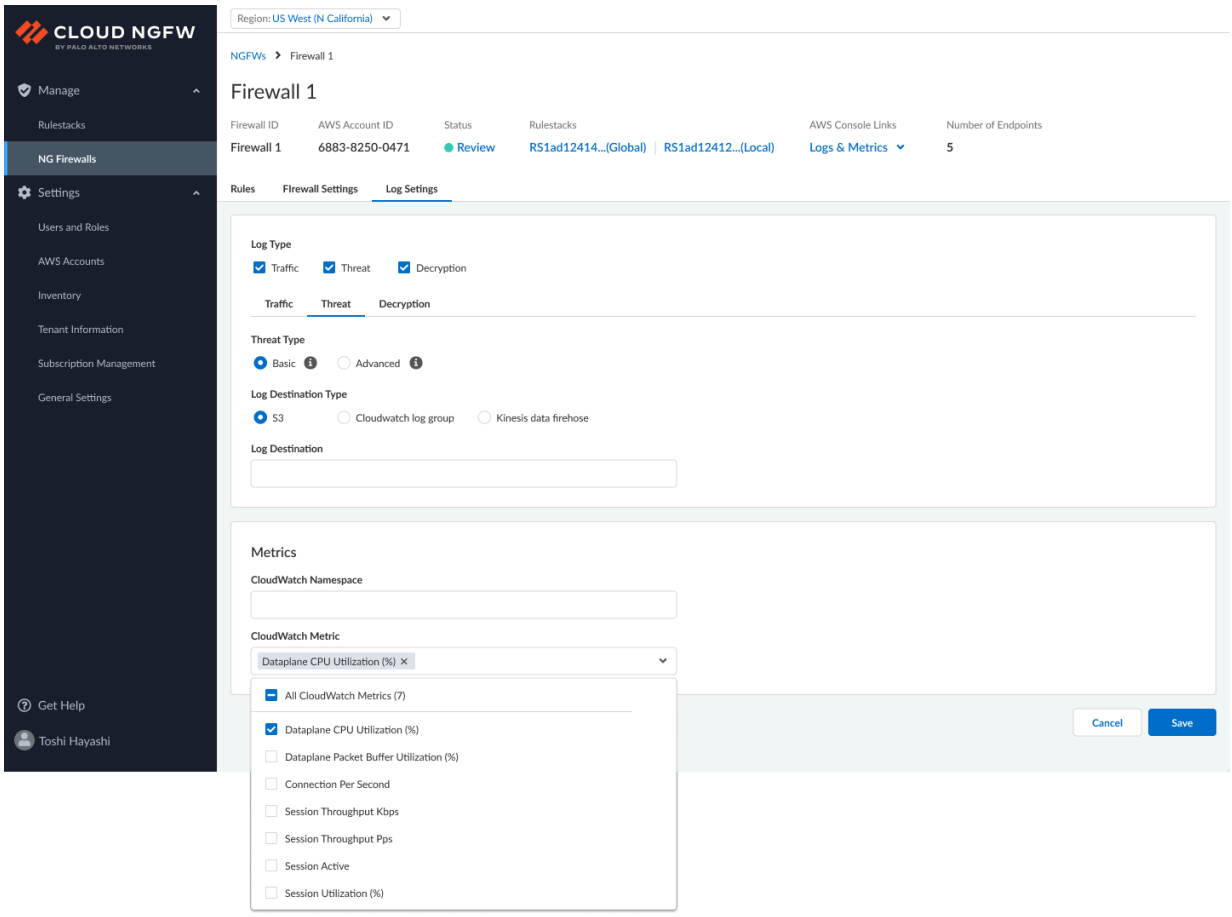
Die folgenden CloudWatch-Metriken werden von der Cloud NGFW-Ressource unterstützt:

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 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 (kbit/s))	Der Sitzungsdurchsatz, gemessen in kbit/s.
Session Throughput Pps (Sitzungsdurchsatz Pakete/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 Firewall-Durchsatz, 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.

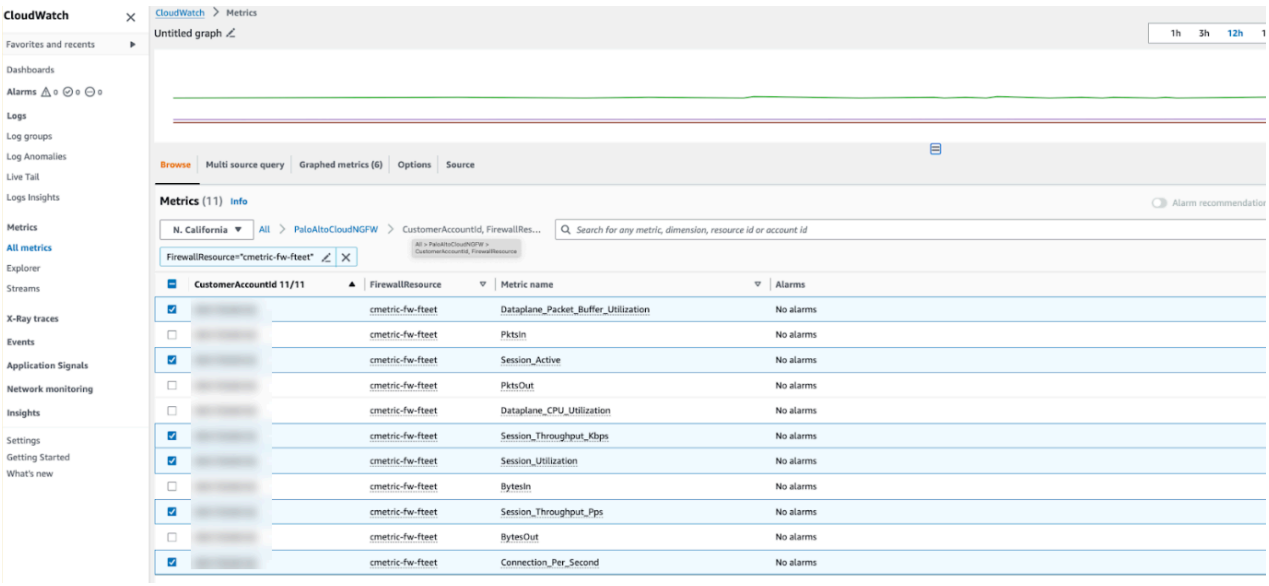
Feldname	Beschreibung
PktsOut (Ausgehende Pakete)	Anzahl der Client-zu-Server-Pakete für die Sitzung.

So veröffentlichen Sie CloudWatch-Metriken:

1. Melden Sie sich bei Ihrer Cloud NGFW-Ressource an.
2. Wählen Sie **NG Firewalls (NG-Firewalls)** aus.
3. Wählen Sie **Log Settings (Protokolleinstellungen)** aus.
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.
5. Klicken Sie auf **Save (Speichern)**.



Eine Beispielausgabe von Metriken, die in einem Konto angezeigt werden, sieht wie folgt aus:



Überwachungsprotokollierung in Cloud NGFW für AWS aktivieren

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.

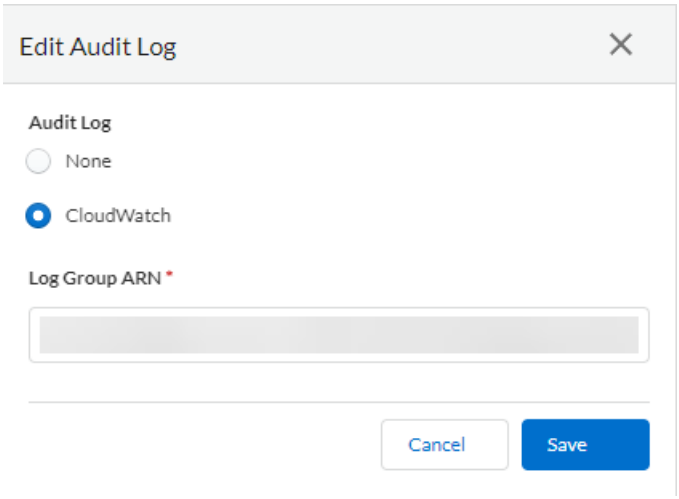
STEP 4 | Klicken Sie auf das Bearbeitungssymbol Edit für **Audit Log Settings (Überwachungsprotokolleinstellungen)**.

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)**.

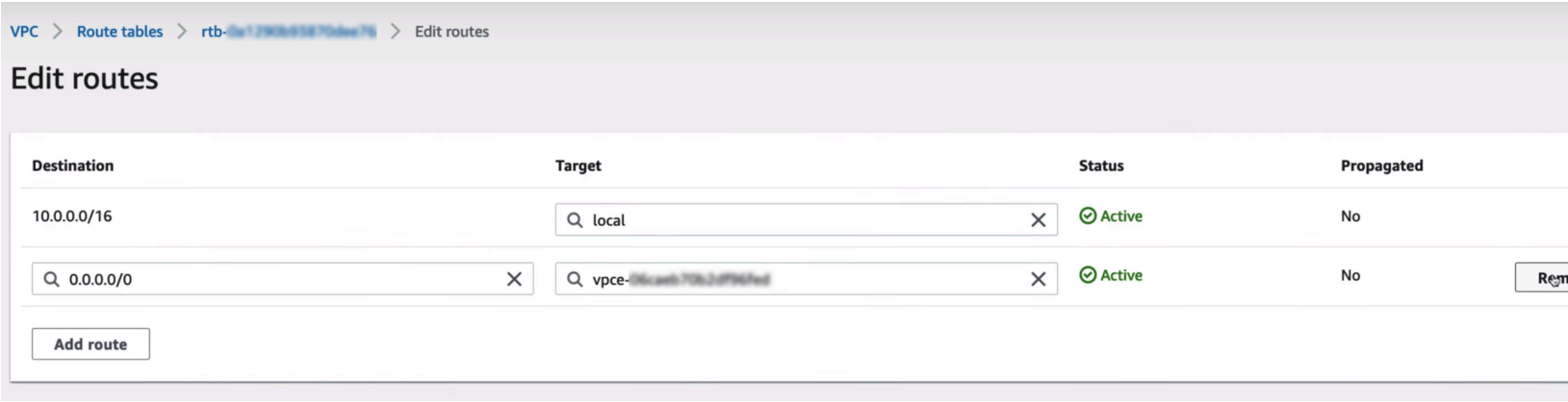


Cloud NGFW-Ressource löschen

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.

Cloud NGFW-Integration mit AWS Cloud WAN

AWS Cloud WAN ist ein verwalteter Wide-Area-Networking(WAN)-Dienst, mit dem Sie ein einheitliches Netzwerk aufbauen können, das Cloud- und lokale Umgebungen miteinander verbindet. Er bietet ein zentrales Dashboard zum Verbinden von lokalen Standorten, Zweigstellen, Rechenzentren und Amazon VPCs über das globale AWS-Netzwerk und selbst andere Cloud-Anbieter.

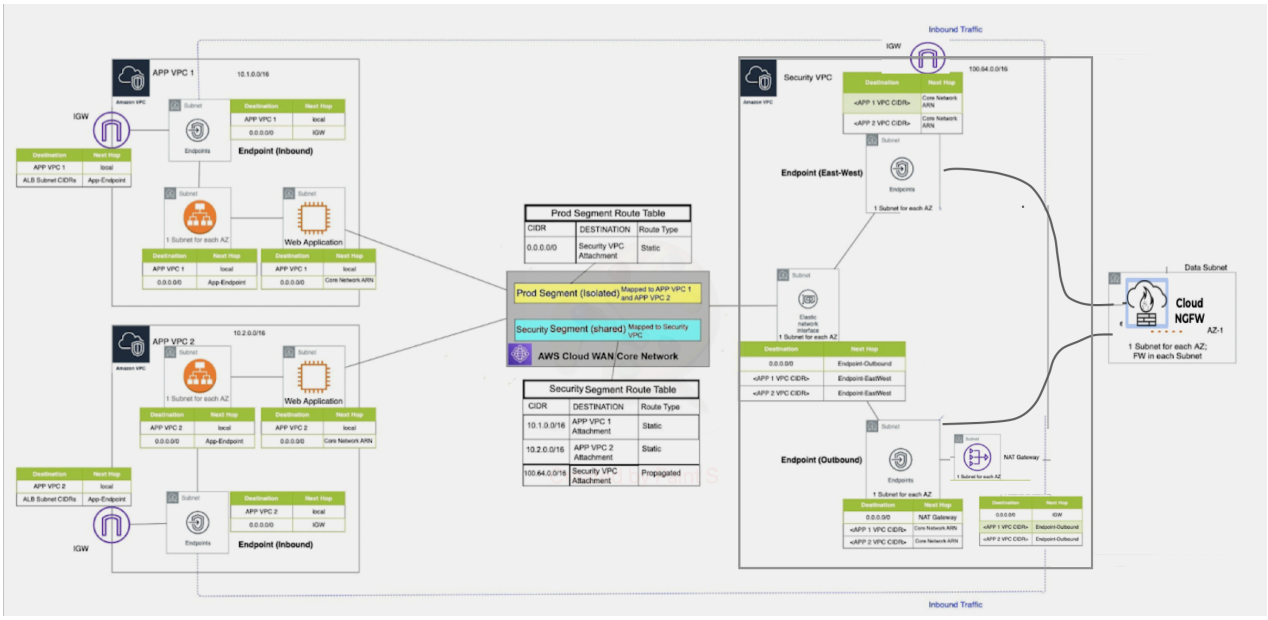
Cloud WAN unterstützt die Konnektivität innerhalb von AWS durch AWS Network Manager, eine Schnittstelle, die Ihr globales Netzwerk zentral verwaltet. Ein globales Netzwerk ist ein einzelnes privates Netzwerk, das als Container auf Stammebene für Ihre Netzwerkobjekte fungiert und sowohl Transit-Gateways als auch ein Kernnetzwerk enthalten kann. Das Kernnetzwerk besteht aus Netzwerkrichtlinien, Anhängen wie VPCs und Transit-Gateway-Routentabellen.

Sie können diese VPCs Segmenten im Kernnetzwerk zuordnen. Diese Segmente werden durch Anhänge wie VPC-Anhänge oder Transit-Gateway-Routentabellen-Anhänge verbunden. Die integrierte Segmentierung hilft Ihnen, die Netzwerkisolation über AWS- und lokale Umgebungen hinweg aufrechtzuerhalten. Jedes Segment erstellt eine dedizierte Routingdomäne. Sie können innerhalb Ihres globalen Netzwerks mehrere Netzwerksegmente erstellen. Cloud WAN schränkt die Kommunikation der AWS-Ressourcen innerhalb des Segments ein. Kurz gesagt ermöglicht Ihnen Cloud WAN die Weiterleitung des Datenverkehrs zwischen:

- VPCs im selben Segment und in derselben Region (isolierte Anhänge).
- VPCs in verschiedenen Segmenten derselben Region.
- VPCs im selben Segment über verschiedene Regionen hinweg (isolierte Anhänge).
- VPCs in verschiedenen Segmenten und in verschiedenen Regionen.

Überlegungen vor der Bereitstellung von AWS Cloud WAN:

- Peering zwischen Transit-Gateways und Cloud WAN wird in derselben Region und nicht regionsübergreifend unterstützt.
- Stellen Sie sicher, dass Sie für Anwendungsfälle, die AWS-Site-to-Site-VPN-Verbindungen über Direct Connect mithilfe von privaten IP-Adressen erfordern, Cloud WAN mit einem Transit-Gateway verbinden.
- Achten Sie beim Bereitstellen von Cloud WAN zusammen mit Transit-Gateways darauf, dass sich die ASN des Transit-Gateways von der ASN unterscheidet, die für die Kernnetzwerk-Edges von Cloud WAN verwendet wird.
- Achten Sie beim Erstellen des Kernnetzwerks darauf, dass Sie im Abschnitt mit den Edge-Standorten unter den Richtlinieneinstellungen des Kernnetzwerks alle Regionen hinzufügen, für die Ihre VPCs konfiguriert sind. Sie müssen außerdem Segmente erstellen und unter dem Segmentnamen den Segmenttyp – „dev“ (Entwicklung), „prod“ (Produktion), „management“ (Verwaltung) oder „security“ (Sicherheit) – hinzufügen, zu dem diese Regionen gehören.



AWS Cloud WAN kann mit zwei Methoden bereitgestellt werden:

- **Verbund aus Transit-Gateways und Cloud WAN erstellen** – Bei dieser Methode ersetzen Sie statisch erstellte Transit-Gateway-Peering-Verbindungen durch Cloud WAN. Während Sie einen Verbund von Transit-Gateways und Cloud WAN erstellen, müssen Sie die Transit-Gateways mithilfe des AWS Network Managers registrieren, ein Peering zwischen den Transit-Gateways erstellen, Anhänge für die Transit-Gateways erstellen und dann die Cloud WAN-Konfiguration anwenden.

- **Nur Cloud WAN** – Bei dieser Methode wird Cloud WAN für die gesamte Konnektivität verwendet und Transit-Gateways werden entfernt.

AWS Cloud WAN bereitstellen

Cloud WAN ist die Verbindung zwischen VPCs und lokalen Netzwerken. Im Folgenden soll näher darauf eingegangen werden, wie Sie mithilfe der Cloud NGFWs von Palo Alto Networks den mit Cloud WAN verbundenen Datenverkehr absichern können. Obwohl Cloud WAN ein globales Konstrukt ist, empfiehlt Palo Alto Networks die Bereitstellung von Cloud NGFW in jeder AWS-Region, die es umfasst, um eine Sicherheitslage mit geringer Latenz und optimierten Kosten aufrechtzuerhalten.

Cloud NGFW kann in einer zentralisierten Sicherheits-VPC in jeder Region bereitgestellt werden. Die Sicherheits-VPC kann per Anhang direkt mit dem Cloud-WAN-Sicherheitssegment verbunden werden. Das den Anhängen und Segmenten zugeordnete Routing definiert, wie der Datenverkehr zur Bedrohungsabwehr an die Cloud NGFW-Ressource weitergeleitet wird. Sie können den von Cloud-Anhängen eingehenden Datenverkehr vor der Weiterleitung an das Ziel zur Sicherheits-VPC umleiten. Wenn Cloud NGFW innerhalb einer Region bereitgestellt wird, kann Folgendes geschützt und gesichert werden

- East-West-Datenverkehr mit interregionalen und intraregionalen Datenverkehrsflüssen
- Ausgehender Datenverkehr kann überprüft und gesichert werden
- Datenverkehr aus der lokalen und Zweigstellenumgebung kann überprüft und geschützt werden

Betrachten wir einen Anwendungsfall, bei dem sich VPCs in derselben Region befinden (isolierte Anhänge). Um diese Einrichtung zu konfigurieren, stellen Sie die Cloud NGFW-Firewall innerhalb der Sicherheits-VPC bereit. Sie können die Cloud NGFW-Firewall in einer Sicherheits-VPC bereitstellen, die direkt mit einem Cloud-WAN oder über ein Transit-Gateway mit einem Cloud-WAN-Anhang verbunden ist.

Um eine vollständige Migration vom Transit-Gateway durchzuführen, müssen Sie Ihre VPCs direkt mit dem Cloud-WAN verbinden.

Der ausgehende Datenverkehr von der Produktions-VPC wird an das Cloud-WAN weitergeleitet, von dort aus wird er zur Überprüfung an die Sicherheits-VPC weitergeleitet und über das NAT-Gateway und das interne Gateway gesendet. In der umgekehrten Richtung erreicht der Datenverkehr von der Sicherheits-VPC das Sicherheitssegment und wird dann basierend auf der Routing-Konfiguration an den VPC-Anhang gesendet.

Um den Datenverkehr zwischen VPCs im selben Segment und in derselben Region mit einer Bereitstellung von **AWS Cloud WAN (ausschließlich)** zu prüfen, führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich beim AWS Network Manager an und **erstellen Sie ein globales Netzwerk**.

2. Erstellen Sie ein Kernnetzwerk und eine Kernnetzwerkrichtlinie.

   Verwenden Sie die AWS Cloud WAN-Konsole, um eine Kernnetzwerkrichtlinienversion zu erstellen, indem Sie die folgenden Schritte ausführen:

   - Konfigurieren Sie die Netzwerkeinstellungen.

     - Klicken Sie zum Bearbeiten einer Richtlinienversion auf **Policy versions (Richtlinienversionen)**, wählen Sie die gewünschte Richtlinie aus und klicken Sie auf **Edit (Bearbeiten)**. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Create Policy (Richtlinie erstellen)**.

     - Nachdem sich der Änderungssatzstatus der Richtlinienversion in **Ready to execute (Bereit zur Ausführung)** geändert hat, führen Sie die Richtlinie aus, indem Sie auf **View or apply change set (Änderungssatz anzeigen oder anwenden)** klicken. Klicken Sie alternativ auf **Compare policy version (Richtlinienversion vergleichen)**, um das JSON-Dokument anzuzeigen.

   - • Erstellen Sie Netzwerkrichtliniensegmente innerhalb Ihres Kernnetzwerks.

     Achten Sie beim Konfigurieren der Richtlinienversionen darauf, dass Sie die Anwendungen hinzufügen: APP VPC 1 (10.1.0.0/16) und APP VPC 2 (10.2.0.0/16) im Produktionssegment und in der Firewall sowie die Sicherheits-VPC (100.64.0.0/16) im Sicherheitssegment.

     - Erstellen Sie Segmentfreigabe- und Segmentroutenaktionen.

     - Erstellen Sie Richtlinienanhänge.

     Sie können wahlweise dem Segment (Schlüssel) Tags wie „prod segment“ (Wert) hinzufügen. Diese Tags werden erst angezeigt, nachdem Sie die Segmente im Cloud-WAN hinzugefügt haben.

3. Erstellen Sie einen Anhang.

   - *Verwenden Sie beim Erstellen eines Anhangs die VPC- oder Transit-Gateway-Routentabelle als Anhangstyp.*
   - *Um sicherzustellen, dass die Cloud NGFW-Firewall den zwischen VPC-Anhängen weitergeleiteten Datenverkehr prüfen kann, müssen Sie den Appliance-Modus im VPC-Anhang für die Sicherheits-VPC aktivieren, die die Cloud NGFW-Firewall enthält.*

4. Aktualisieren Sie VPC-Routentabellen.

   Nachdem die erforderlichen Cloud-WAN-Konstrukte nun vorhanden sind, müssen die VPCs angepasst werden, um die Paketweiterleitung zum Kernnetzwerk zu erleichtern. Die Anwendungs- und Firewall-Instanzen oder die jeweiligen VPCs müssen mit ähnlichen Tags wie das Segment gekennzeichnet werden. Fügen Sie dem Anhang spezifische Tags hinzu, damit er mit dem Anhang übereinstimmt, der während Schritt 2, Erstellen Sie Richtlinienanhänge, erstellt wurde.

Um die Kommunikation zwischen angeschlossenen VPCs und dem Kernnetzwerk zu ermöglichen, müssen die VPC-Routentabellen von der vorhandenen Ziel-Transit-Gateway-Route auf den entsprechenden Kernnetzwerk-ARN aktualisiert werden, wie unten veranschaulicht.

Weg eines Pakets

Im Folgenden ist der Weg eines Pakets beschrieben, wenn eine EC2-Instanz in APP VPC 1 mit einer EC2-Instanz in APP VPC 2 kommuniziert:

- Wenn ein Client in APP VPC 1 (10.1.0.0/16) eine Verbindung zu einem Server in APP VPC 2 (10.2.0.0/16) beginnt, führt er eine Suche in der VPC-Routentabelle (App-Subnetz) durch. Das Paket stimmt mit dem Standardrouteneintrag überein, wobei der ARN des Kernnetzwerks als Ziel angegeben ist, und wird an das Kernnetzwerk weitergeleitet.
- Wenn das Paket im Kernnetzwerk ankommt, führt es eine Suche in der Routentabelle des Produktionssegments durch, da APP VPC 1 dem Produktionssegment zugeordnet ist. Das Paket stimmt mit dem Standardeintrag überein, wobei der Sicherheitsanhang als Ziel angegeben ist, und wird an die Sicherheits-VPC weitergeleitet.

- Wenn das Paket beim Sicherheits-VPC-Anhang (100.64.0.0/16) ankommt, führt es eine Suche in der VPC-Routentabelle (CWAN-Subnetz) durch. Das Paket stimmt mit der Standardroute überein, wobei Firewall-Endpunkt 1 als Ziel angegeben ist, und wird – zunächst über den Endpunkt der Firewall zur Überprüfung – an eine Firewall weitergeleitet.
- Die Firewall prüft den Datenverkehr, vergleicht ihn mit ihrer Sicherheitsrichtlinie und lässt ihn durch. Die Firewall leitet das Paket zurück an den Endpunkt der Firewall, wo es eine Suche in der VPC-Routentabelle (Firewall-Subnetz) durchführt. Das Paket stimmt mit dem Standardrouteneintrag überein, wobei der ARN des Kernnetzwerks als Ziel angegeben ist, und wird an das Kernnetzwerk weitergeleitet.
- Wenn das Paket im Kernnetzwerk ankommt, führt es eine Suche in der gemeinsamen Sicherheitsroutentabelle durch, da die Sicherheits-VPC dem Sicherheitssegment zugeordnet ist. Das Paket stimmt mit dem APP VPC 2 CIDR(10.2.0.0/16)-Eintrag überein, wobei der APP VPC 2-Anhang als Ziel angegeben ist, und wird an APP VPC 2 weitergeleitet.

- Wenn das Paket bei APP VPC 2 ankommt, führt es eine Suche in der VPC-Routentabelle (CWAN-Subnetz) durch. Das Paket stimmt mit dem VPC CIDR-Eintrag überein, wobei „local“ (lokal) als Ziel angegeben ist, und wird an die Instanz weitergeleitet.

Der zurückgegebene Datenverkehr folgt demselben Weg in die entgegengesetzte Richtung.

Sicherheitsfunktionen in Cloud NGFW für AWS

Cloud NGFW für AWS bietet Sicherheitsfunktionen. Mögliche Aktionen:

- DNS Security konfigurieren
- WildFire in Cloud NGFW für AWS konfigurieren

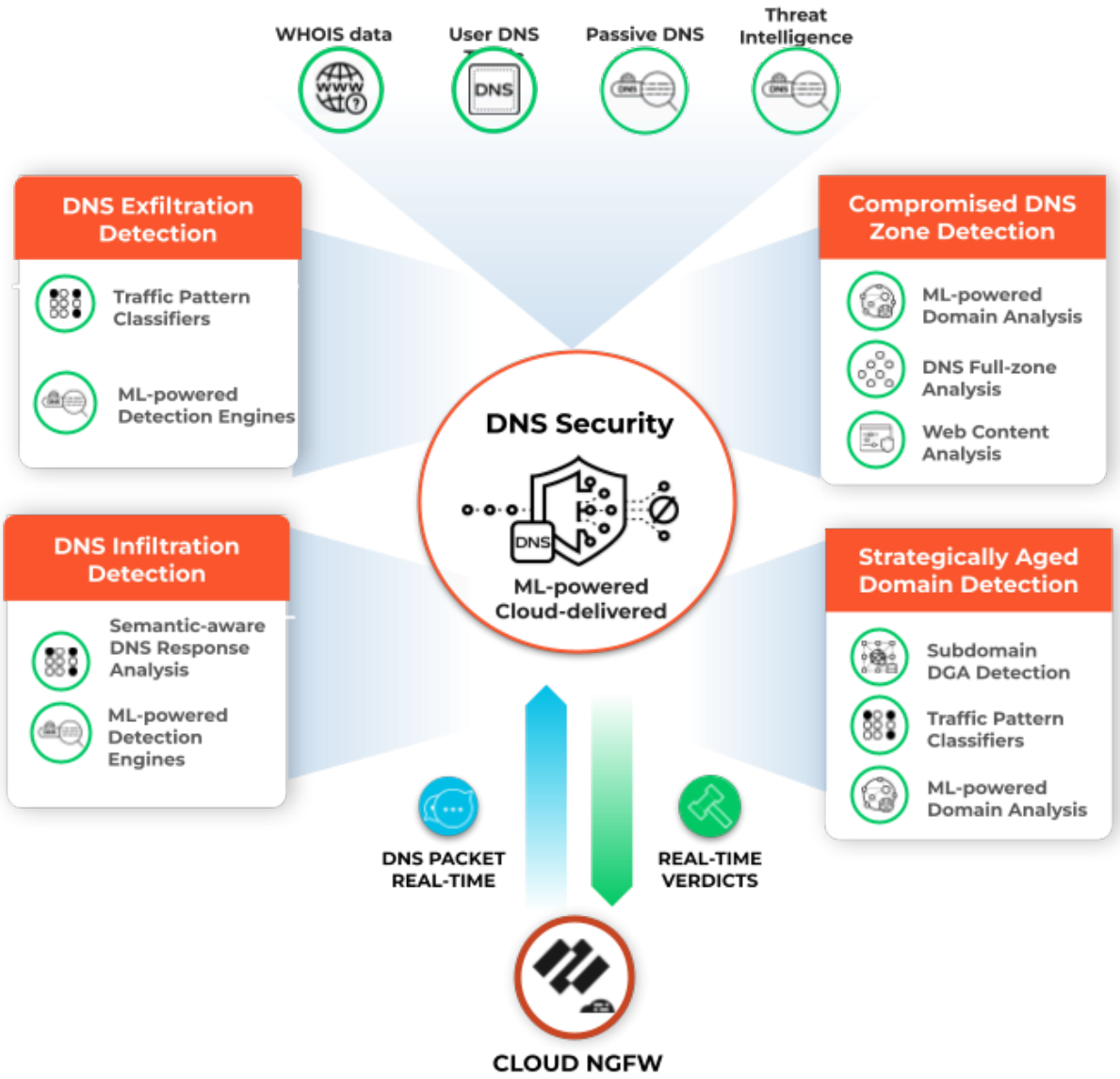
DNS Security konfigurieren

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.

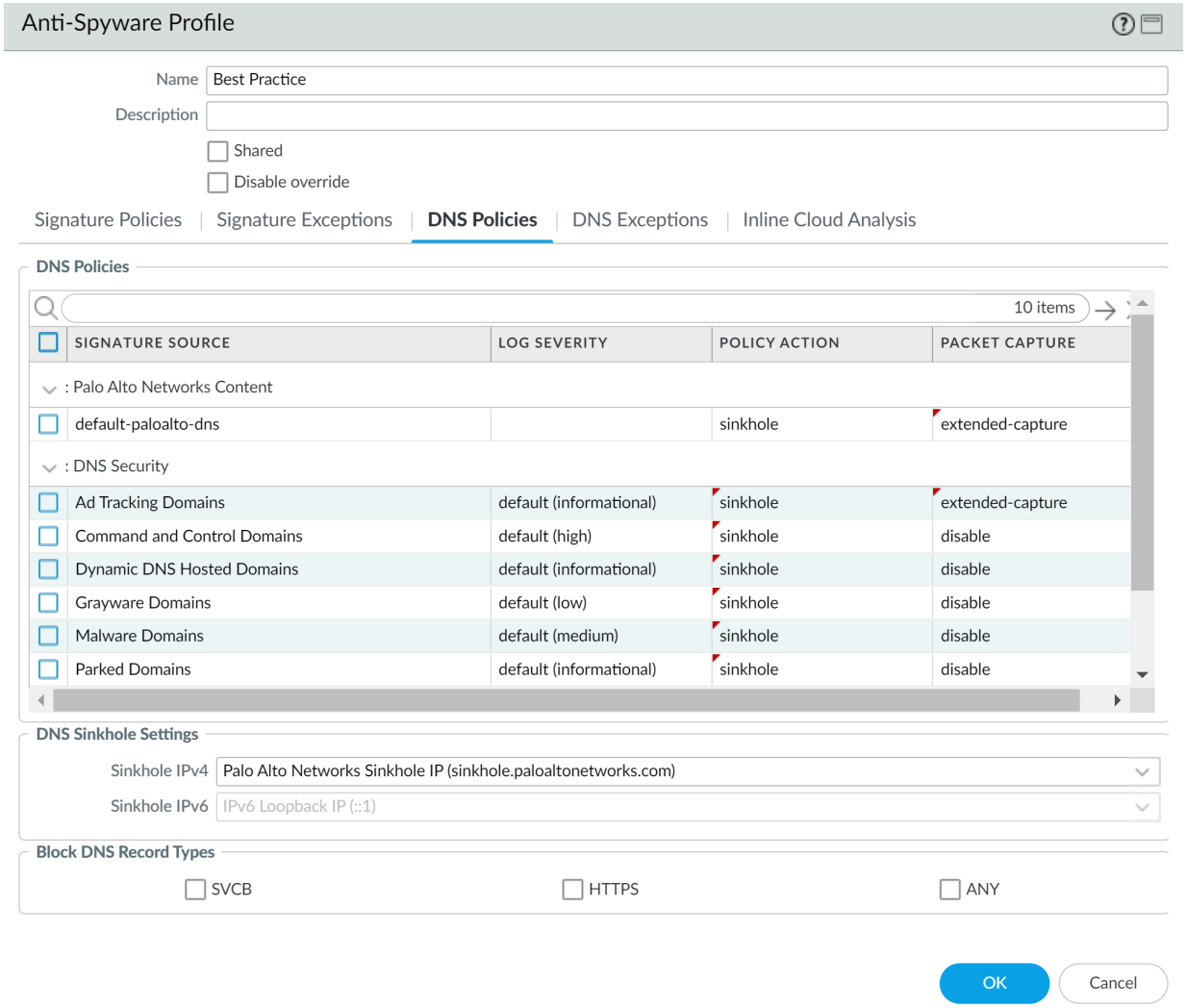
Cloud NGFW verwendet den DNS Security-Dienst von Palo Alto Networks, der bösartige Domänen proaktiv erkennt, indem er DNS-Signaturen mithilfe von erweiterten prädiktiven Analysen und maschinellem Lernen generiert und dazu Daten aus mehreren Quellen verwendet (z. B. WildFire-Verkehrsanalysen sowie Analysen 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

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



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

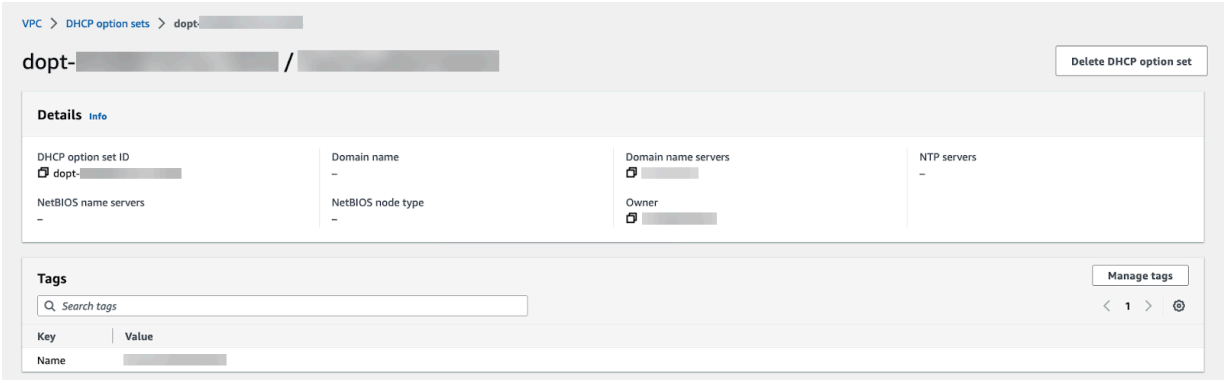
Privater DNS-Server

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.

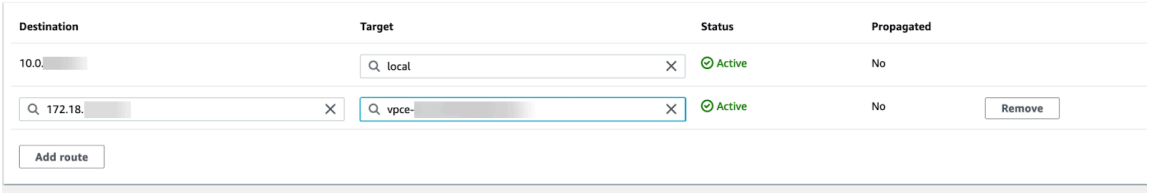
STEP 6 | Wählen Sie unter **DHCP settings (DHCP-Einstellungen)** aus der Dropdown-Liste **DHCP option set (DHCP-Optionssatz)** den für Ihren privaten DNS-Server konfigurierten DHCP-Optionssatz aus.

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.

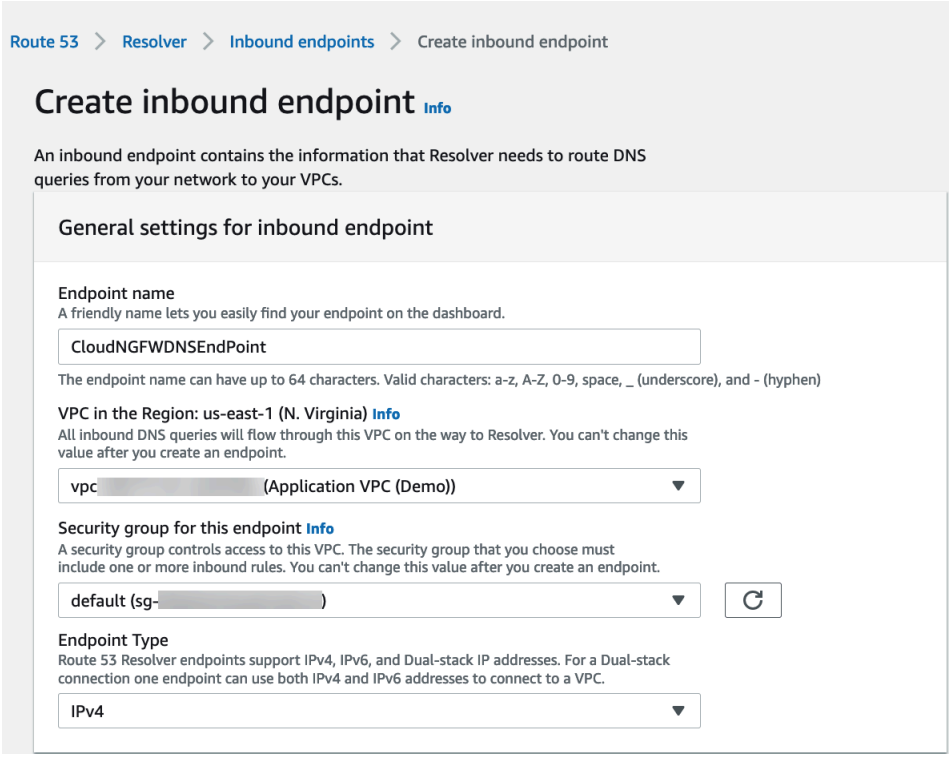
DNS-Dienst Route 53

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.

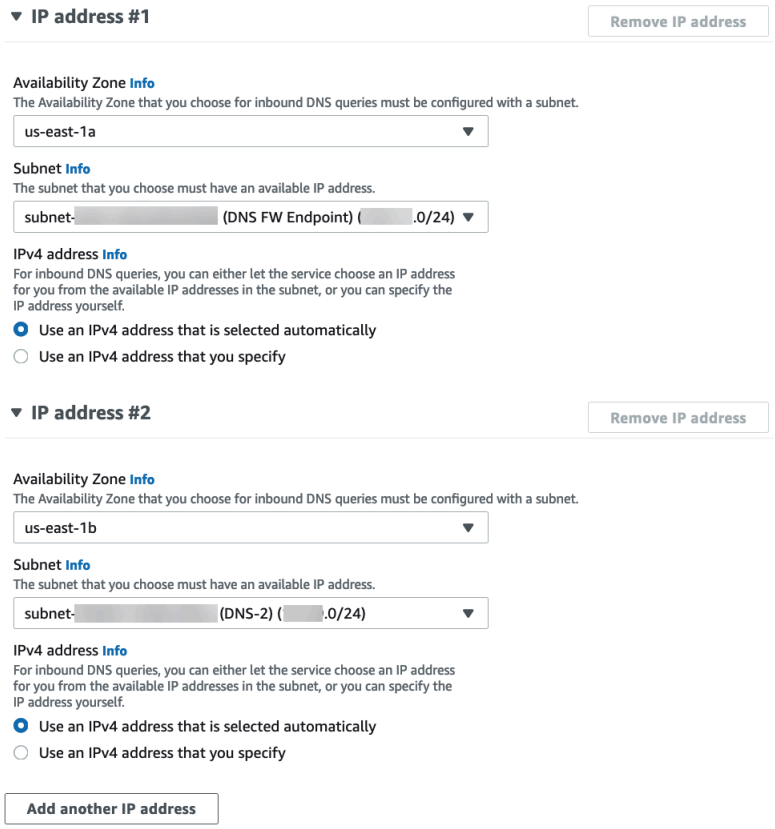
STEP 2 | Erstellen Sie einen eingehenden Endpunkt.

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.

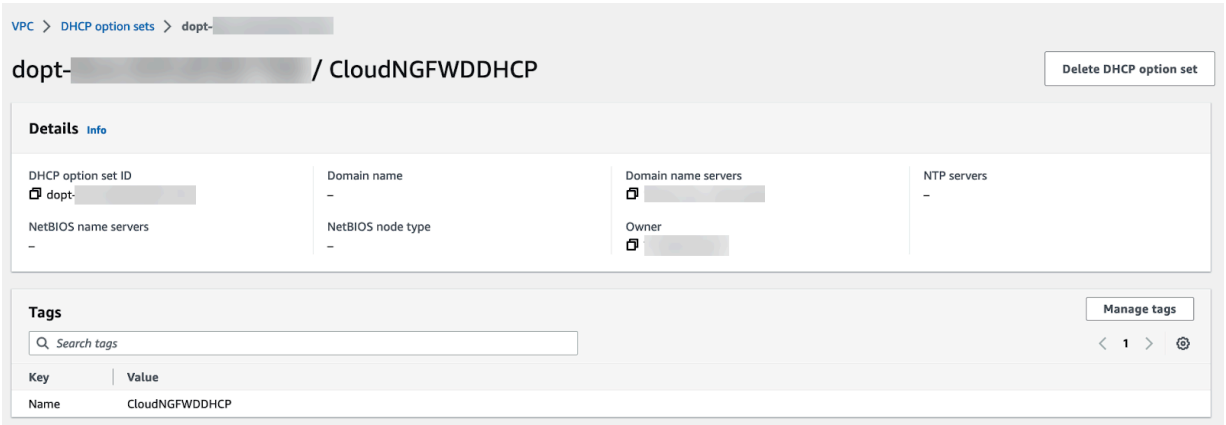
Wenn mehr als eine Verfügbarkeitszone vorhanden ist, müssen Sie jeweils die Verfügbarkeitszone und das entsprechende Subnetz angeben.



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.

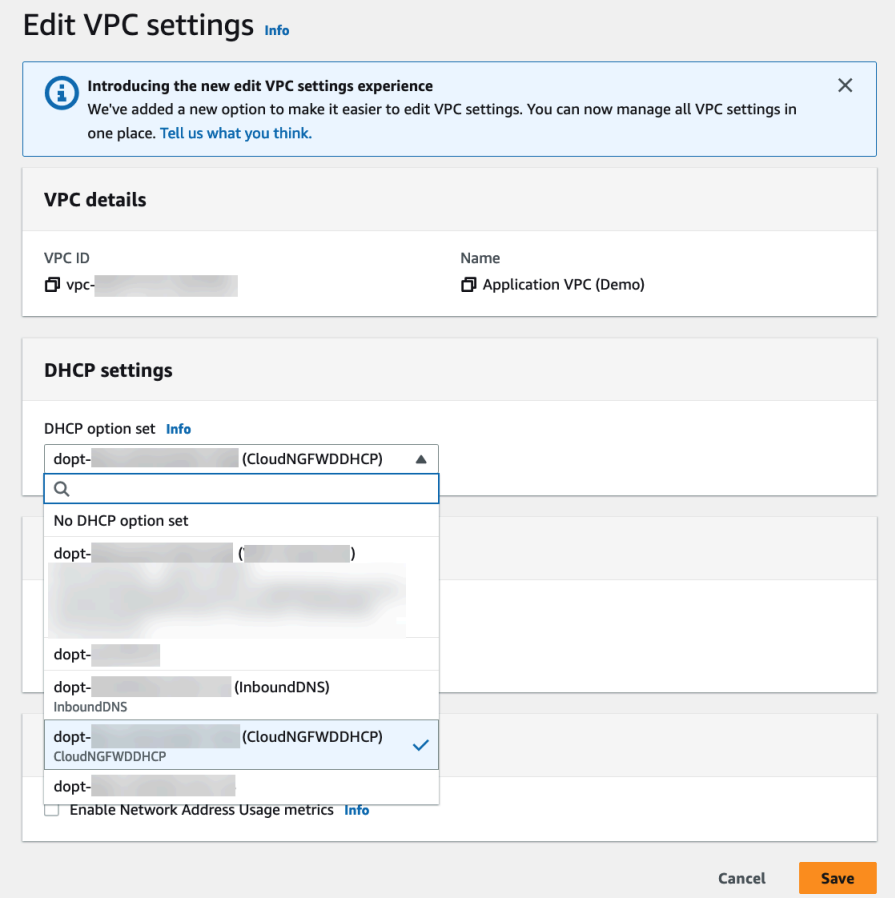
STEP 4 | Sie können einen neuen DHCP-Optionssatz erstellen und die IP-Adresse für jede Verfügbarkeitszone hinzufügen. Wenn mehrere Verfügbarkeitszonen vorhanden sind, geben Sie alle IP-Adressen als durch Kommas getrennte Liste ein.



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.

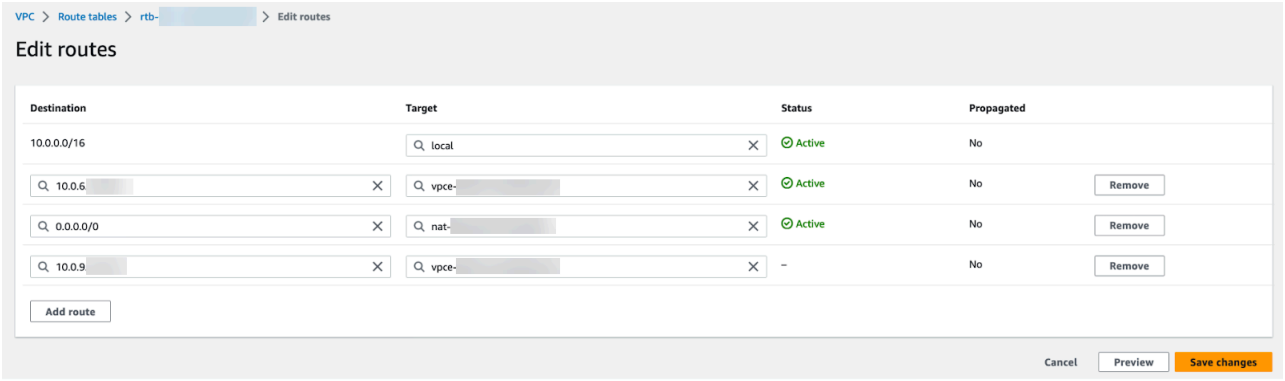


STEP 8 | Klicken Sie auf **Änderungen speichern**.

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

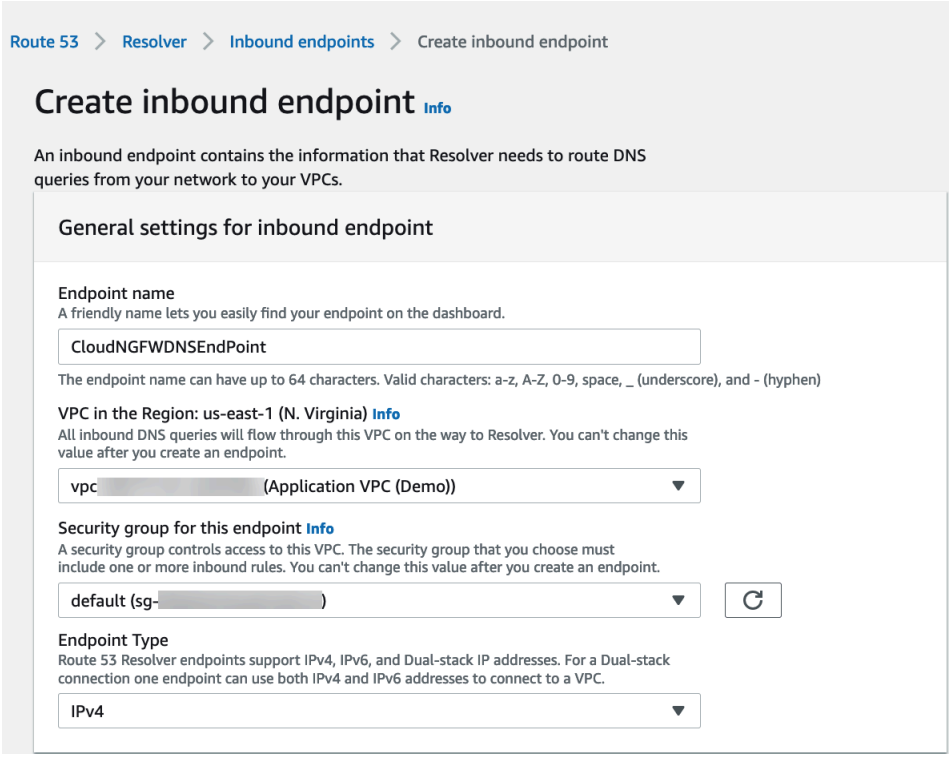
Informationen zum Erstellen einer privaten gehosteten Zone in AWS finden Sie unter Private gehostete Zone erstellen.

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.

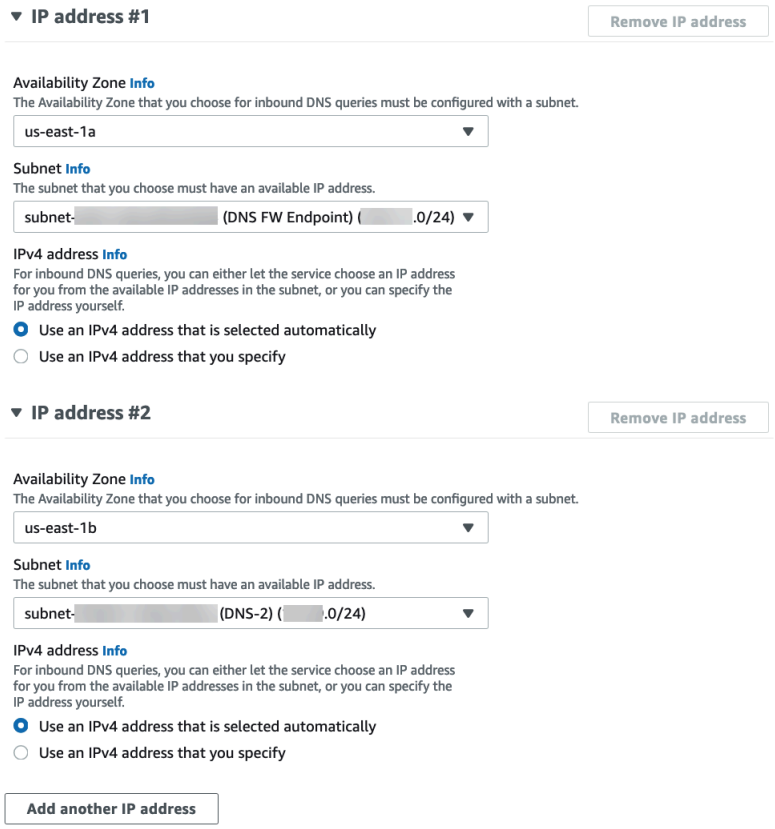
STEP 2 | Erstellen Sie einen eingehenden Endpunkt.

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.

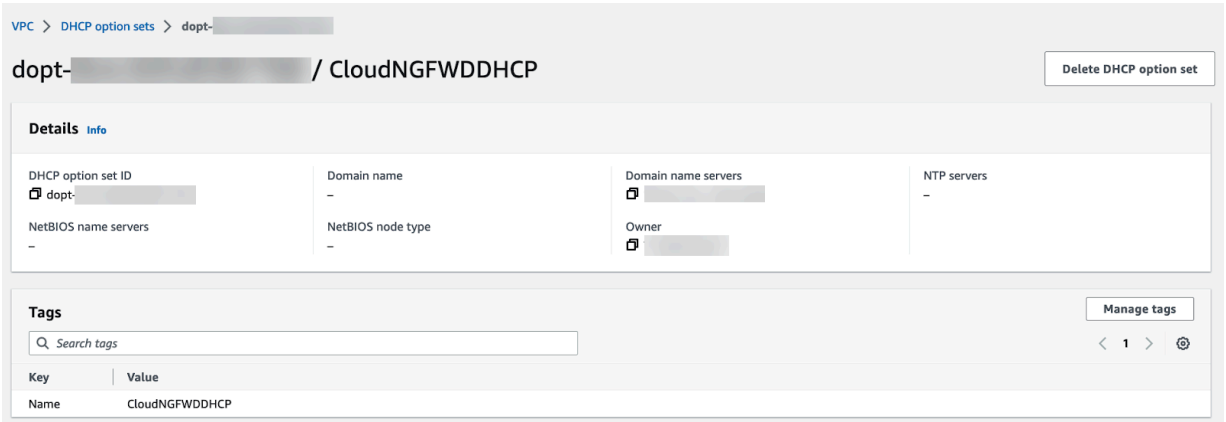
Wenn mehr als eine Verfügbarkeitszone vorhanden ist, müssen Sie jeweils die Verfügbarkeitszone und das entsprechende Subnetz angeben.



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.

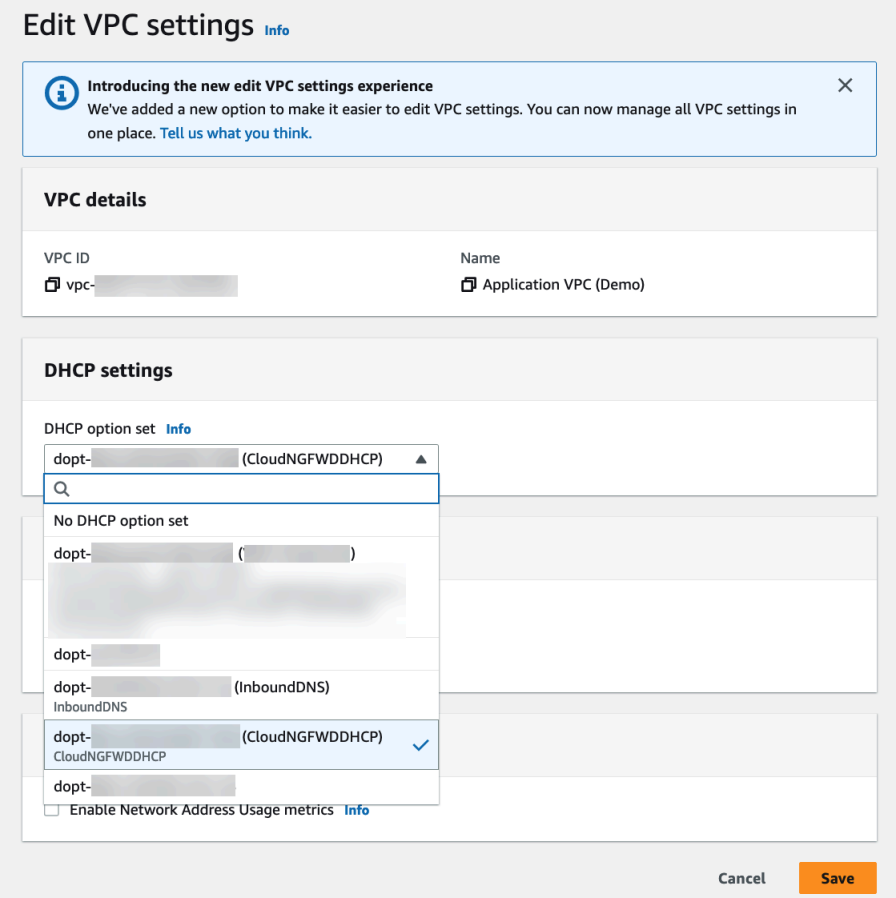
STEP 4 | Sie können einen neuen DHCP-Optionssatz erstellen und die IP-Adresse für jede Verfügbarkeitszone hinzufügen. Wenn mehrere Verfügbarkeitszonen vorhanden sind, geben Sie alle IP-Adressen als durch Kommas getrennte Liste ein.



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.

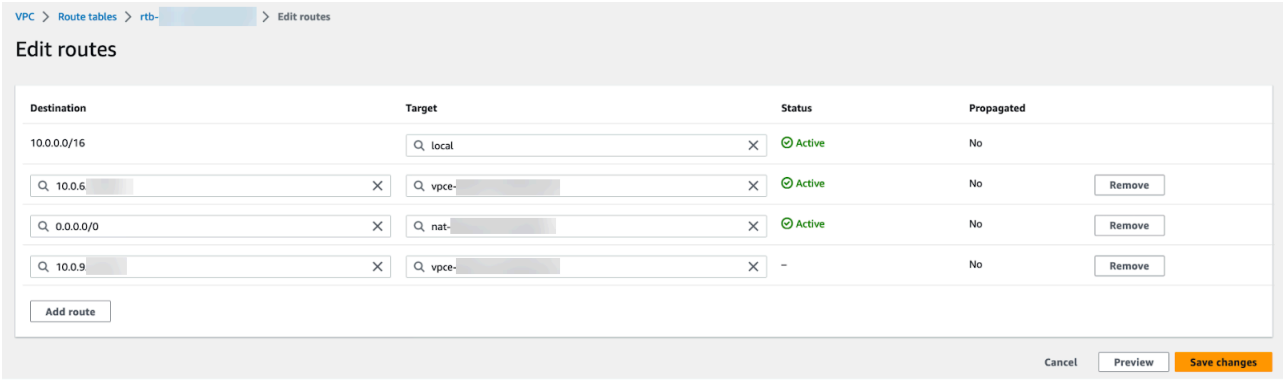
STEP 7 | Wählen Sie unter **DHCP settings (DHCP-Einstellungen)** den oben erstellten DHCP-Optionssatz aus der Dropdown-Liste **DHCP option set (DHCP-Optionssatz)** aus.



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**.

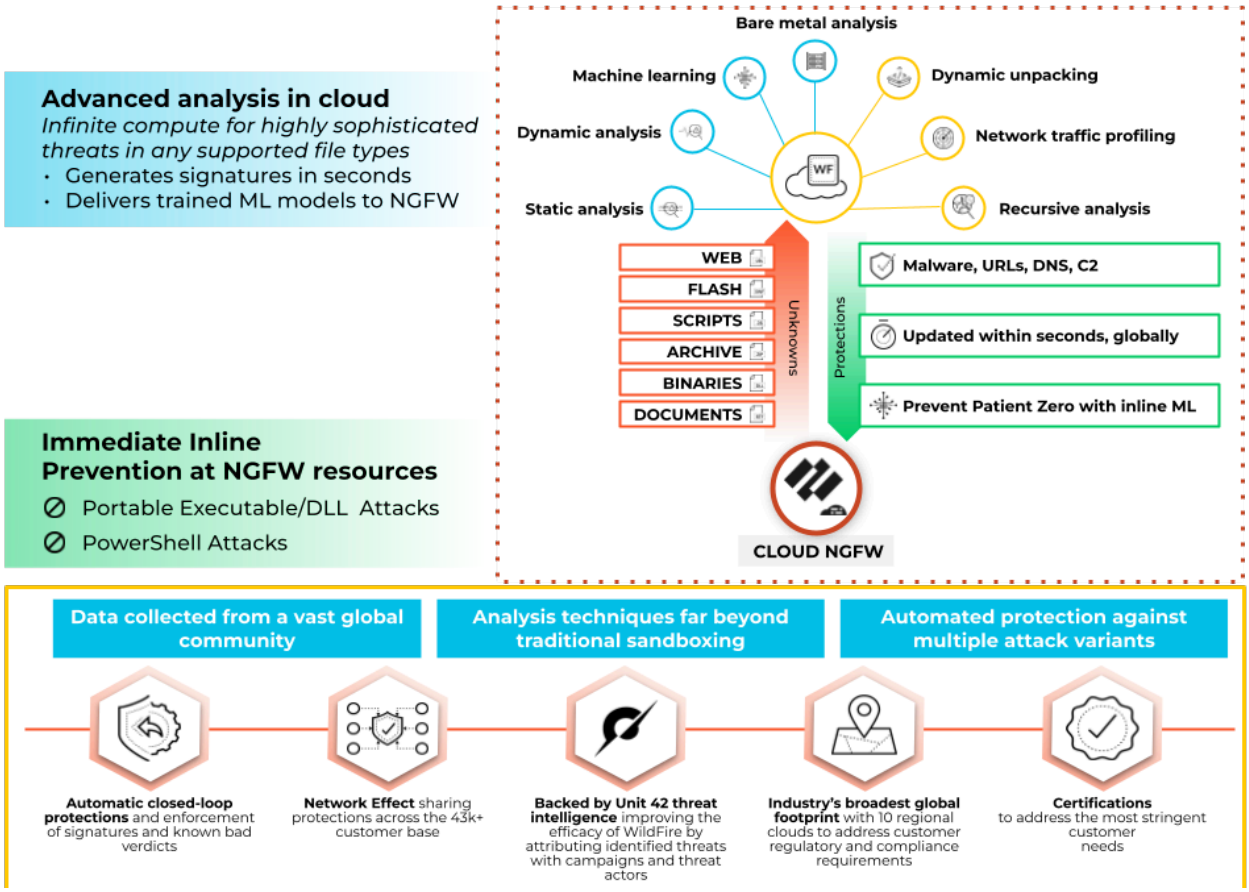
   Jeglicher DNS-Datenverkehr aus dem geschützten Subnetz wird über den Cloud NGFW-Endpunkt und zur Überprüfung und Durchsetzung an die Cloud NGFW weitergeleitet.

WildFire in Cloud NGFW für AWS konfigurieren

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™ (WF) 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 Umgehungstechniken von Angreifern verhindert.



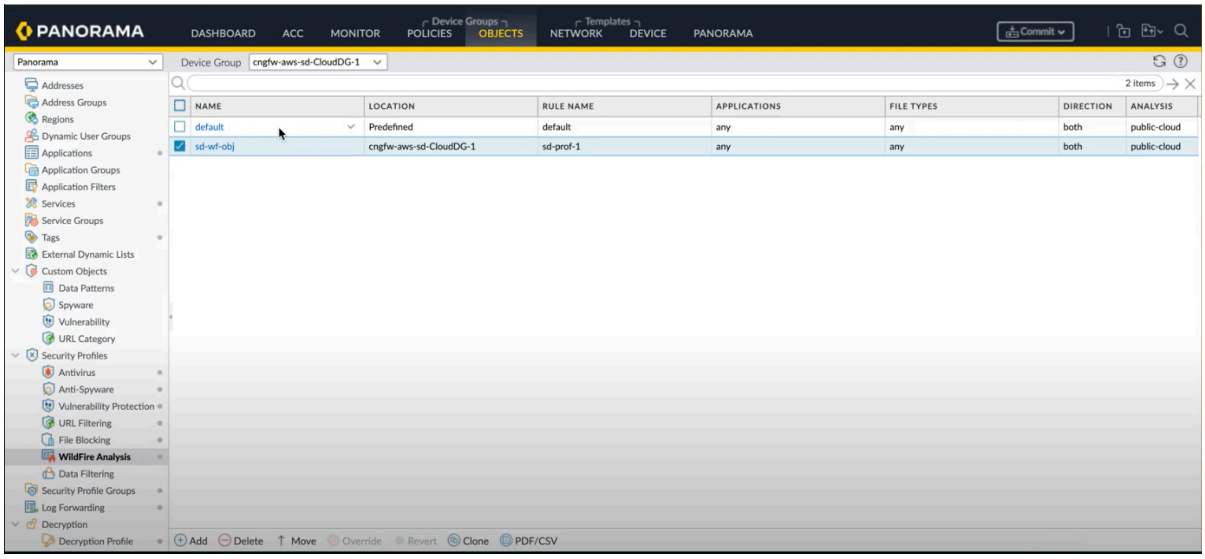
Um WildFire auf Ihrer Cloud NGFW AWS-Ressource zu konfigurieren, müssen Sie wie folgt vorgehen:

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

Konfigurieren Sie ein WildFire-Profil

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

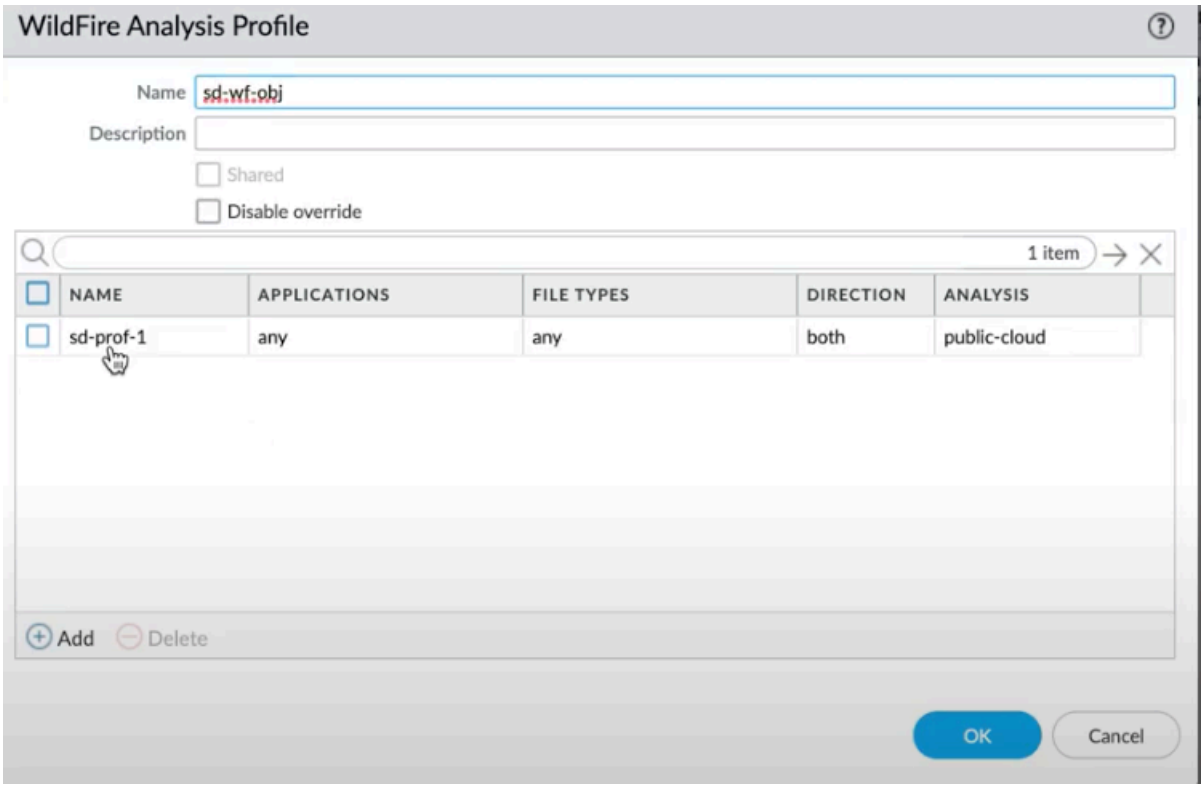
STEP 4 | Geben Sie einen **Namen** für das WildFire-Profil ein und klicken Sie auf **Add (Hinzufügen)**.

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/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 **Policies (Richtlinien)**.

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.

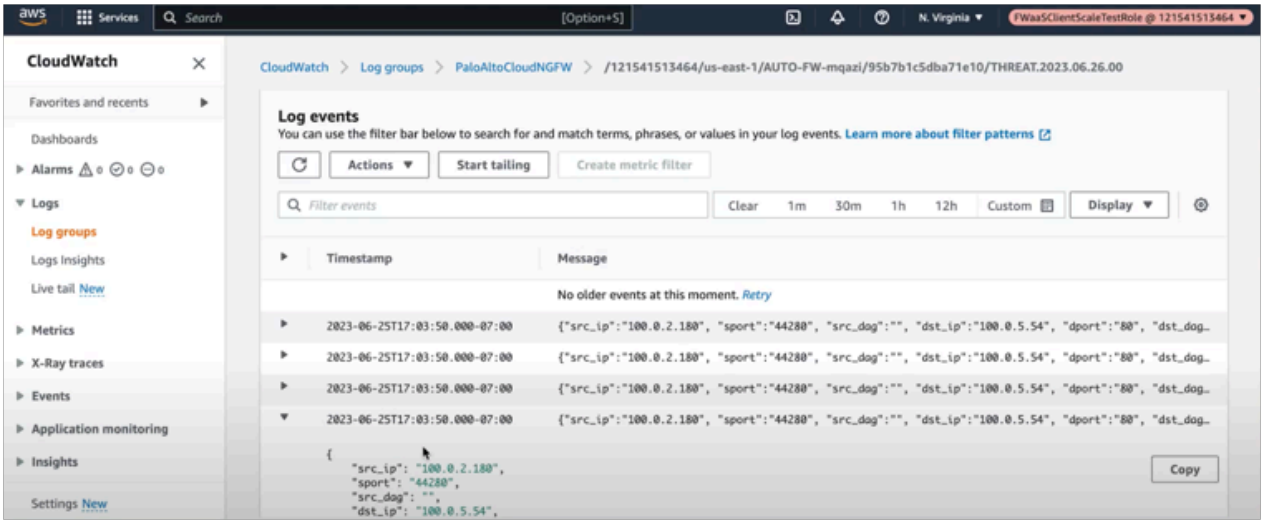
WildFire-Übermittlungsprotokolle anzeigen

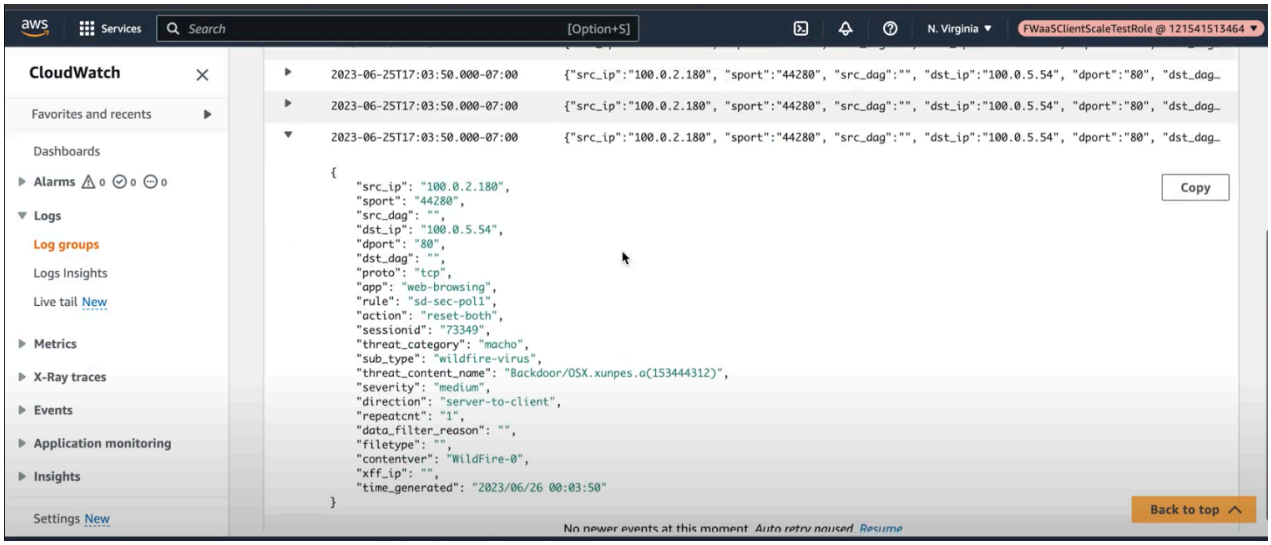
Die Anzeige von WildFire-Übermittlungsprotokollen ist möglich in:

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

Protokolle in AWS-Zielen anzeigen

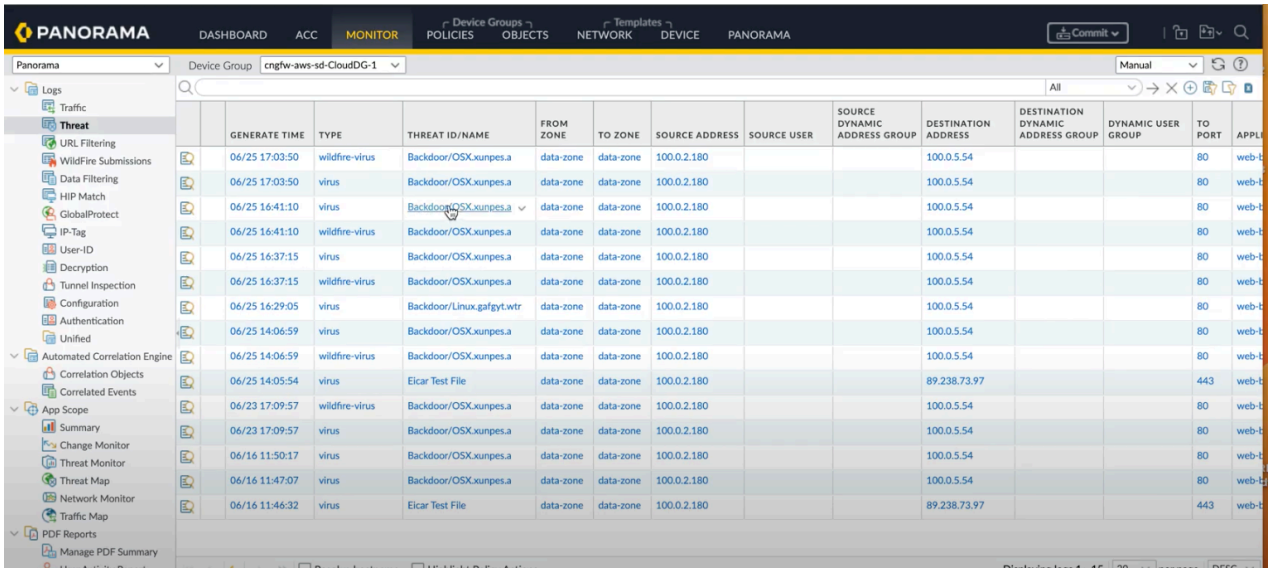
Wenn Sie zuvor Amazon CloudWatch, Amazon S3 oder Amazon Kinesis als Ihr Protokollziel konfiguriert haben, können Sie diese mit WildFire auf Blöcke mit bösartigem Datenverkehr überprüfen.





Protokolle in Panorama anzeigen

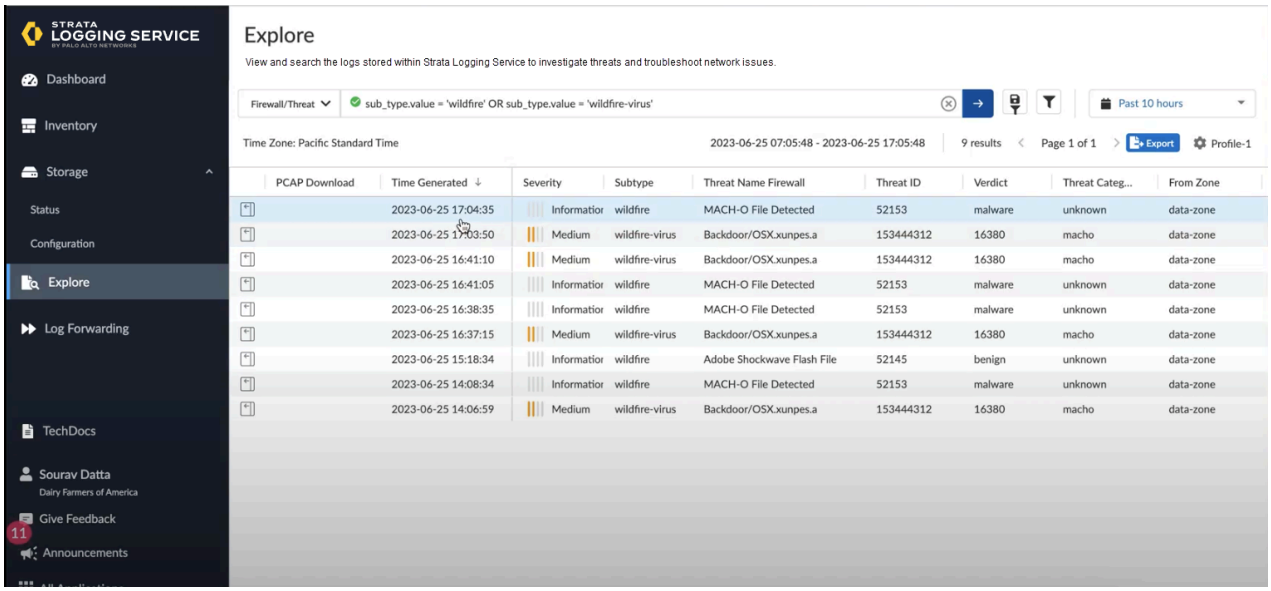
In Panorama können Sie die Protokolle zur Gerätegruppe über **Monitor (Überwachen)** > **Threats (Bedrohungen)** anzeigen.



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.

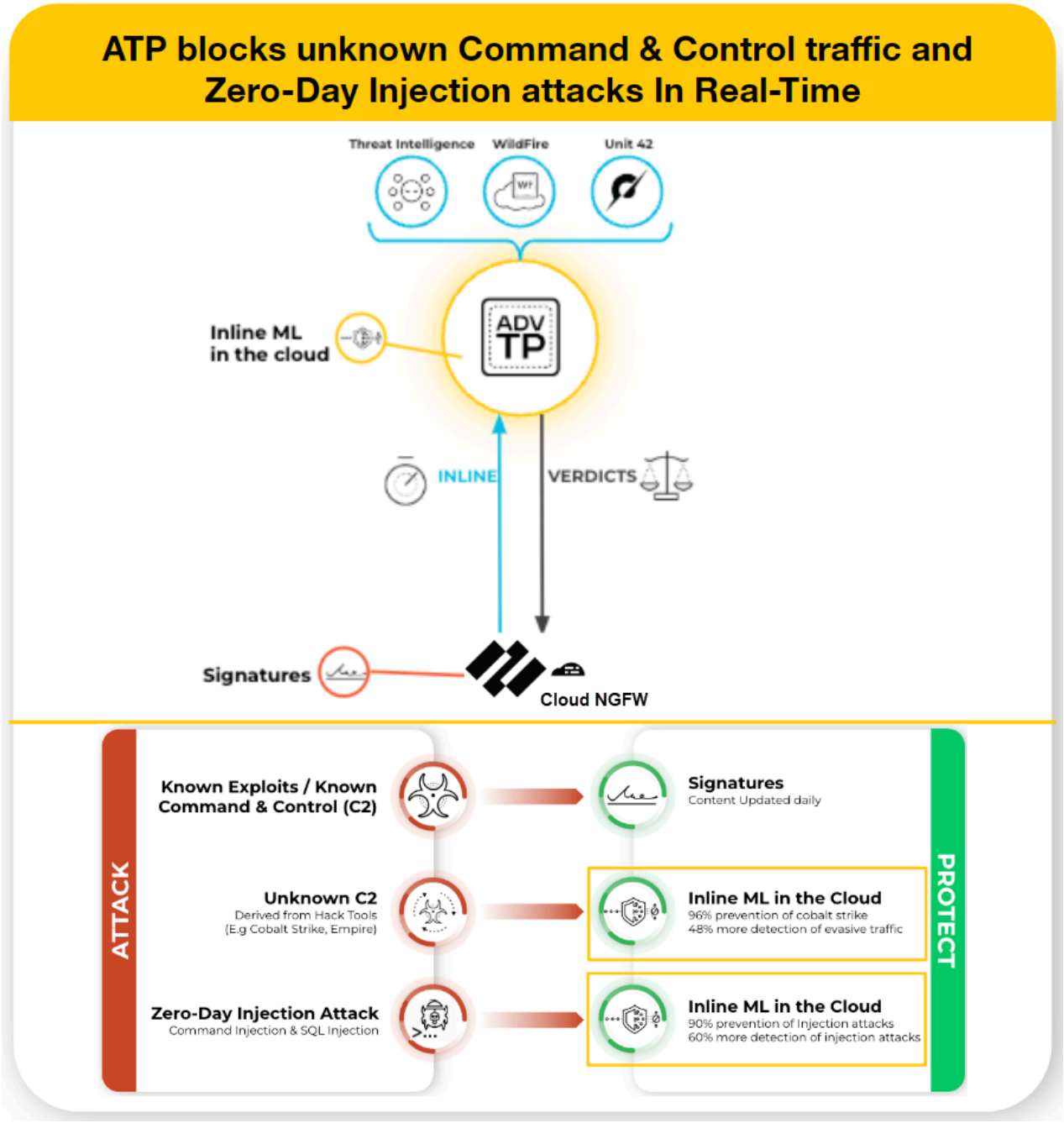


Advanced Threat Prevention in Cloud NGFW

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.

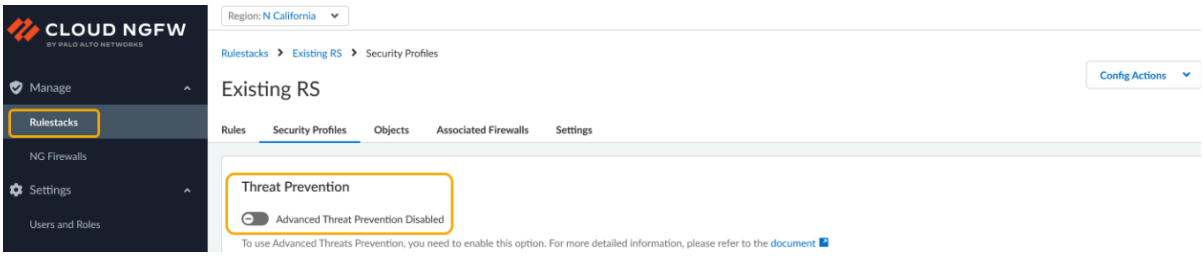
So aktivieren Sie ATP für einen Regelstapel:

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.

Panorama-Richtlinienverwaltung

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.

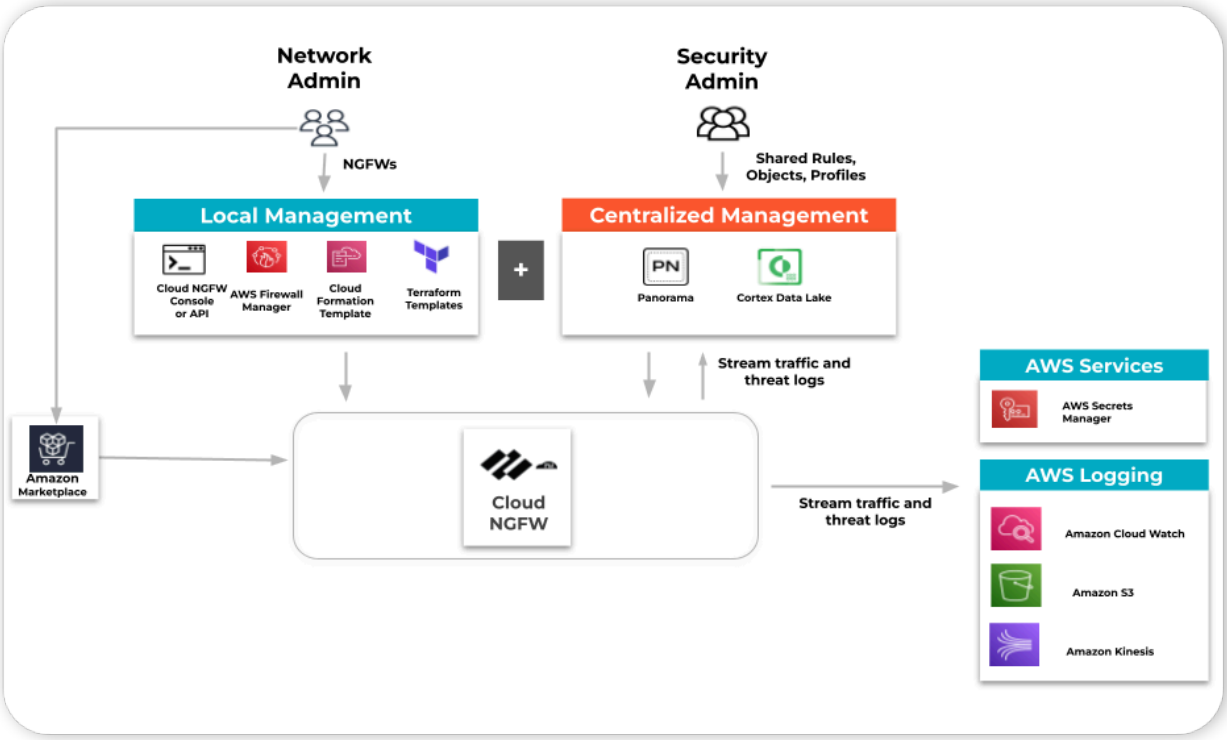
Wie funktioniert die Integration?

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 Cortex Data Lake(CDL)-Konto streamen. Anschließend können Sie die CDL-Benutzeroberfläche, den Panorama-Protokoll-Viewer oder das Application Command Center (ACC) verwenden, um die Protokolle von CDL anzuzeigen und zu analysieren. Panorama verwendet das Cloud Services-Plug-in, um die Protokolle Ihres CDL-Kontos abzufragen.

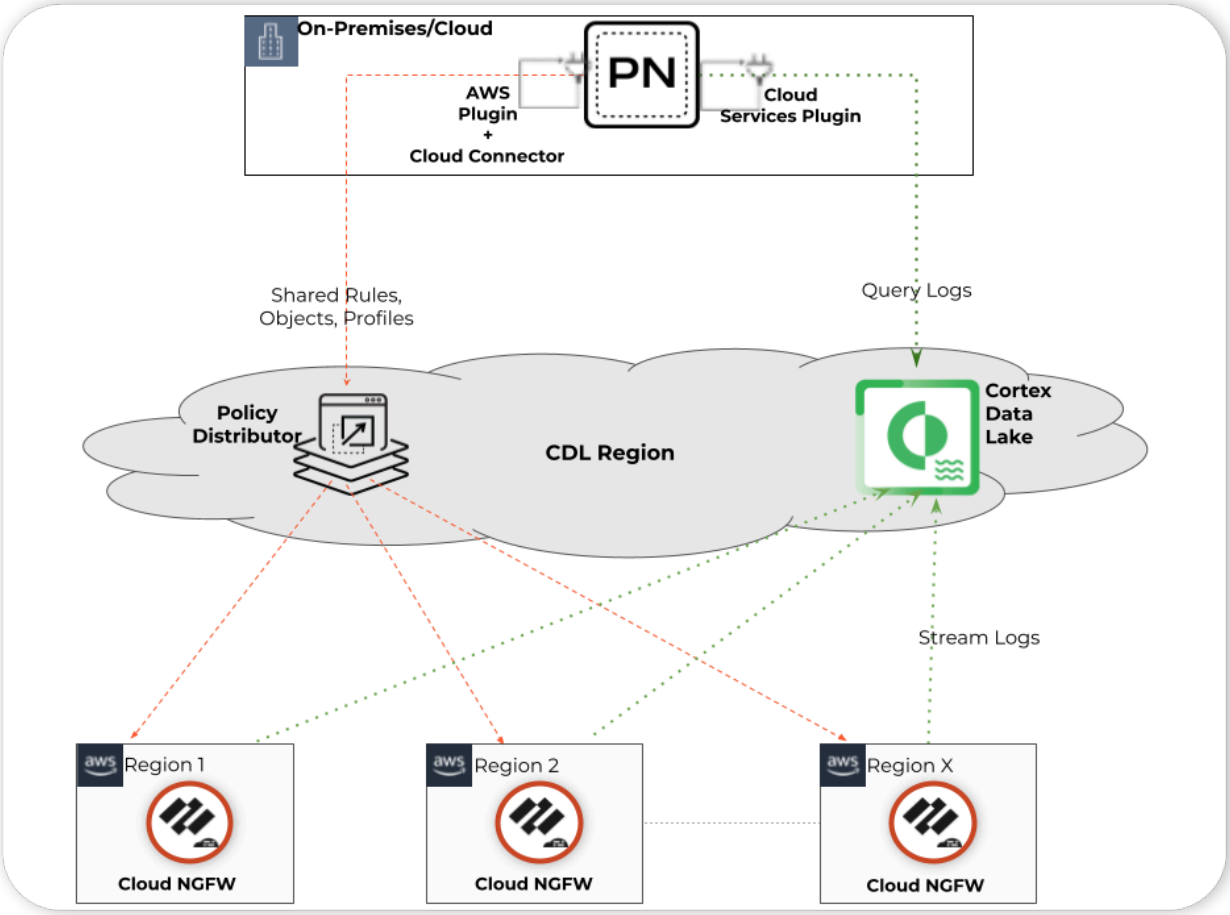
Sie können die Cloud NGFW-Ressourcen auch so konfigurieren, dass Protokolle an AWS-Protokollziele wie S3, CloudWatch und Kinesis-Streams gestreamt werden.



Sie können mehrere Panorama- und CDL-Paare mit dem Cloud NGFW-Mandanten verknüpfen.

Integrationskomponenten

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



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

Palo Alto Networks Log Management ist keine obligatorische Komponente für diese Lösung. Sie verwenden Cortex Data Lake (CDL), 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 Cortex Data Lake und eines der AWS-Protokollziele (S3, CloudWatch oder Kinesis Stream) gesendet werden.

1) Verknüpfen Sie Ihre Panorama-Instanz mit Cortex Data Lake, 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 Cortex Data Lake-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-Vorlagenstapel erstellen, mit denen Sie Richtlinien 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, Cloud DG) sind Panorama-Gerätegruppen für spezielle Zwecke, mit denen Sie Regeln und Objekte für Cloud NGFW-Ressourcen erstellen können. Sie erstellen Cloud-Gerätegruppen mithilfe der Benutzeroberfläche/APIs des Panorama AWS-Plug-ins, indem Sie den Cloud NGFW-Mandanten und die AWS-Regionsinformationen angeben. Eine Cloud-Gerätegruppe manifestiert sich als globaler Regelstapel in diesem Mandanten/dieser Region.

- Mit dem Panorama AWS-Plug-in können Sie mehrere Cloud-Gerätegruppen erstellen.
- Sie können die Gerätegruppenseite der nativen Panorama-Benutzeroberfläche verwenden, um Richtlinien- und Objektkonfigurationen in Cloud-Gerätegruppen und die diesen zugeordneten 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 mehreren Regionen des Cloud NGFW-Mandanten zuordnen. Diese Cloud-Gerätegruppe wird als dedizierter globaler Regelstapel in jeder AWS-Region Ihres Cloud NGFW-Mandanten manifestiert.

Cloud-Vorlagenstapel (Cloud Template Stacks, Cloud TS) sind Panorama-Vorlagenstapel für spezielle Zwecke, die es Ihren Sicherheitsregeln in Cloud-Gerätegruppen ermöglichen, auf Objekteinstellungen zu verweisen, die Sie mit Panorama mithilfe von Vorlagen verwalten können. Beim Erstellen einer Cloud-Gerätegruppe können Sie mit dem Panorama AWS-Plug-in einen Cloud-Vorlagenstapel

erstellen oder angeben. Das Plug-in erstellt diesen Cloud-Vorlagenstapel automatisch und fügt ihn der Cloud-Gerätegruppe als Referenzvorlagenstapel hinzu. Von nun an können Sie die Seite „Template Stack“ (Vorlagenstapel) der nativen Panorama-Benutzeroberfläche verwenden, um Ihre Vorlagen zu konfigurieren und sie diesen Cloud-Vorlagenstapeln 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-Vorlagenstapel 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-Vorlagenstapeln keine verwalteten Geräte zu.

Cloud NGFW wird mit mehreren Schritten in Panorama integriert. 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.

Integration von Panorama

Cloud NGFW wird mit mehreren Schritten in Panorama integriert. 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.

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

- Vorbereiten von Panorama für die Verknüpfung mit Cloud NGFW-Mandanten
- Cloud NGFW mit der zentralen Verwaltung von Palo Alto Networks verknüpfen
- Verknüpfte Panorama-Instanz der Cloud NGFW-Ressource zuordnen
- Verknüpfung von Cloud NGFW mit Palo Alto Networks Management aufheben
- Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden
- Cloud NGFW-Protokolle und -Aktivitäten in Panorama anzeigen
- Cloud NGFW-Protokolle und -Aktivitäten im Strata-Protokollierungsdienst anzeigen

Wiederholen Sie die obigen Schritte, wenn Sie mehrere Panorama-Instanzen mit einem Cloud NGFW-Mandanten verknüpfen.

Panorama-Integration vorbereiten

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.

  Sie müssen das Gerätezertifikat auf dem Panorama-Verwaltungsserver installieren, 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 Cortex Data Lake konfigurieren.
- Stellen Sie sicher, dass Sie Cloud NGFW erfolgreich abonniert haben, sodass ein Cloud NGFW-Mandant vorhanden ist. Für eine erfolgreiche Integration in Panorama müssen Sie das Cloud NGFW-Abonnement verwenden.
- 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

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 Cortex Data Lake für die Protokollverwaltung.

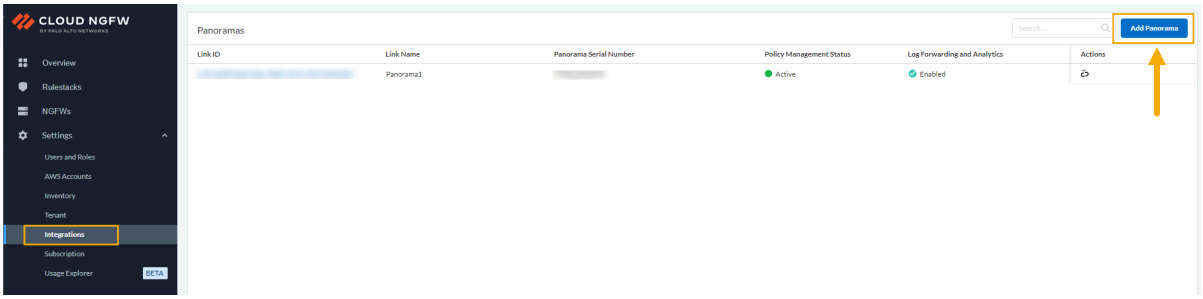
Sie müssen den Cloud NGFW-Dienst mithilfe von AWS Marketplace abonniert *haben, um Cloud NGFW in Panorama zu integrieren. Nachdem Sie Ihren Cloud NGFW-Mandanten mit Panorama verknüpft haben, können Sie die Mandanten und Ressourcen zusammen mit ihrem Status in der Panorama-Konsole unter dem AWS-Plug-in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

Informationen zum Entfernen einer virtuellen Panorama-Appliance aus der Cloud NGFW-Ressource finden Sie unter Verknüpfung von Cloud NGFW mit Palo Alto Networks Management 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.

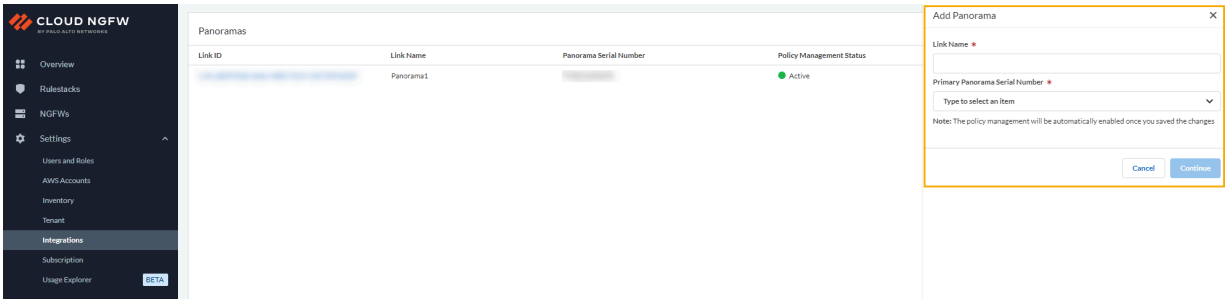
STEP 2 | Klicken Sie auf der Seite **Integrations (Integrationen)** auf **Add Panorama (Panorama hinzufügen)**.



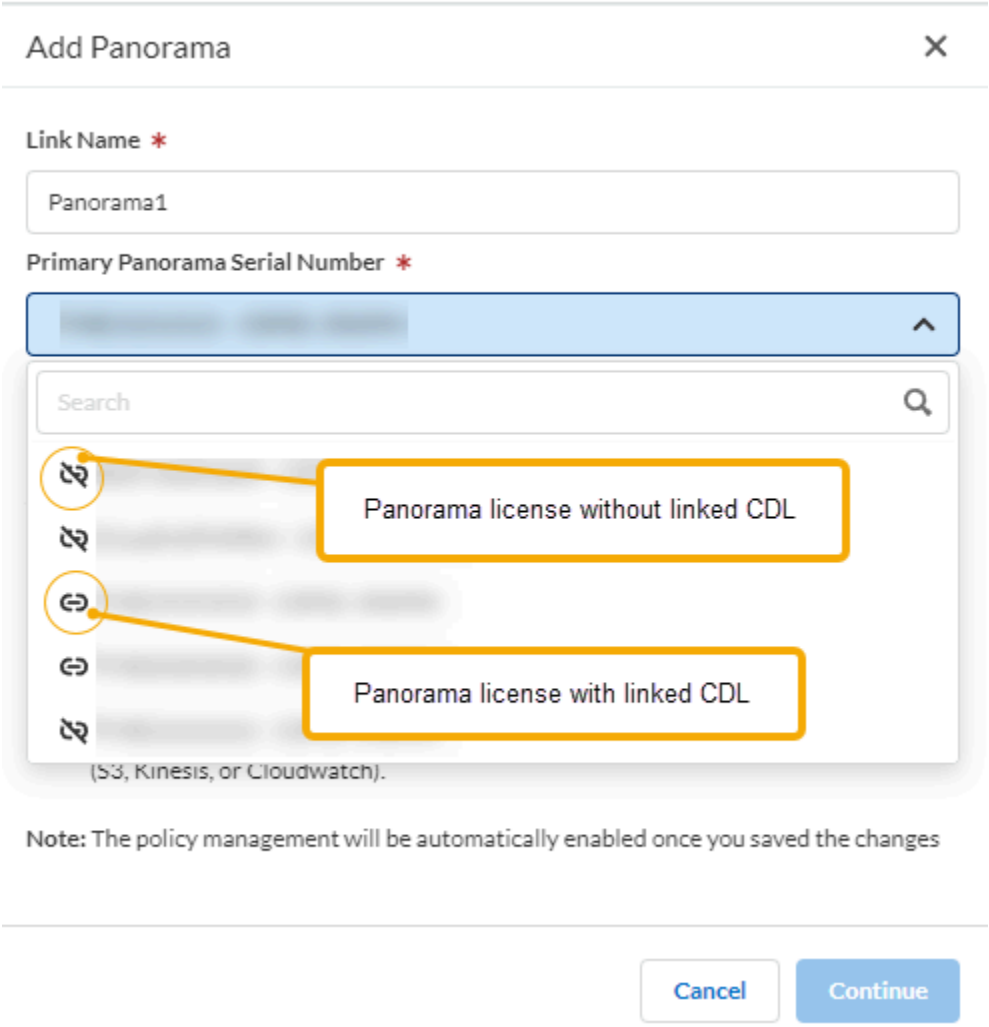
Wenn Sie einen Mandanten verwenden, der mit Panorama verknüpft ist und mit dem AWS Firewall Manager erstellt wurde, können Sie die Verknüpfung der Cloud NGFW-Ressource nicht aufheben.

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.



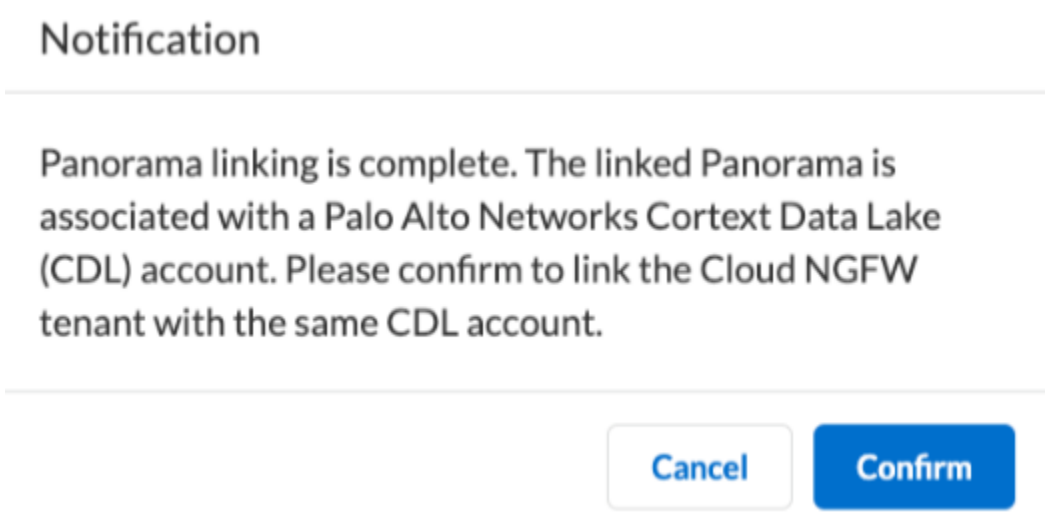
Auf diesem Bildschirm werden zwei verschiedene Symbole angezeigt, die den Status der Panorama-Lizenz beschreiben: eine mit CDL verknüpfte Panorama-Lizenz und eine Panorama-Lizenz, die nicht mit CDL verknüpft ist. In der folgenden Abbildung sind diese Symbole veranschaulicht:



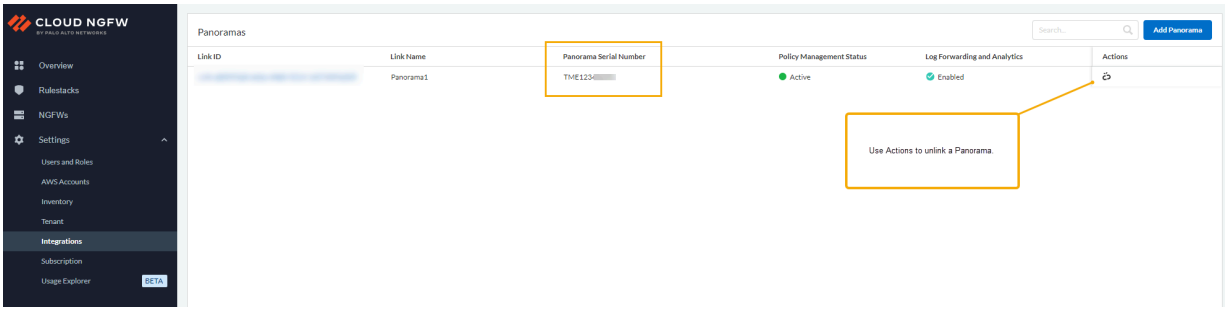
Wenn Sie eine Panorama-Seriennummer auswählen, die nicht mit CDL verknüpft ist, haben Sie die Option, den Verknüpfungsvorgang abzubrechen. In diesem Fall stimmen Sie zu, eine CDL-Lizenz zu

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 CDL verknüpft ist, werden Sie aufgefordert, die Zuordnung zu **bestätigen**, bevor Sie mit dem Integrationsprozess fortfahren:

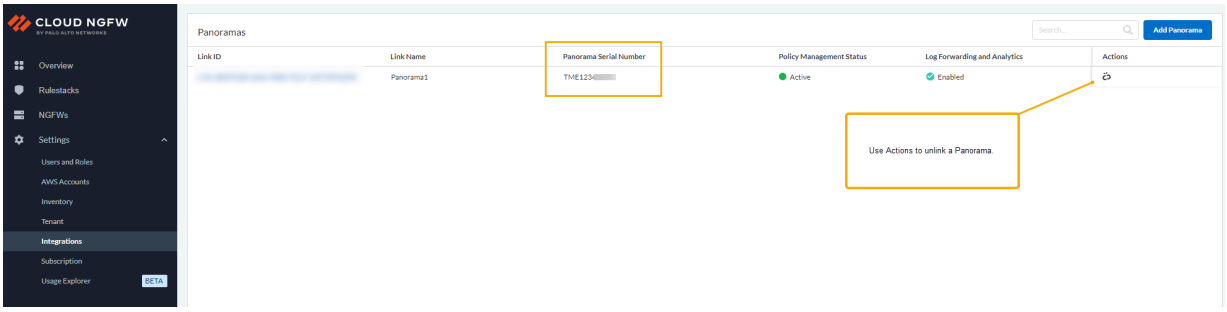


Nachdem Sie die Panorama-Lizenz ausgewählt haben, klicken Sie auf **Continue (Weiter)**. Auf der Seite **Integrations (Integrationen)** werden die **Verknüpfungs-ID** und die verknüpfte **Panorama-Seriennummer** angezeigt:

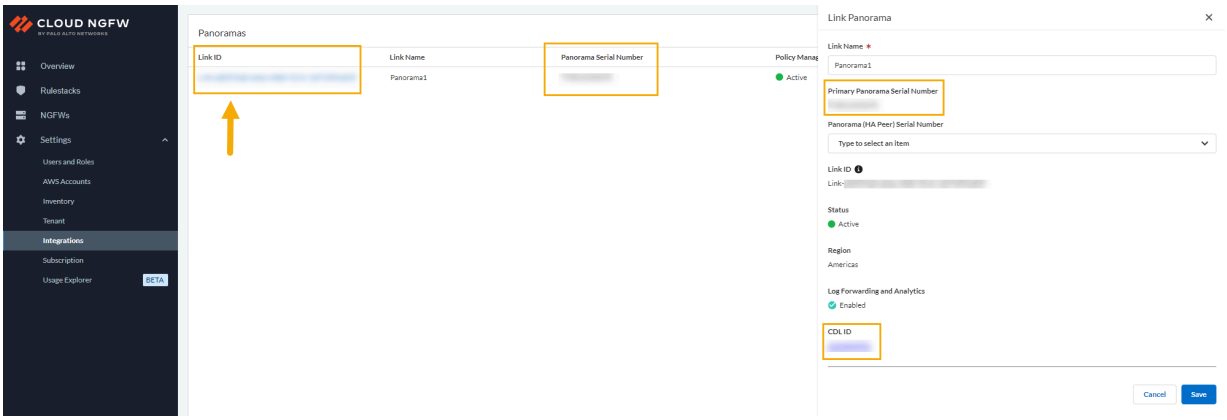


Der Cloud NGFW-Mandant ruft die CDL-Informationen automatisch aus Panorama ab. Wenn Sie nicht vorhaben, CDL für die Protokollierung zu verwenden, können Sie Protokolle an AWS senden. Weitere Informationen finden Sie unter Protokollierung in Cloud NGFW für AWS konfigurieren.

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



Um weitere Informationen zu erhalten, einschließlich der Cortex Data Lake-ID, die der verknüpften Panorama-Instanz zugeordnet ist, klicken Sie auf die **Verknüpfungs-ID** auf der Seite **Integrations (Integrationen)**. 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.

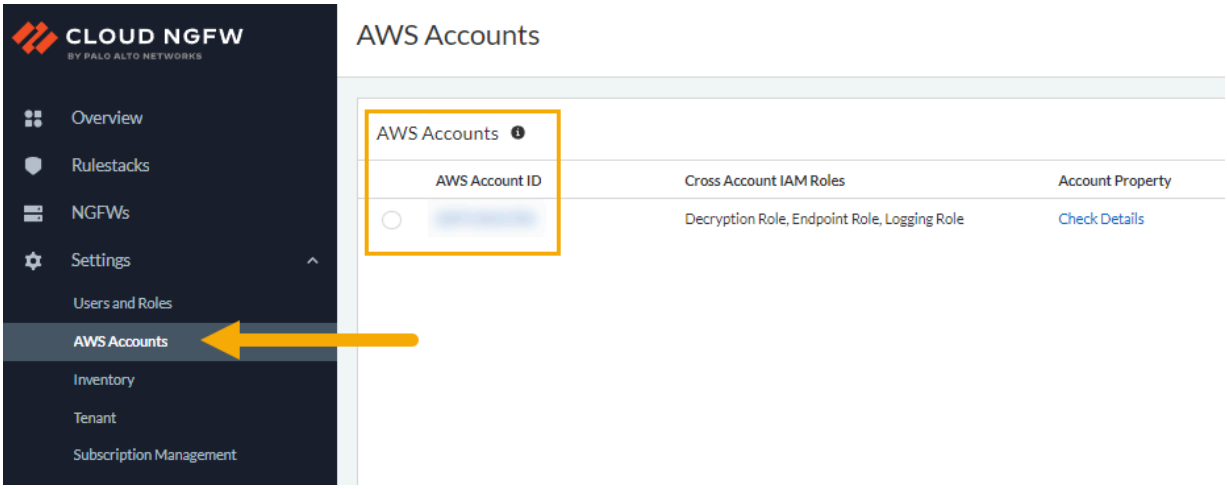
Weitere Informationen finden Sie auf der Seite zur Kündigung Ihres Abonnements.

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.

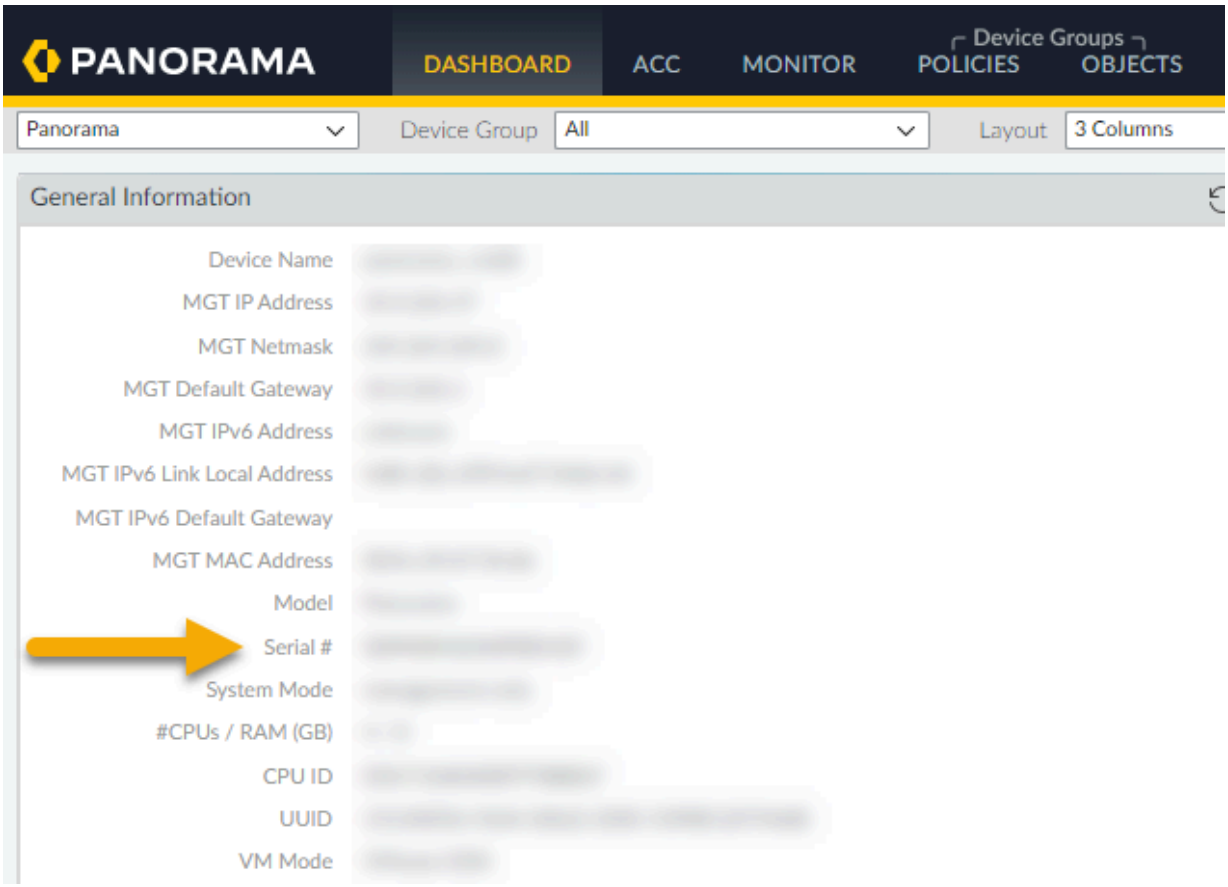
So erstellen Sie einen Supportfall mithilfe der Cloud NGFW-Konsole:

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

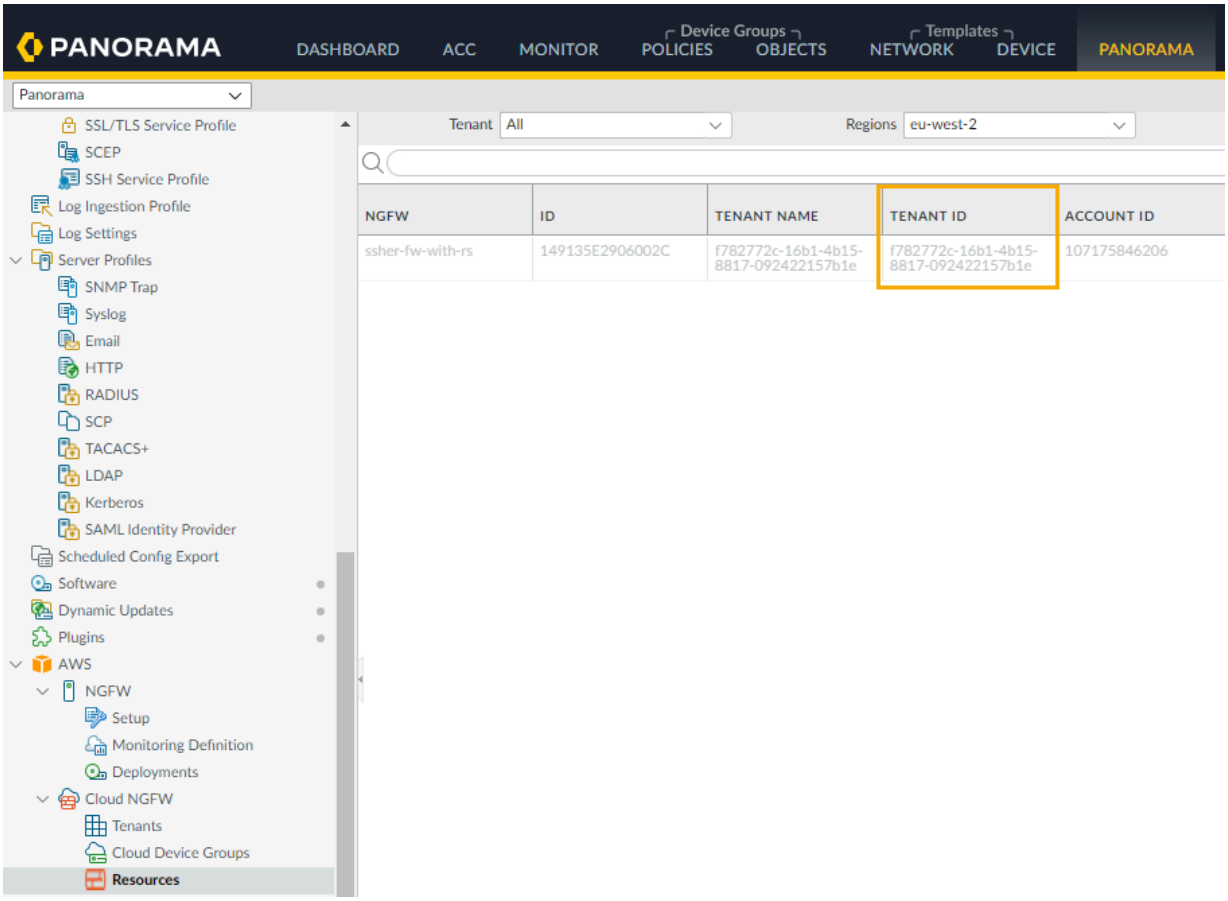


STEP 2 | Verwenden Sie bei Bedarf die Panorama-Konsole, um zusätzliche Informationen für den Supportfall zu ermitteln, beispielsweise die Mandanten-ID oder die Panorama-Seriennummer.

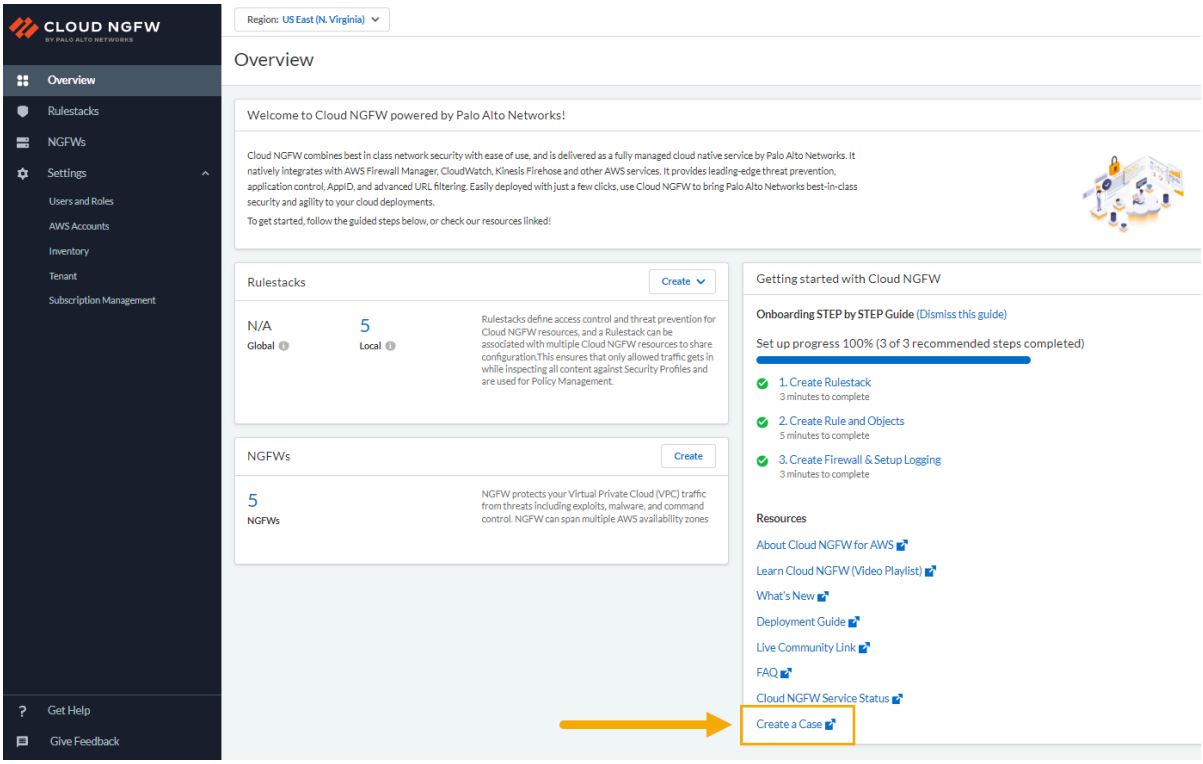
Suchen Sie die **Panorama-Seriennummer** mithilfe des **Dashboards**:



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)**.



Verknüpfung von Cloud NGFW mit Palo Alto Networks Management aufheben

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 Cloud-Gerätegruppe aus einer Ressource löschen oder unter Zuordnung einer Cloud-Gerätegruppe zu einer Ressource aufheben.

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

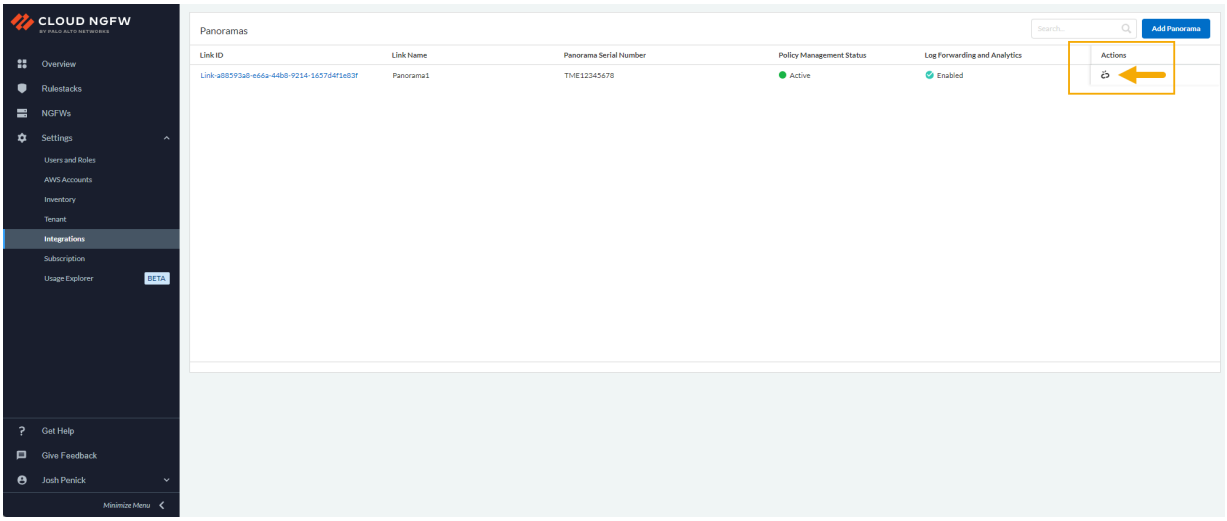
STEP 1 | Wählen Sie auf der Seite „Firewall“ oder „Rulestacks“ (Regelstapel) die Region aus, zum Beispiel **us-east-1**.

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

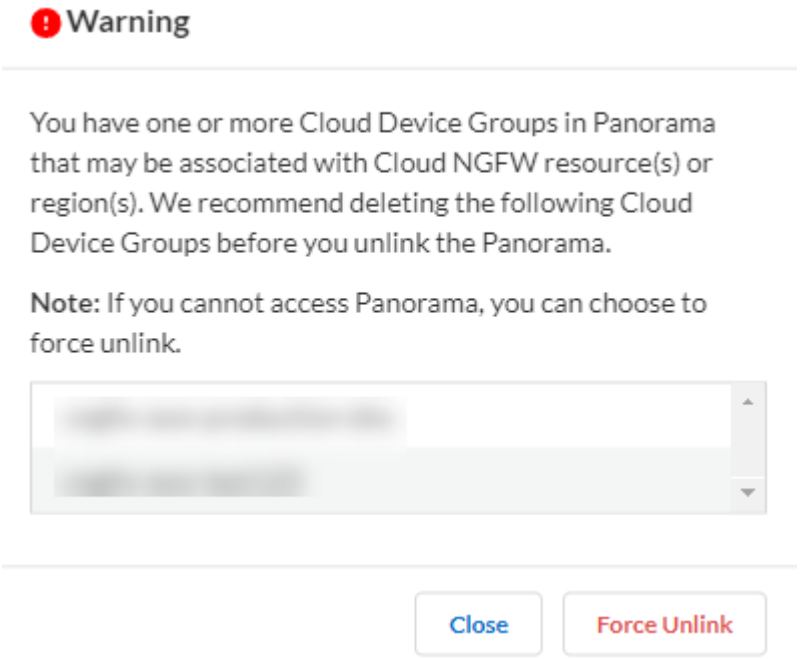
STEP 3 | Suchen Sie auf der Seite **Integrations (Integrationen)** den Abschnitt **Actions (Aktionen)**. Eine bereits verknüpfte Panorama-Instanz wird ausgegraut angezeigt.

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
```


Verknüpfte Panorama-Instanz der Cloud NGFW-Ressource zuordnen

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

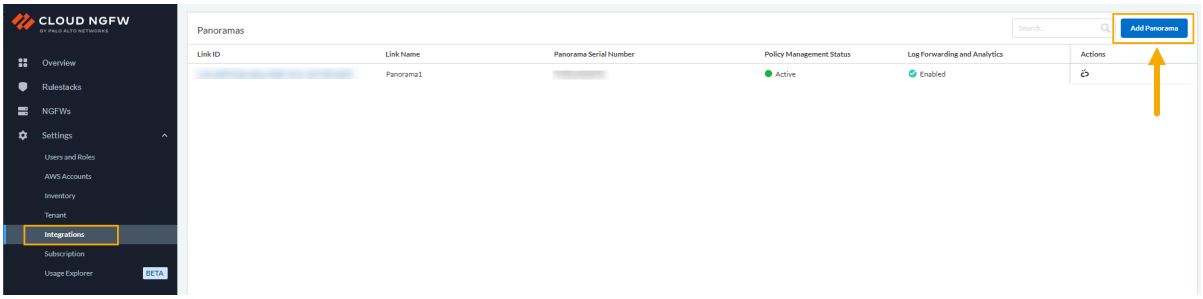
So verknüpfen Sie mehrere Panorama-Instanzen mit demselben Cloud NGFW-Mandanten:

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.

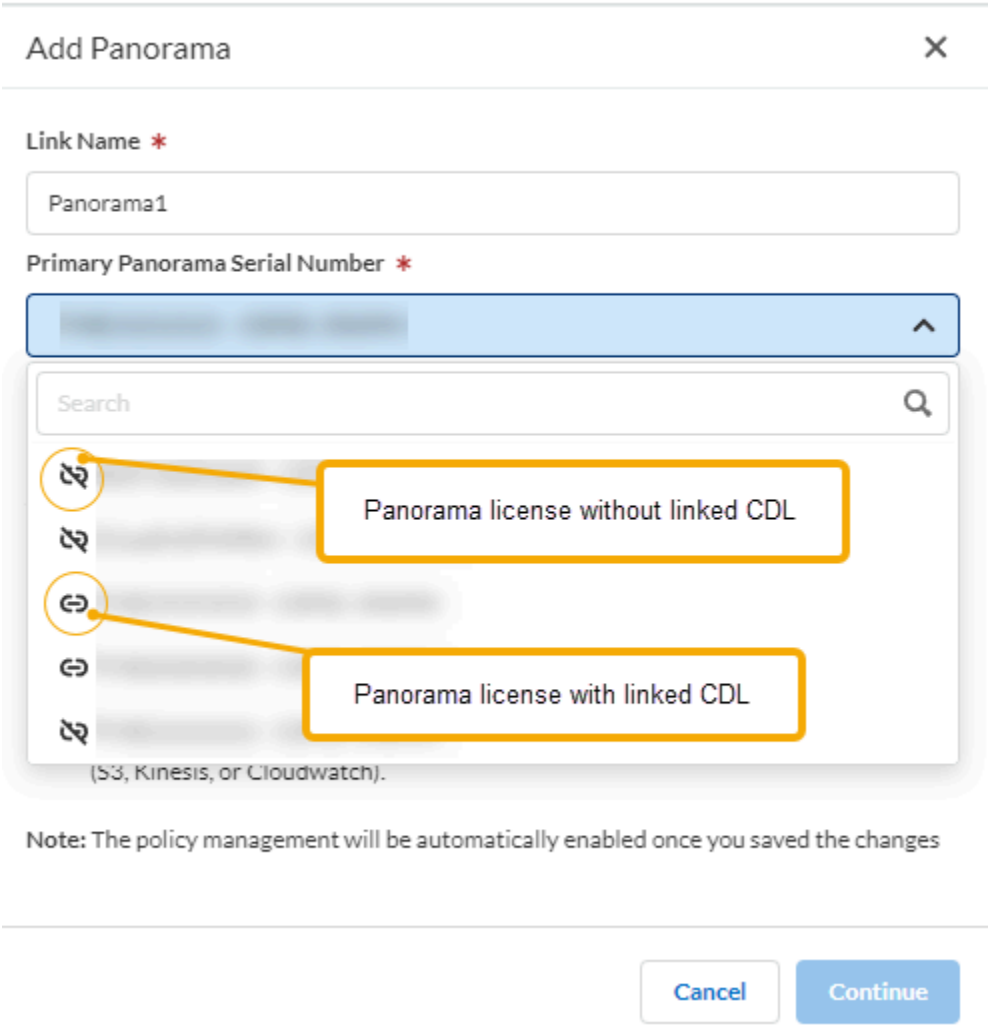
STEP 3 | Verwenden Sie die Seite **Integrations (Integrationen)**, um eine zusätzliche Panorama-Instanz hinzuzufügen. Klicken Sie auf **Add Panorama (Panorama hinzufügen)**.



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

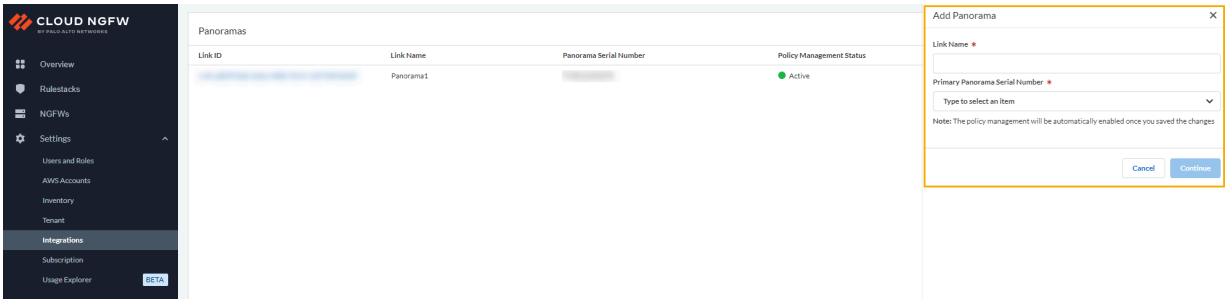
aus der Dropdown-Liste die Option **Secondary Panorama Serial Number (Sekundäre Panorama-Seriennummer)** aus.

Auf diesem Bildschirm werden zwei verschiedene Symbole angezeigt, die den Status der Panorama-Lizenz beschreiben: eine mit CDL verknüpfte Panorama-Lizenz und eine Panorama-Lizenz, die nicht mit CDL verknüpft ist. In der folgenden Abbildung sind diese Symbole veranschaulicht:

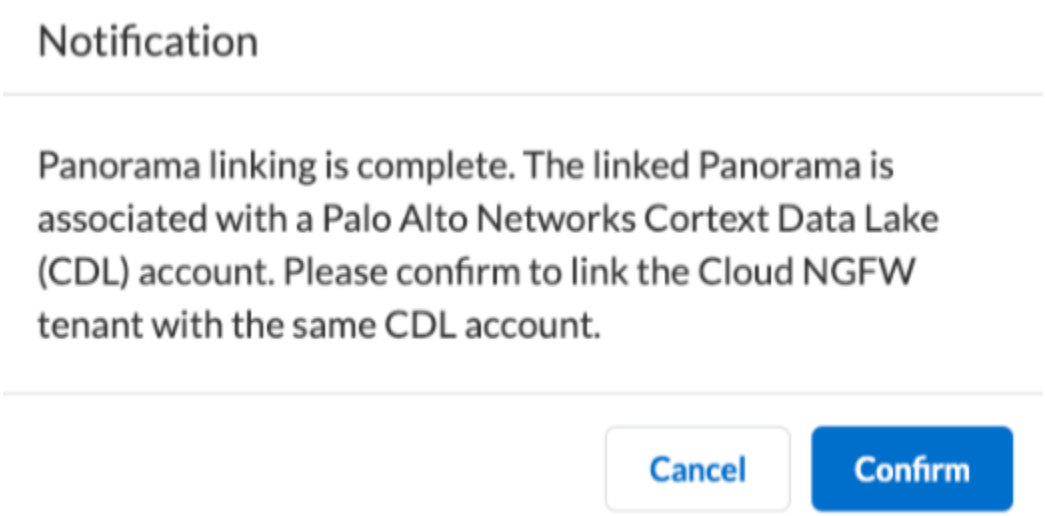


Wenn Sie eine Panorama-Seriennummer auswählen, die nicht mit CDL verknüpft ist, haben Sie die Option, den Verknüpfungsvorgang abzubrechen. In diesem Fall stimmen Sie zu, eine CDL-Lizenz zu

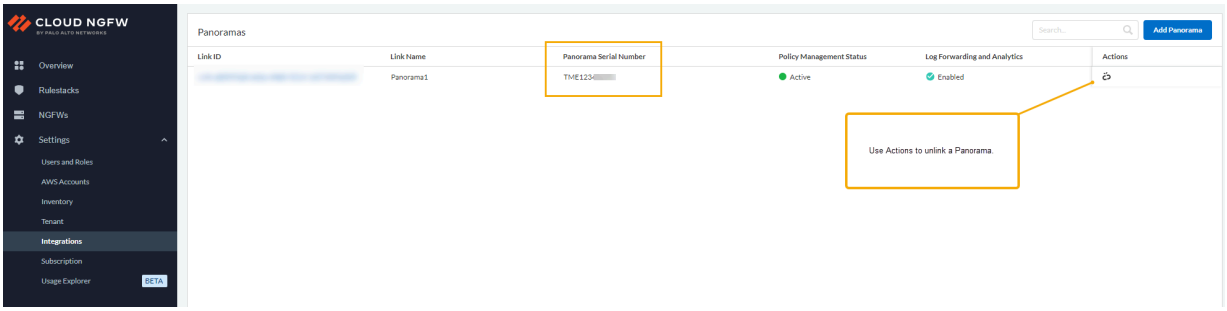
erwerben und sie Ihrer Panorama-Appliance zuzuordnen. Alternativ können Sie zustimmen, Panorama weiterhin nur zur Richtlinienverwaltung zu verwenden:



Wenn Sie eine Panorama-Lizenz auswählen, die bereits mit CDL verknüpft ist, werden Sie aufgefordert, die Zuordnung 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)**.

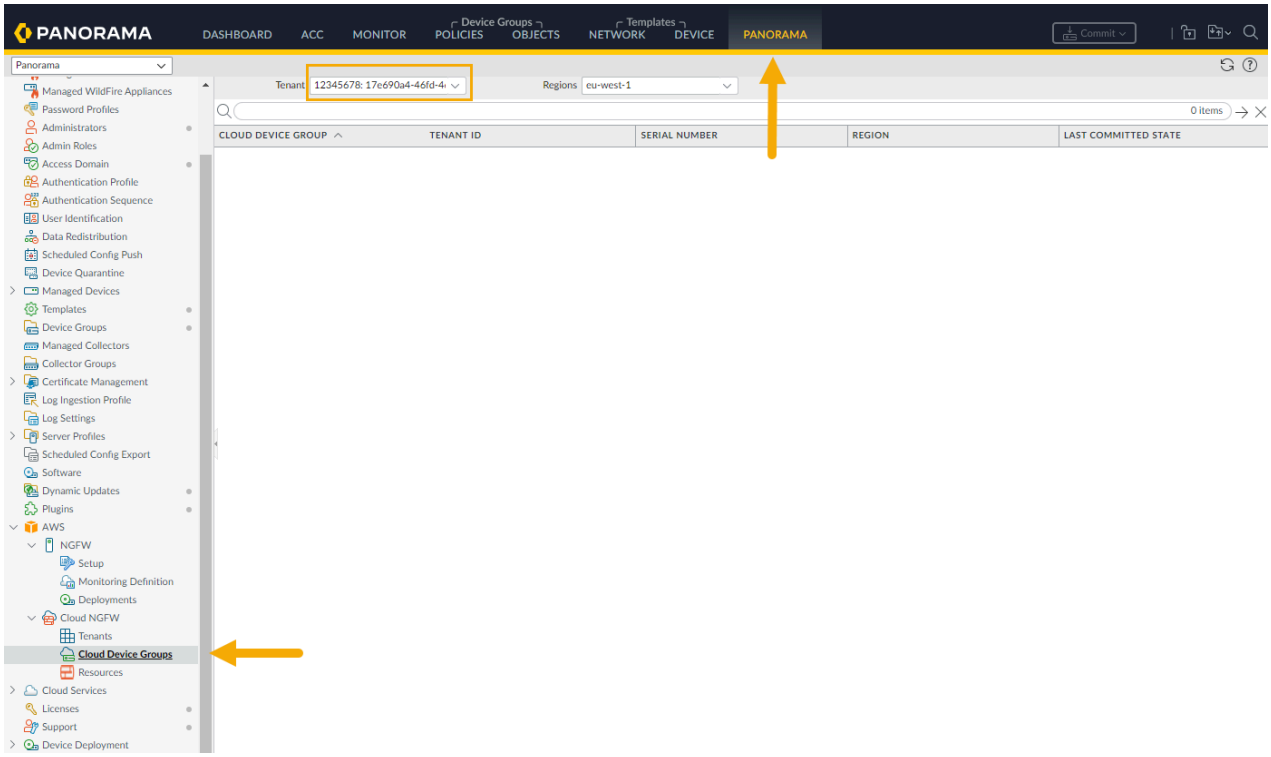
STEP 11 | Wiederholen Sie die Schritte 6 bis 10, um der Ressource eine weitere Panorama-Instanz hinzuzufügen.

Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden

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.

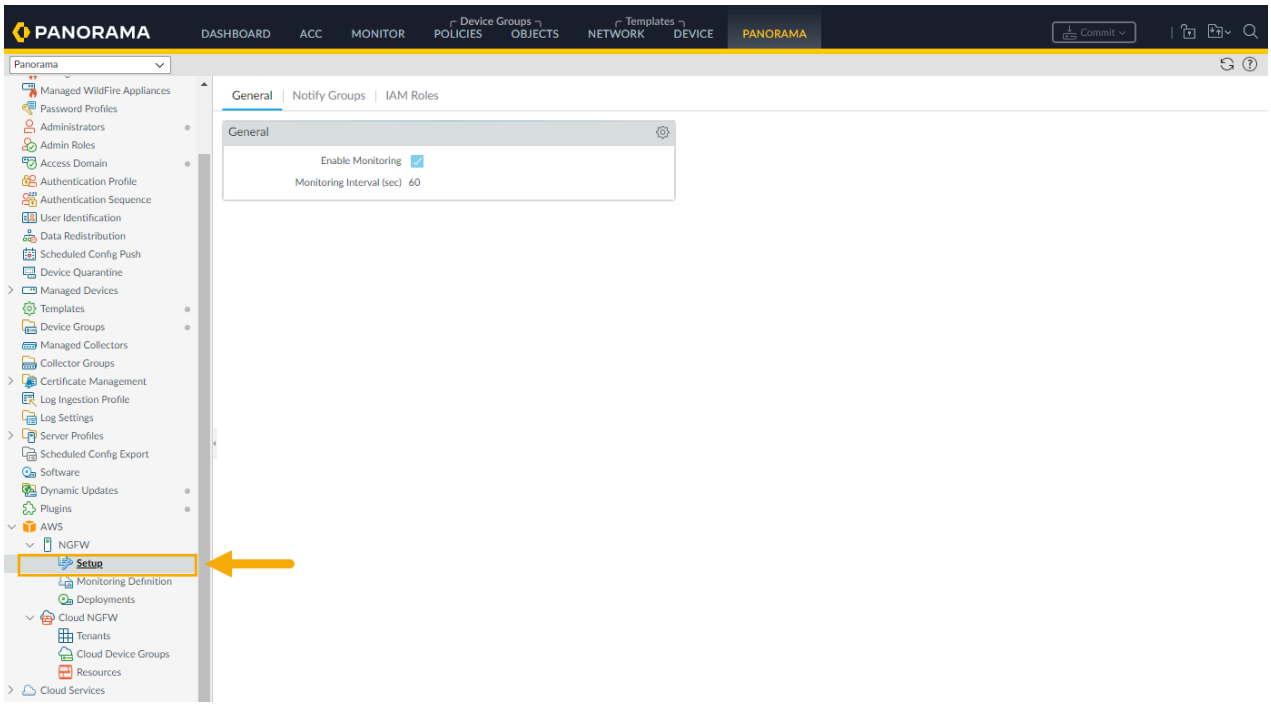
Wenn Sie die Panorama-Konsole zum Konfigurieren der Cloud NGFW verwenden, speichert der Browser lokale Informationen wie die Cloud-Gerätegruppe, den Vorlagenstapel und die Region im Cache, sodass beim Wechseln zwischen Panorama-Aufgaben zwischengespeicherte Cloud NGFW-Informationen in der Panorama-Konsole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

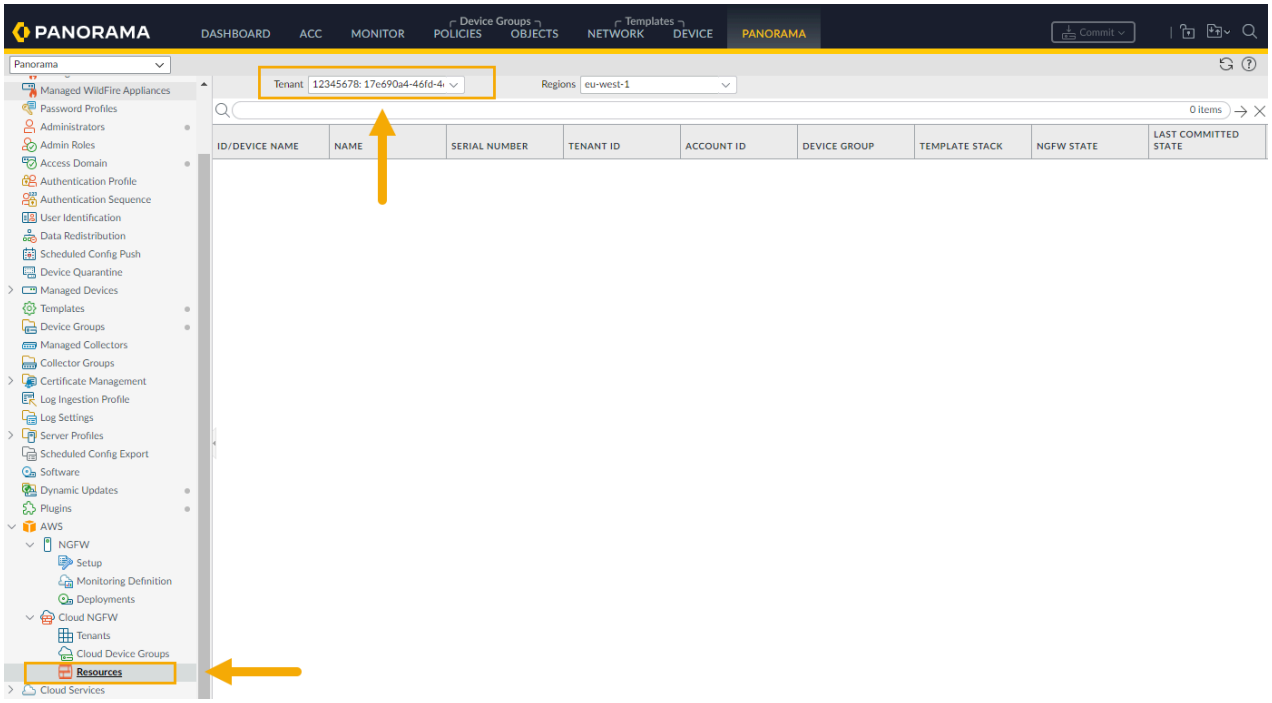


Wenn Sie zu einem anderen Bereich in der Panorama-Konsole navigieren und dann zu **Cloud NGFW > Cloud Device Groups (Cloud-Gerätegruppen)** zurückkehren, zeigt die Konsole den einzelnen

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



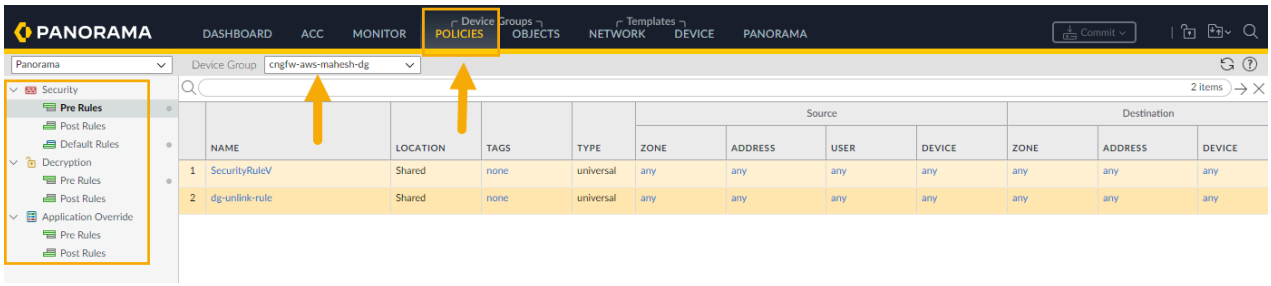
Wenn Sie zum Bildschirm **Cloud NGFW > Resources (Ressourcen)** zurückkehren, merkt sich die Panorama-Konsole den zuvor ausgewählten Mandanten, anstatt alle der Cloud NGFW-Ressource zugeordneten Mandanten anzuzeigen.



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

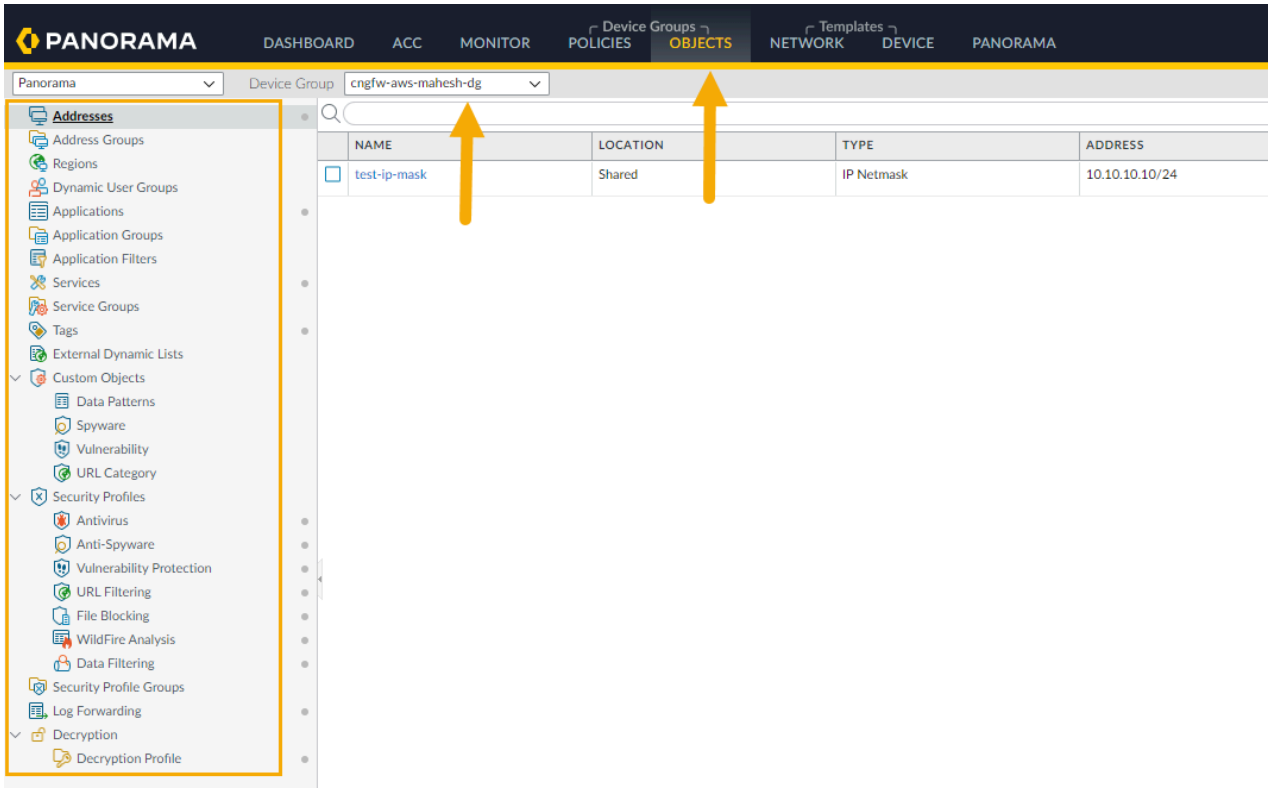
Die Panorama-Integration zeigt nur die Konfigurationsoptionen an, die für die Cloud NGFW-Ressource verfügbar sind. Wählen Sie beispielsweise **Policies (Richtlinien)** aus, um die für die Cloud NGFW-

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

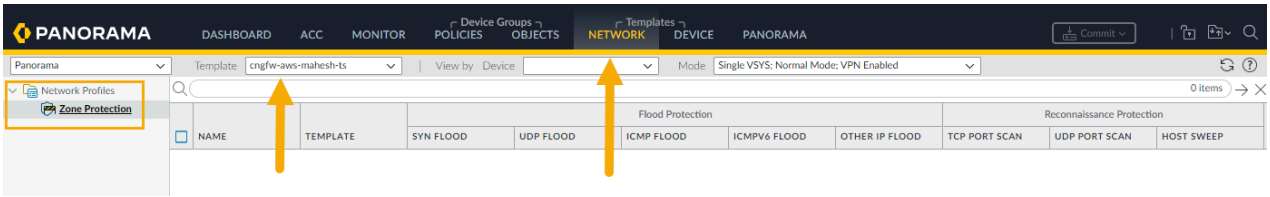


Der Gerätegruppenname weist das Präfix `cngfw-aws` auf.

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.

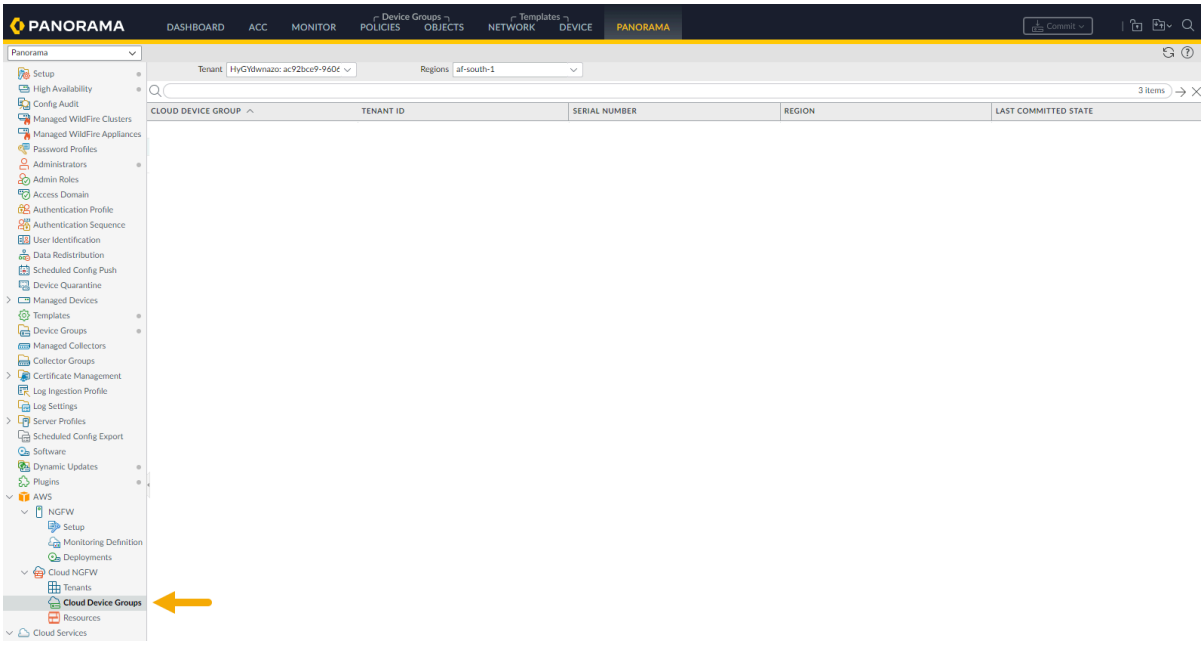
Mithilfe von Gerätegruppen können Sie Richtlinienregeln und die von ihnen referenzierten Objekte konfigurieren. Organisieren Sie Gerätegruppen hierarchisch mit gemeinsamen Regeln und Objekten an der Spitze und gerätegruppenspezifischen Regeln und Objekten auf nachfolgenden Ebenen. So können Sie eine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

Weitere Informationen finden Sie unter Gerätegruppen verwalten.

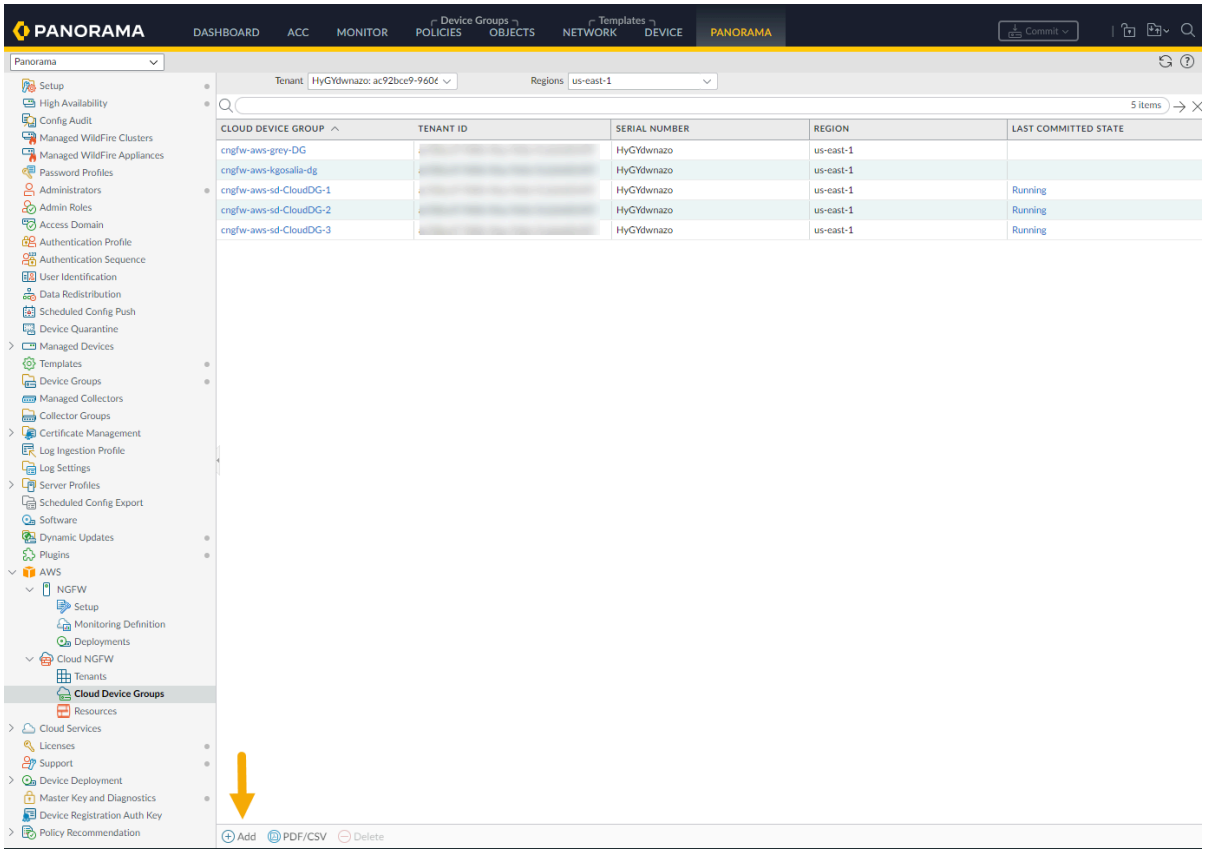
So fügen Sie mithilfe der Panorama-Konsole eine Cloud-Gerätegruppe hinzu:

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.

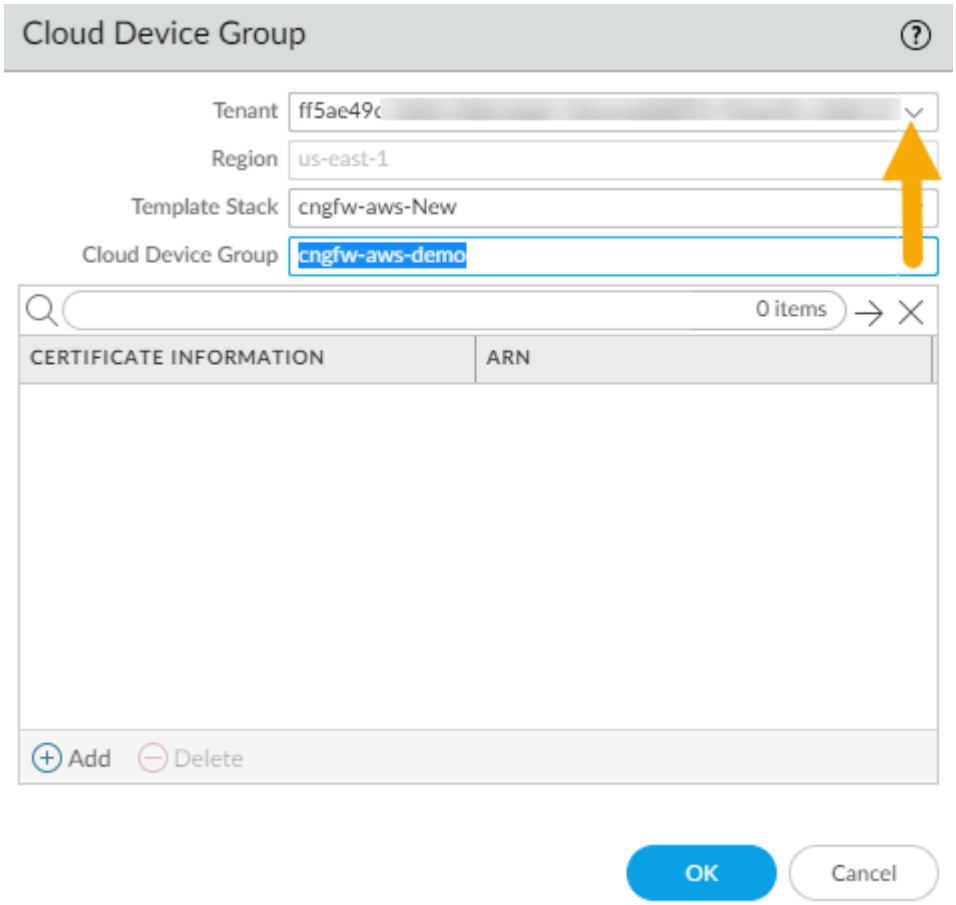
Zuvor erstellte Cloud-Gerätegruppen werden angezeigt, wenn sie mit AWS für den Cloud NGFW-Mandanten eingerichtet wurden.



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



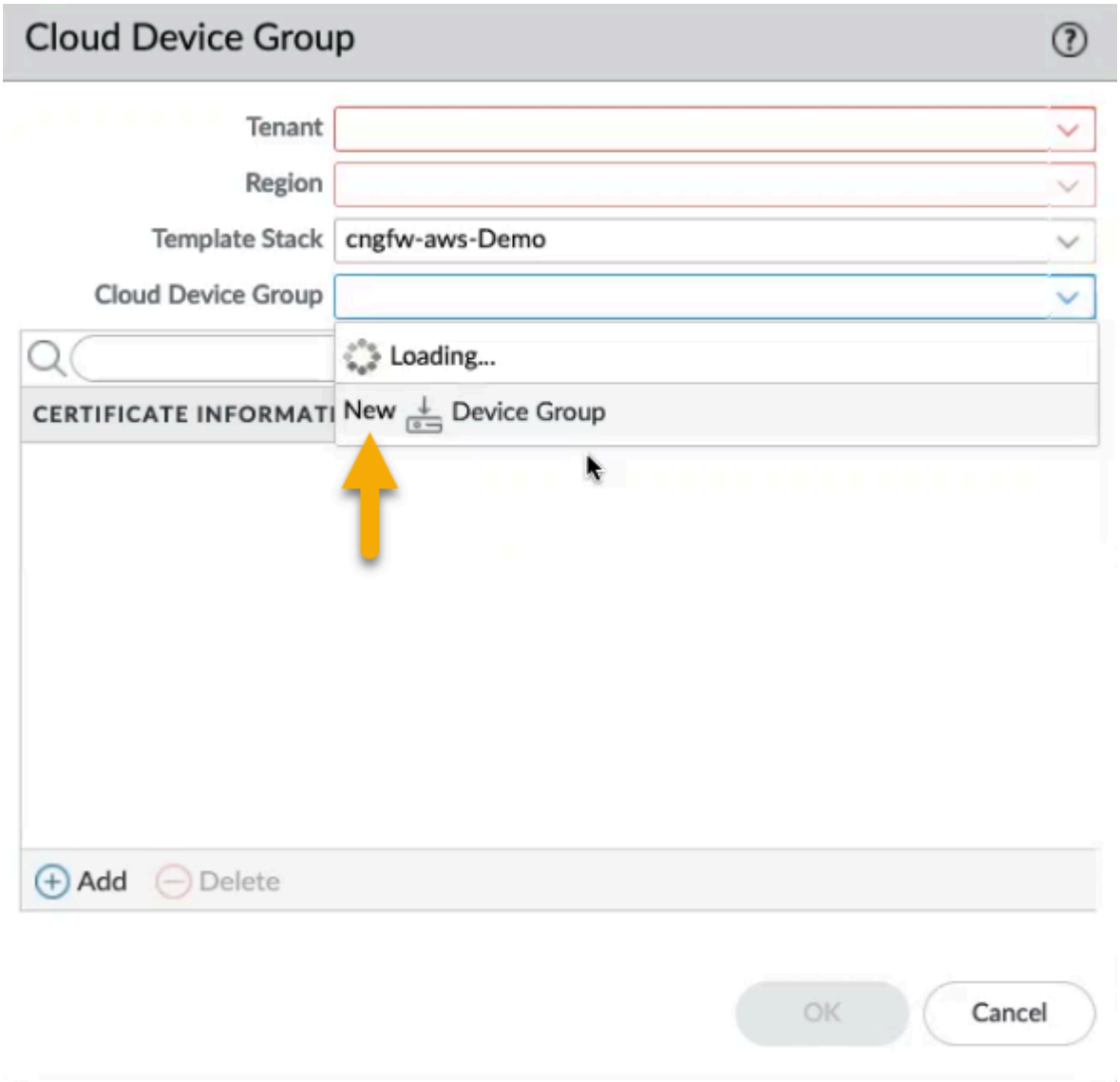
STEP 3 | Wählen Sie im Bildschirm **Cloud Device Group (Cloud-Gerätegruppe)** über das Dropdown-Menü den zu verwendenden **Mandanten** aus.



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

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

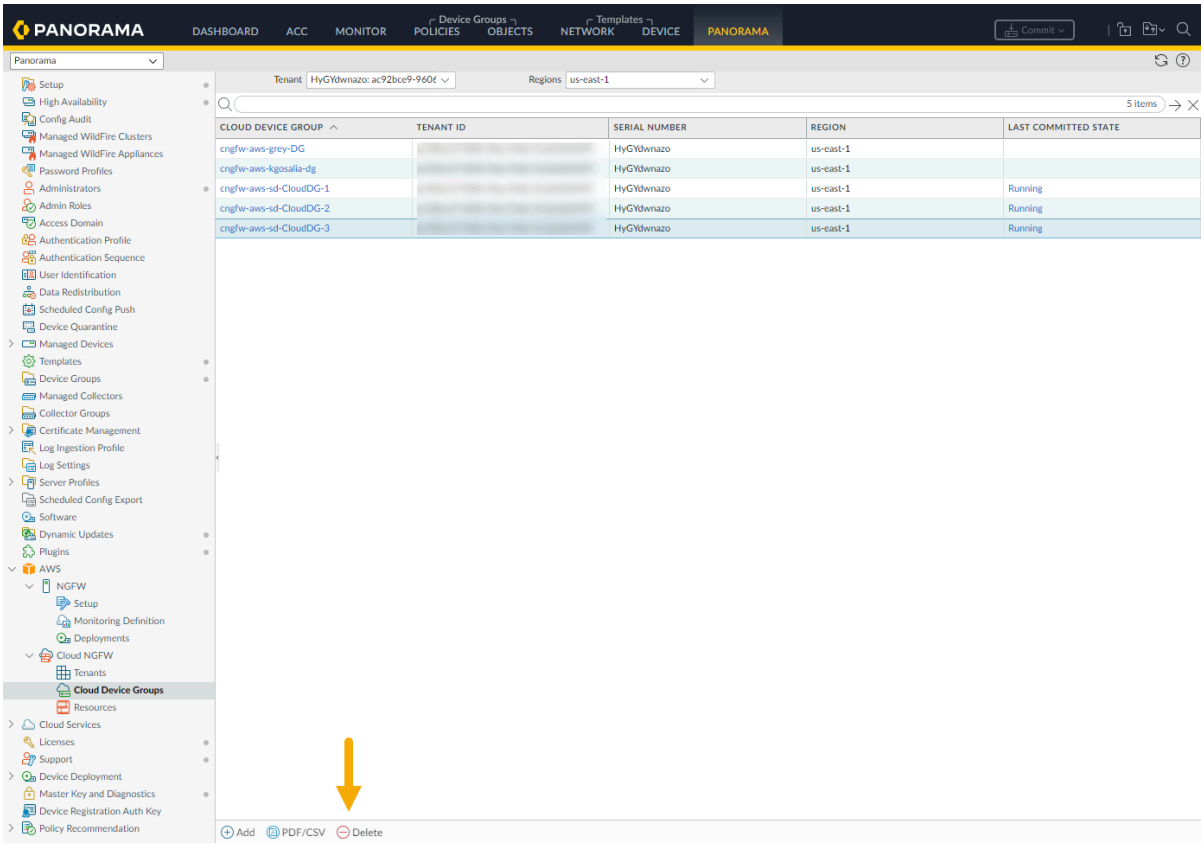
Verwenden Sie die Panorama-Konsole, um eine Cloud-Gerätegruppe zu löschen. Sie können eine Cloud-Gerätegruppe nur löschen, wenn ihr keine Firewalls zugeordnet sind.

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.

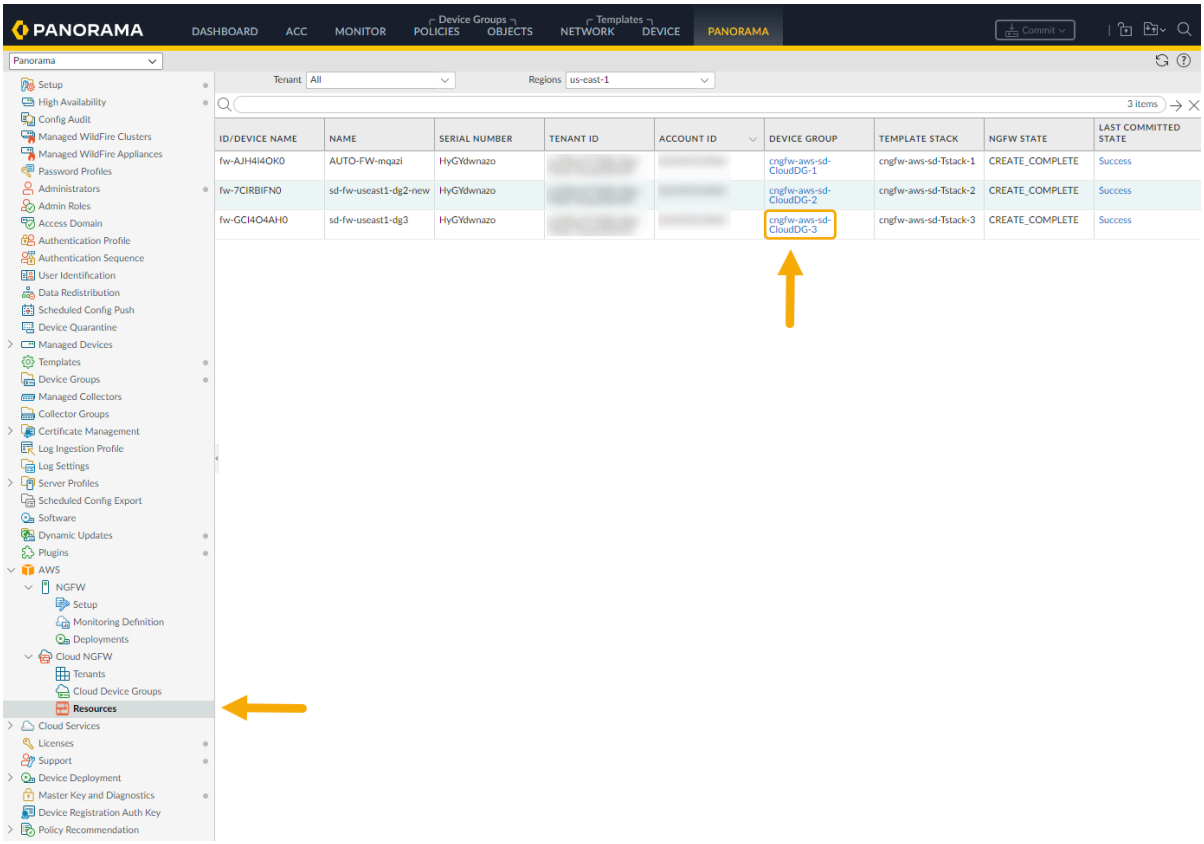
Cloud-Gerätegruppe einer Ressource zuordnen

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.

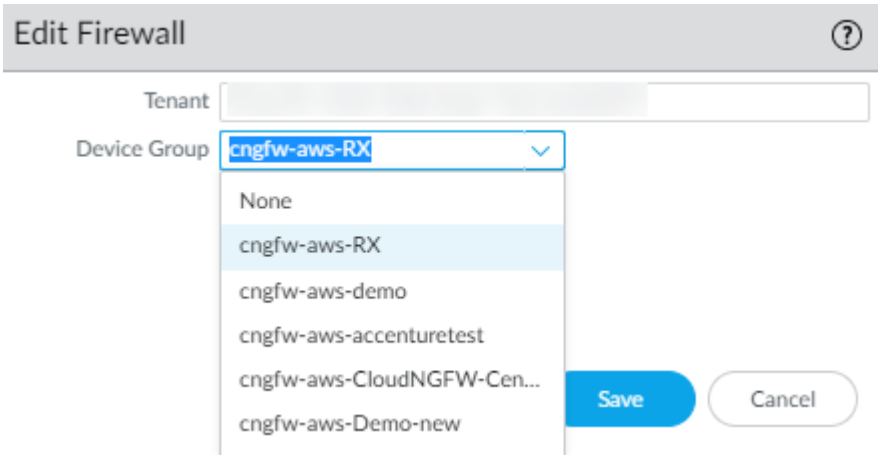
So ordnen Sie eine Cloud-Gerätegruppe mithilfe der Panorama-Konsole einer Cloud NGFW-Ressource zu:

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.

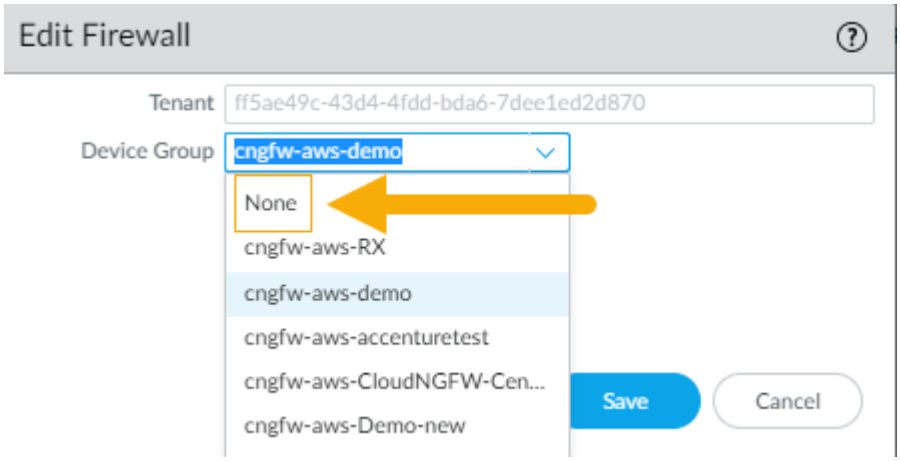
Zuordnung einer Cloud-Gerätegruppe zu einer Ressource aufheben

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-

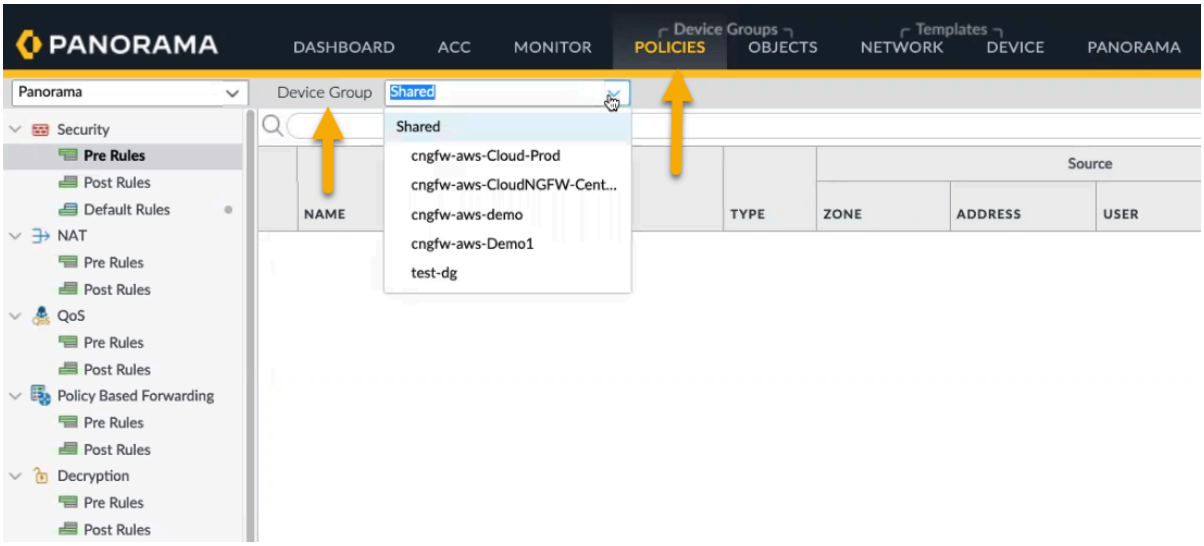
Regeln ermöglichen Ihnen einen mehrschichtigen Ansatz zur Implementierung von Richtlinien. Weitere Informationen finden Sie unter Richtlinien auf Panorama definieren.

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:

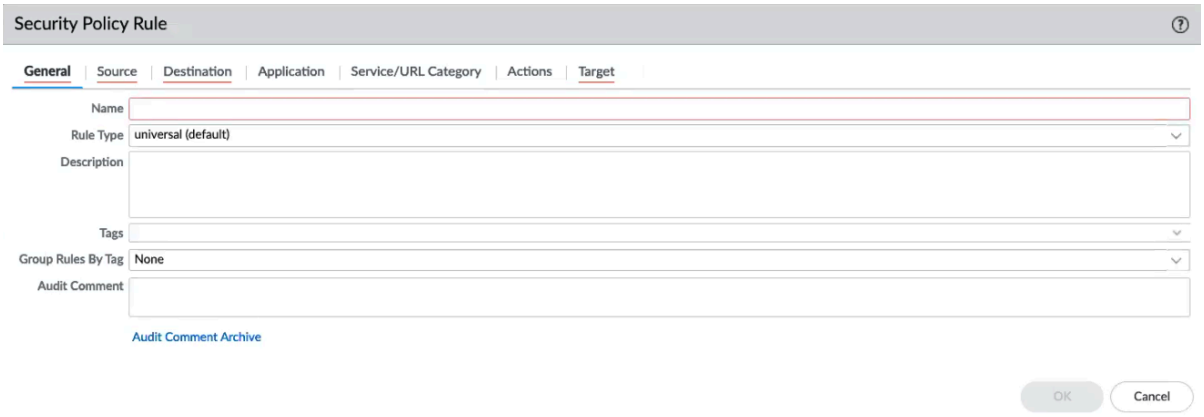
STEP 1 | Wählen Sie **Policies (Richtlinien)** aus.

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*.



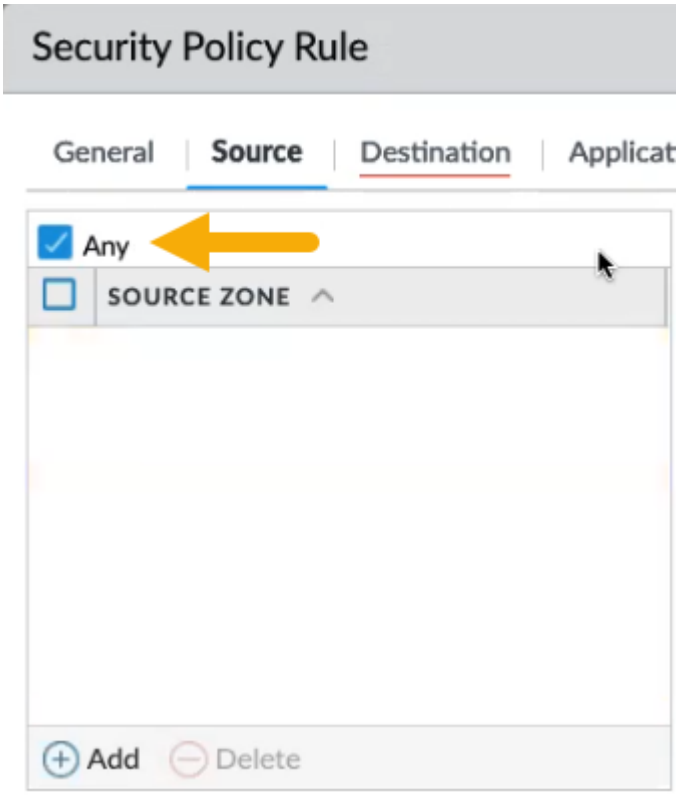
STEP 3 | Klicken Sie unten links in der Konsole auf **Add (Hinzufügen)**.

STEP 4 | Konfigurieren Sie im Bildschirm Security Policy Rule (Sicherheitsrichtlinienregel) die Elemente der Richtlinie, die Sie auf die Gerätegruppe anwenden möchten:



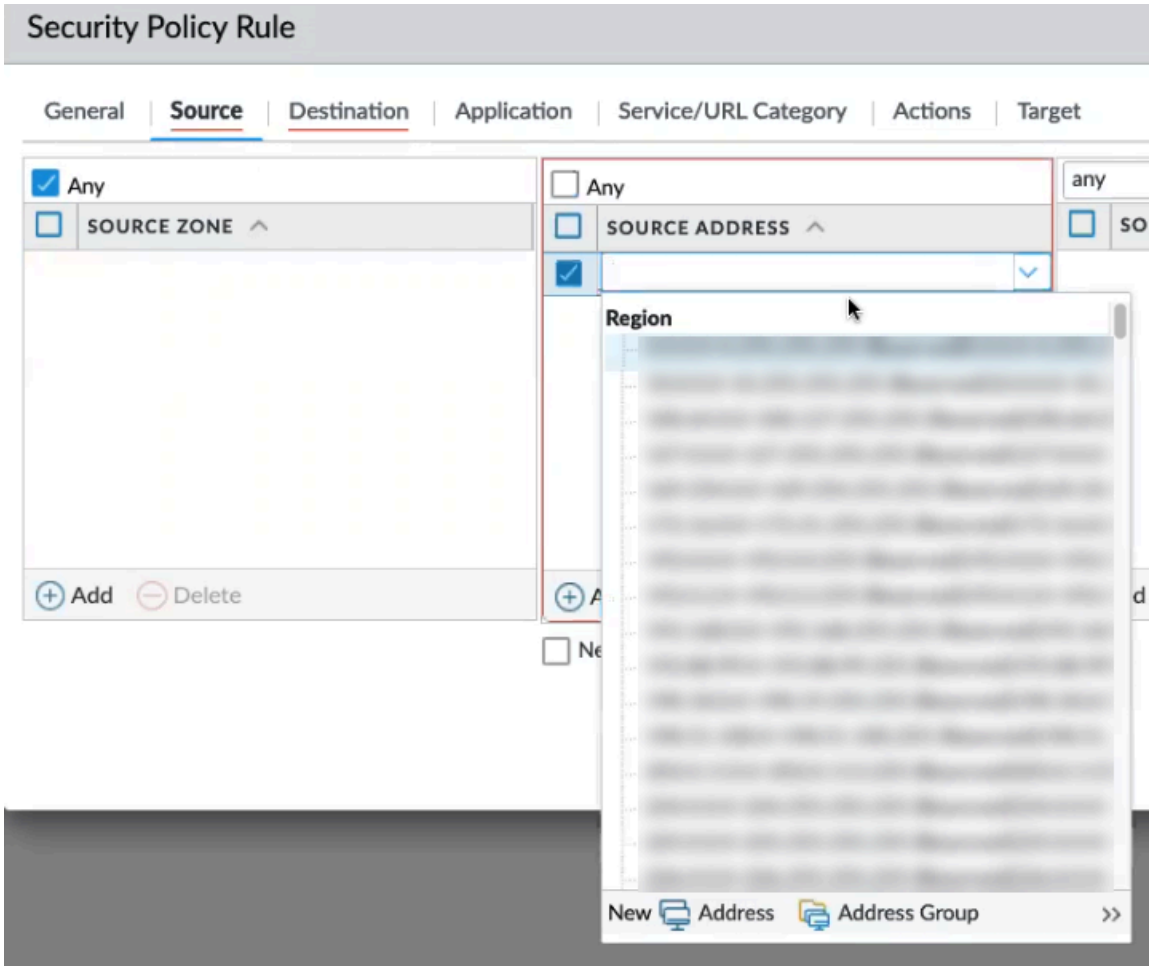
STEP 5 | Geben Sie auf der Registerkarte **General (Allgemein)** einen **Namen** für die Richtlinie ein.

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.

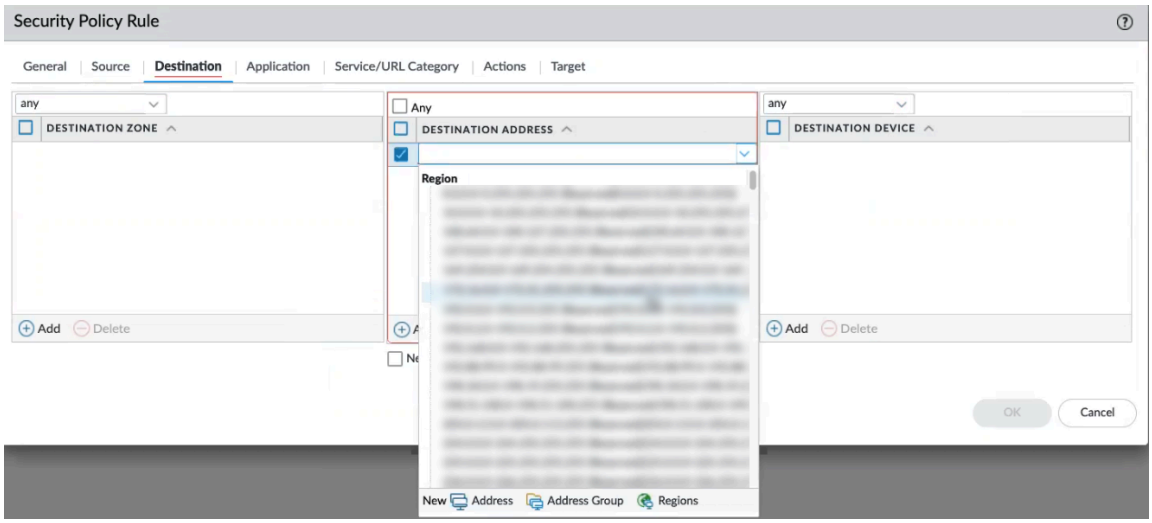


2. Klicken Sie für die Richtlinien **Source User (Quellbenutzer)** und **Source Device (Quellgerät)** auf **Any (Beliebig)**. In Cloud NGFW wird die Angabe bestimmter Quellbenutzer oder Quellgeräte nicht unterstützt

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.

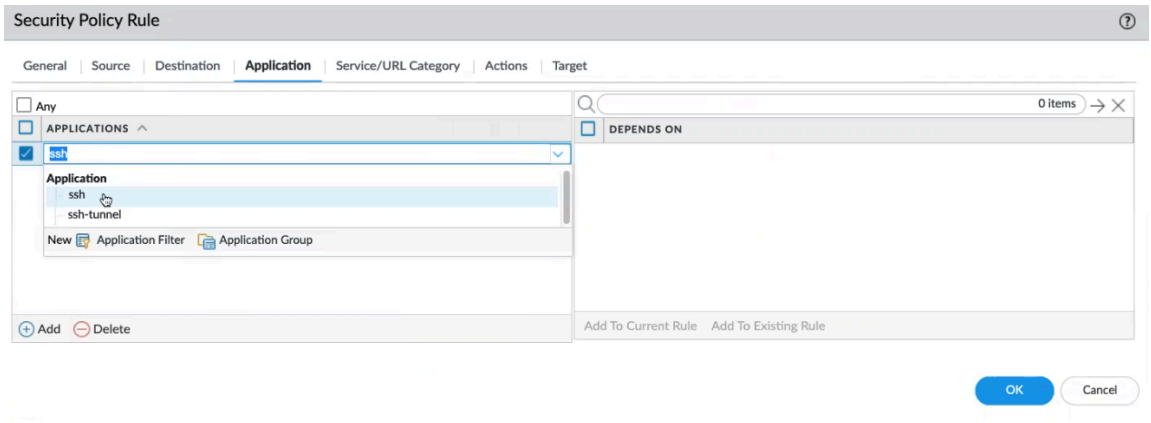
2. Klicken Sie für **Destination Address (Zieladresse)** auf **Any (Beliebig)** oder verwenden Sie das Dropdown-Menü, um eine vorhandene Zone auszuwählen. Klicken Sie auf **New (Neu)**, um eine neue Adresse, Adressgruppe oder Region hinzuzufügen.
3. Klicken Sie für **Destination Device (Zielgerät)** auf **Any (Beliebig)**. 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

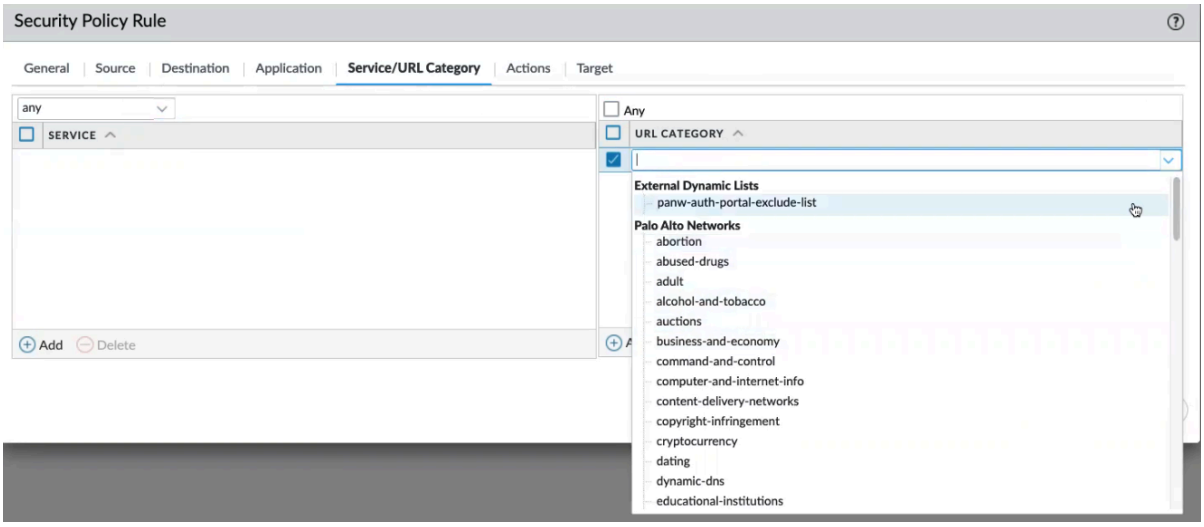
oder bestimmte Attribute einer vorhandenen Anwendung zu erkennen. Benutzerdefinierte Anwendungen werden in **ObjectsApplications** definiert.

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.



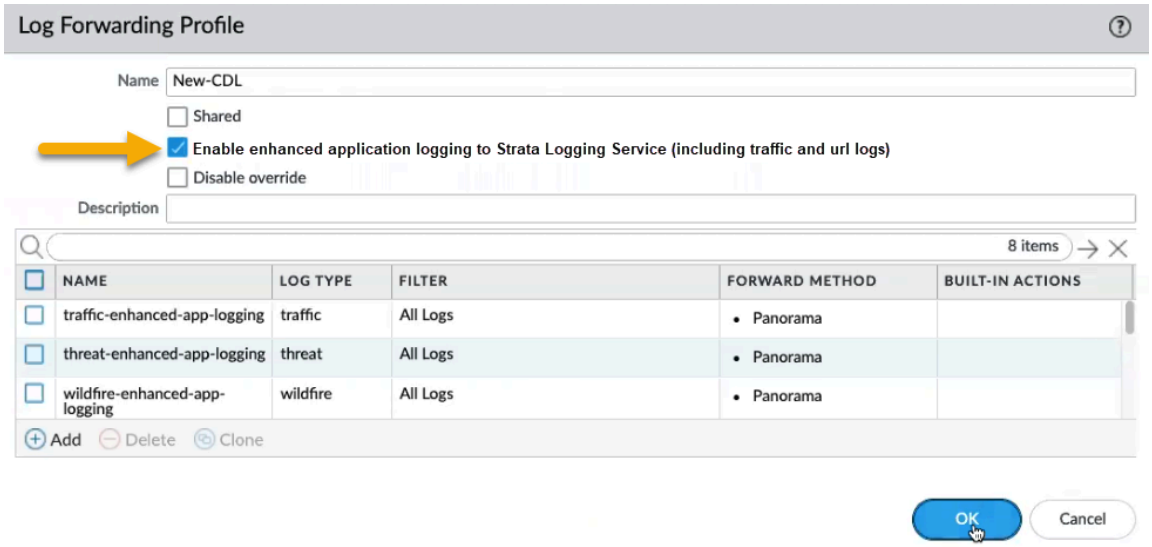
STEP 10 | Konfigurieren Sie unter **Actions (Aktionen)** eine Aktionsrichtlinie, um die auszuführende Aktion basierend auf Datenverkehr zu bestimmen, der den definierten Richtlinienattributen entspricht.

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)**

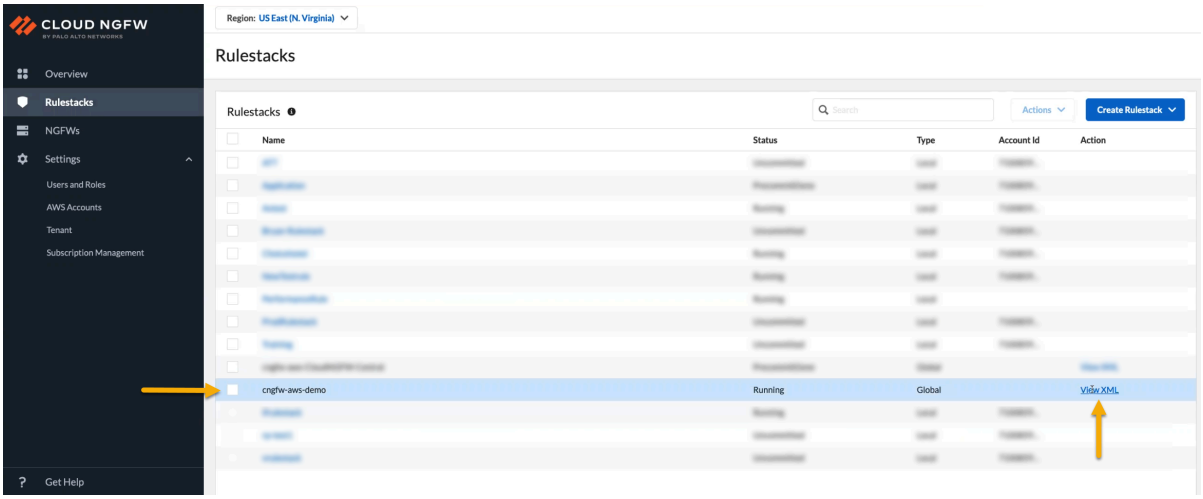
(Erweiterte Anwendungsprotokollierung für Strata-Protokollierungsdienst aktivieren (einschließlich Datenverkehrs- und URL-Protokolle)) aus. Klicken Sie auf **OK**.



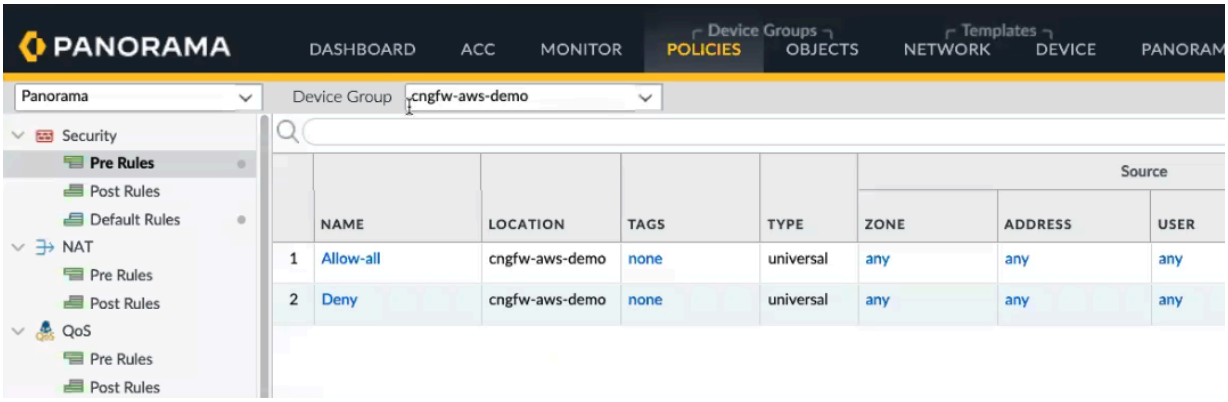
Weitere Informationen zum Strata-Protokollierungsdienst finden Sie unter Protokolle erkunden.

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:

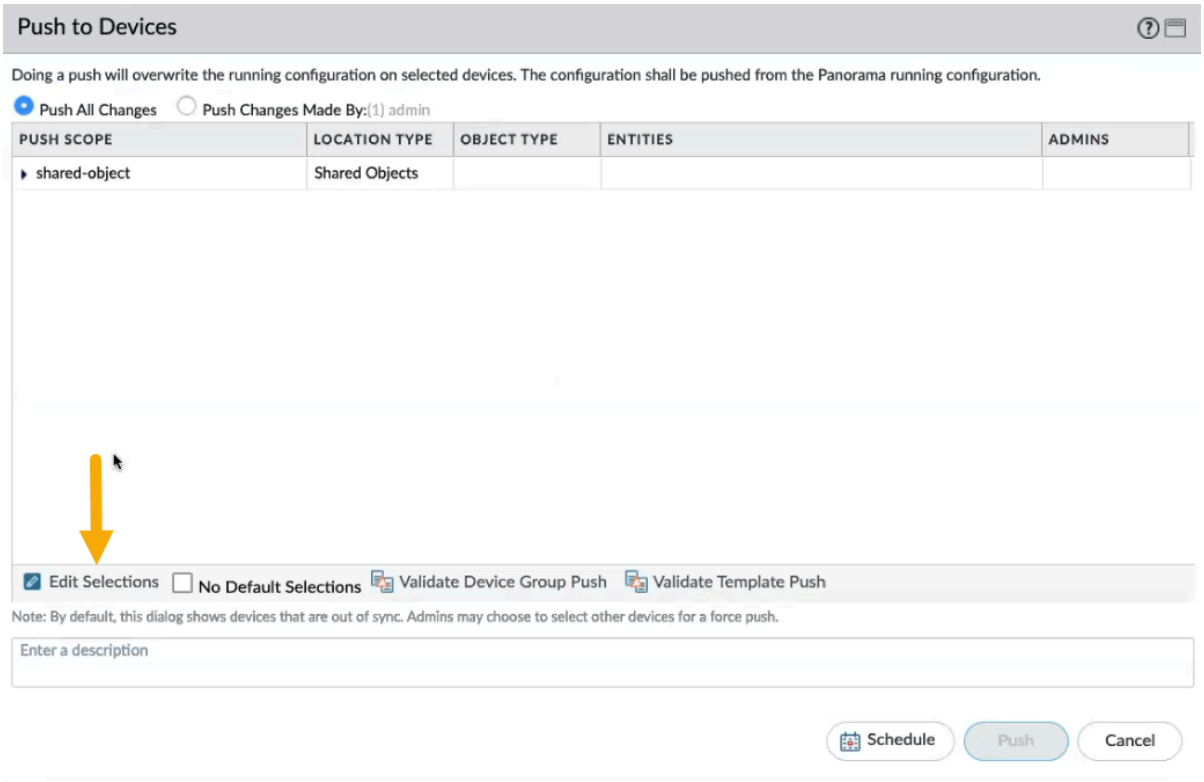


Der Regelstapel ist jetzt den Richtlinien zugeordnet, die auf die in Panorama erstellte Cloud-Gerätegruppe angewendet werden:



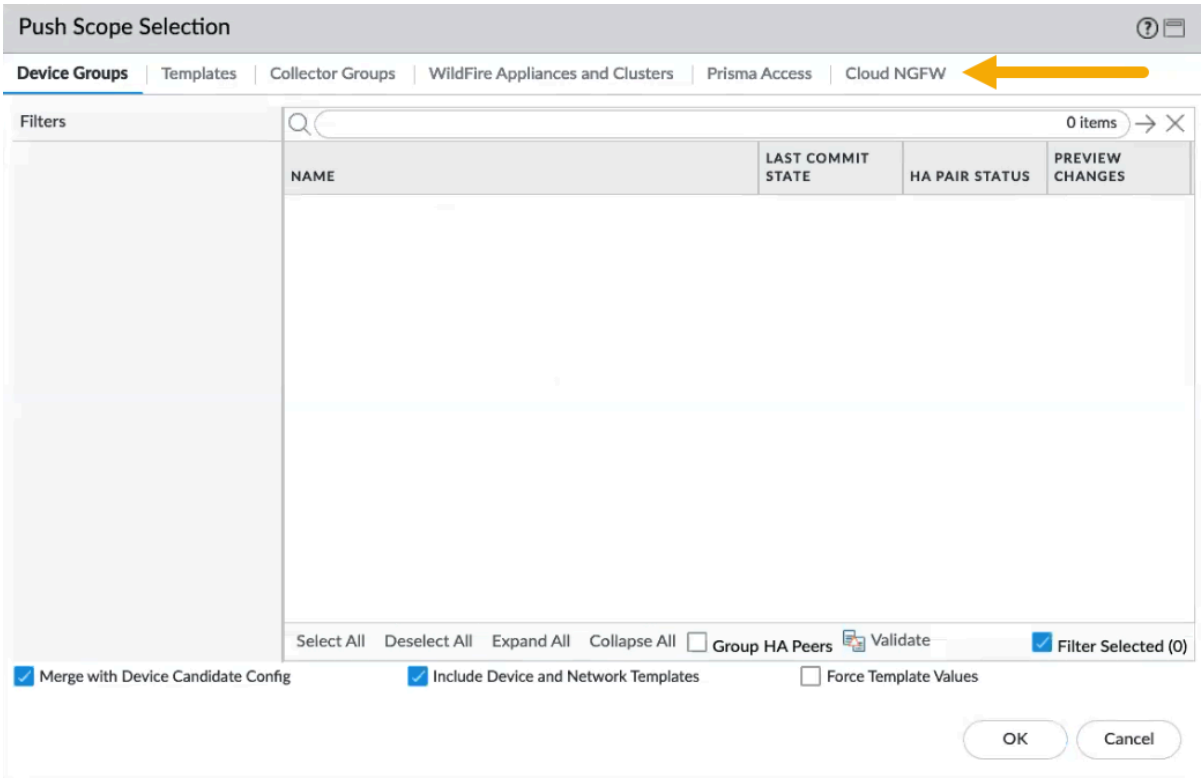
STEP 12 | Nachdem Sie Richtlinien auf die Cloud-Gerätegruppe für den Cloud NGFW-Mandanten angewendet haben, übertragen Sie die Änderungen per Push in die Panorama-Konsole.

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

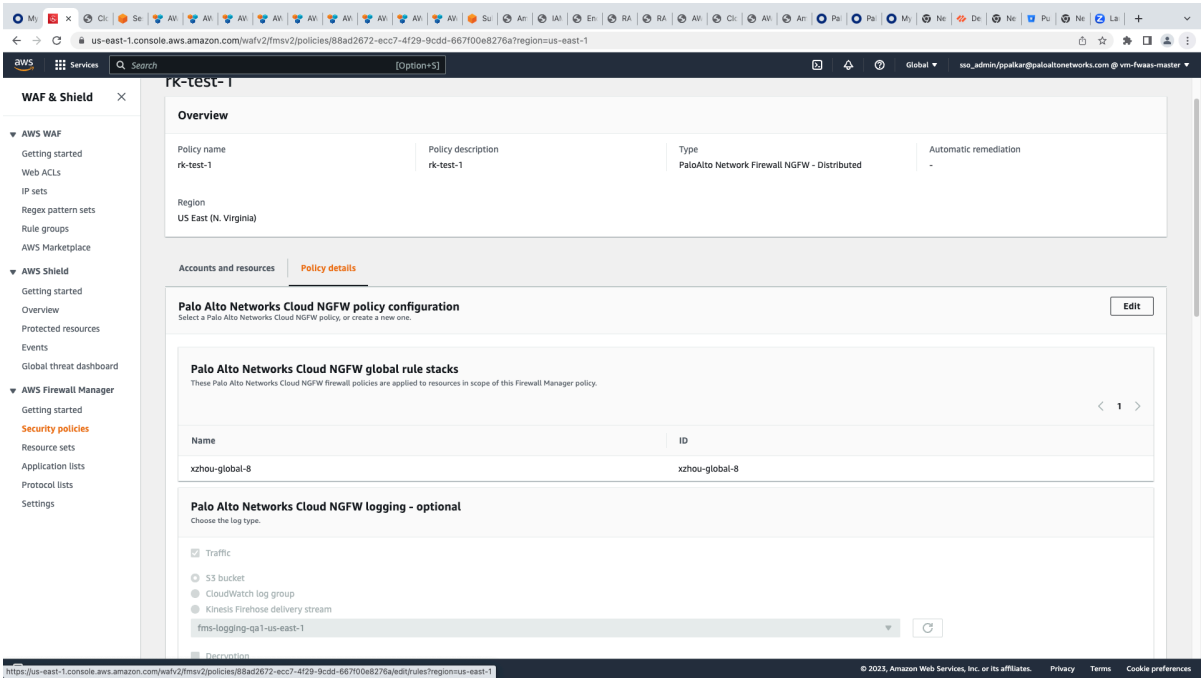
Die Informationen in diesem Abschnitt richten sich an Benutzer, die den AWS Firewall Manager Service (FMS) zum Konfigurieren von Gerätegruppen verwenden, die von Panorama per Push übertragen wurden.

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.

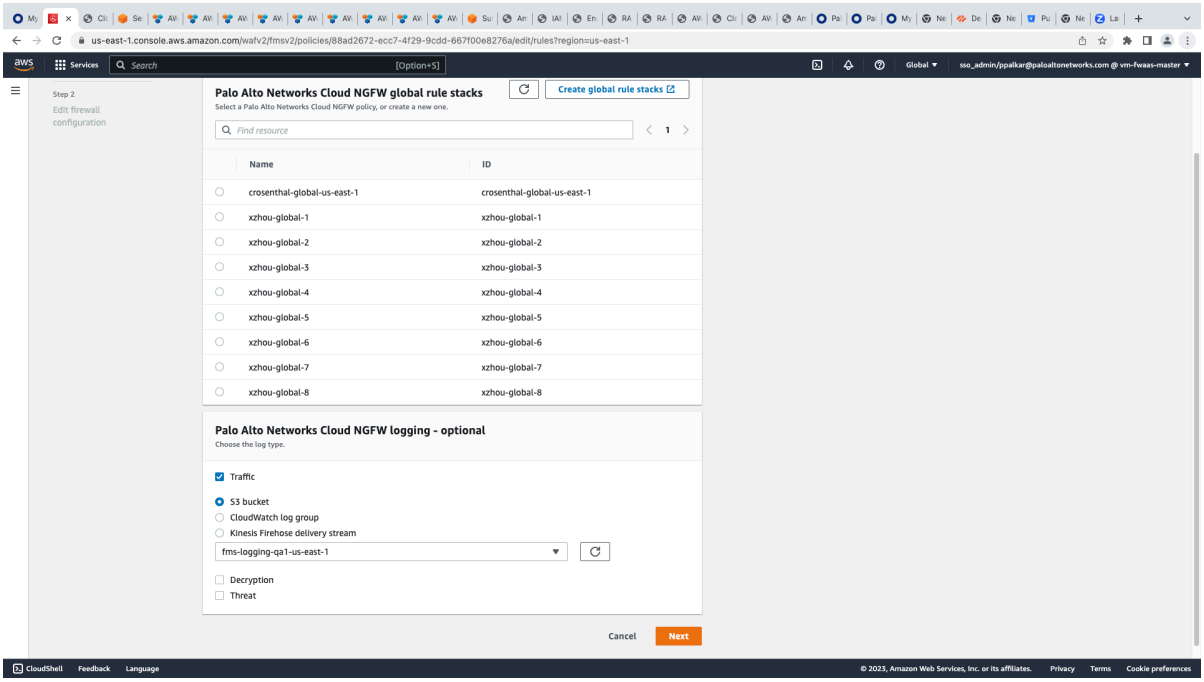
STEP 1 | Verknüpfen Sie einen Mandanten mit Panorama.

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)**.

Cloud NGFW-Protokolle und -Aktivitäten in Panorama anzeigen

Cloud NGFW-Protokolle in Panorama anzeigen

Wenn Ihre Cloud NGFW-Ressourcen in Panorama und Cortex Data Lake (CDL) 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 (Überwachung)** 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.

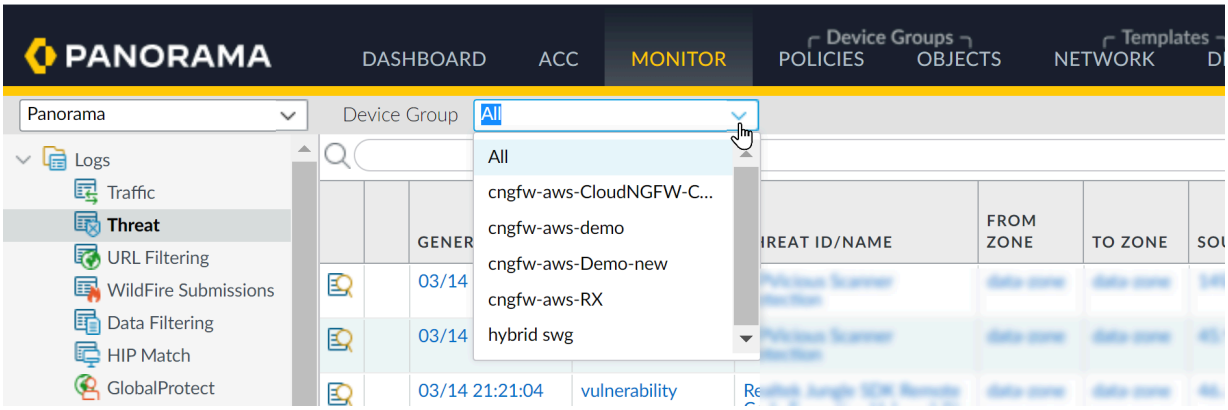
STEP 1 | Melden Sie sich bei Panorama an.

STEP 2 | Wählen Sie **Monitor (Überwachen)** aus.

STEP 3 | Wählen Sie aus der Dropdown-Liste **Device Group (Gerätegruppe)** das Symbol **Cloud Device Group (Cloud-Gerätegruppe)** 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 (Gerätename)**. 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 (Speichern)**. Klicken Sie auf das Symbol **Load Filter (Filter laden)**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

STEP 5 | Auf der linken Seite der Panorama-Konsole können Sie im Menü **Logs (Protokolle)** einen bestimmten Protokolltyp auswählen, der angezeigt werden soll.



Cloud NGFW-Aktivität im ACC anzeigen

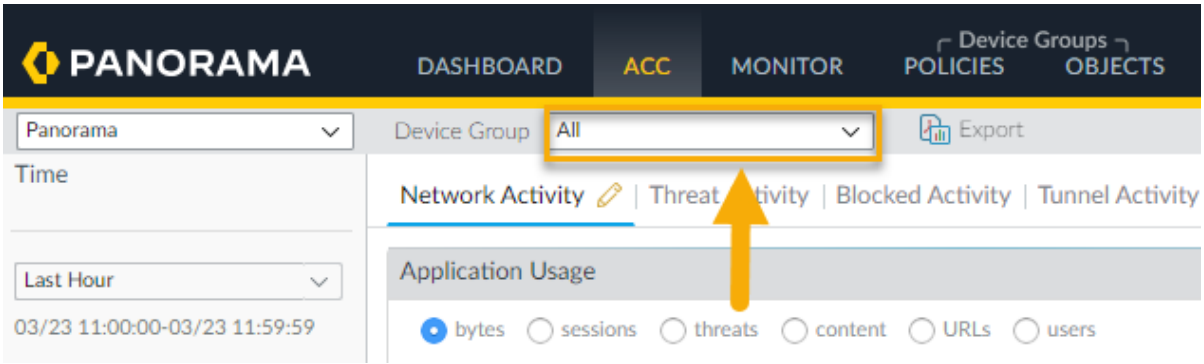
Das ACC ist ein Analysetool, das verwertbare Informationen über die Aktivitäten in Ihrem Netzwerk liefert. Das ACC verwendet die Cloud NGFW-Protokolle, um die Datenverkehrstrends in Ihrem Netzwerk grafisch darzustellen. Die grafische Darstellung ermöglicht es Ihnen, mit den Daten zu interagieren und die Beziehungen zwischen Ereignissen im Netzwerk zu visualisieren, einschließlich Netzwerknutzungsmustern, Datenverkehrsmustern sowie verdächtigen Aktivitäten und Anomalien.

In Panorama können Sie Inhalte des ACC 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 Dropdown-Liste **Device Group (Gerätegruppe)** das Symbol **Cloud Device Group (Cloud-Gerätegruppe)** 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 (Gerätename)**. 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 (Speichern)**.

Klicken Sie auf das Symbol **Load Filter (Filter laden)**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

Cloud NGFW-Protokolle im Strata-Protokollierungsdienst anzeigen

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 Webschnittstelle von Strata Logging Service können Sie die Datenverkehrs-, Bedrohungs- und Entschlüsselungsprotokolle anzeigen, die von Ihren Cloud NGFW-Ressourcen generiert wurden.

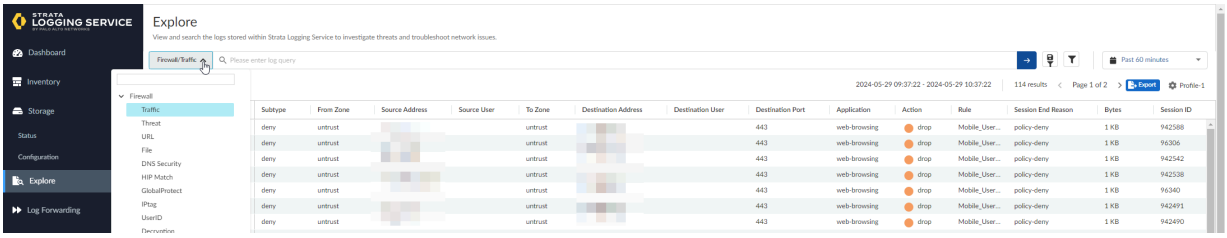
Wenn Sie Panorama verwenden und den Strata-Protokollierungsdienst nicht für die Protokollerfassung verwenden, können Sie Protokolle an eine andere Entität weiterleiten, müssen jedoch den Strata-Protokollierungsdienst in Ihrem Protokollierungsprofil aktivieren.

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.

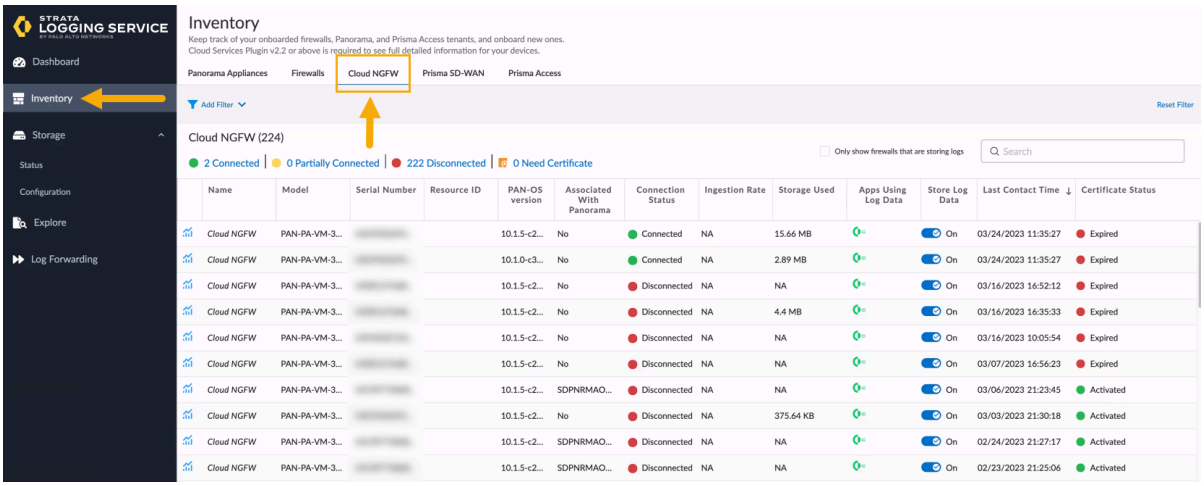
STEP 2 | Wählen Sie **Explore (Erkunden)** aus.

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.



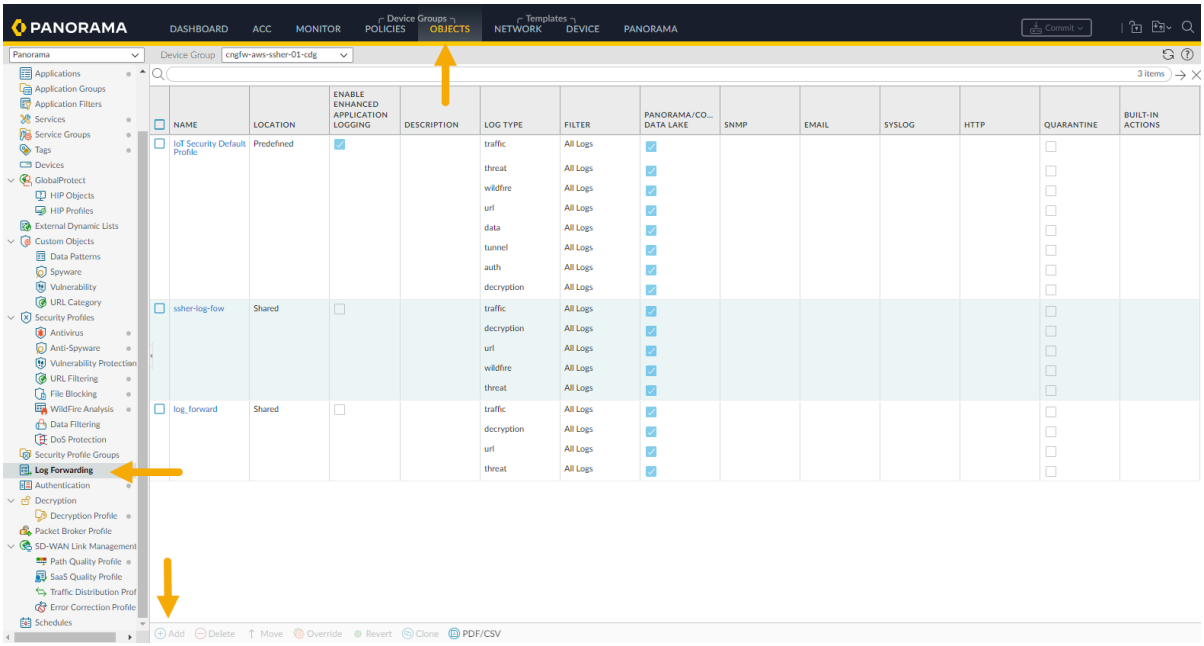
Protokolle an den Strata-Protokollierungsdienst weiterleiten

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.

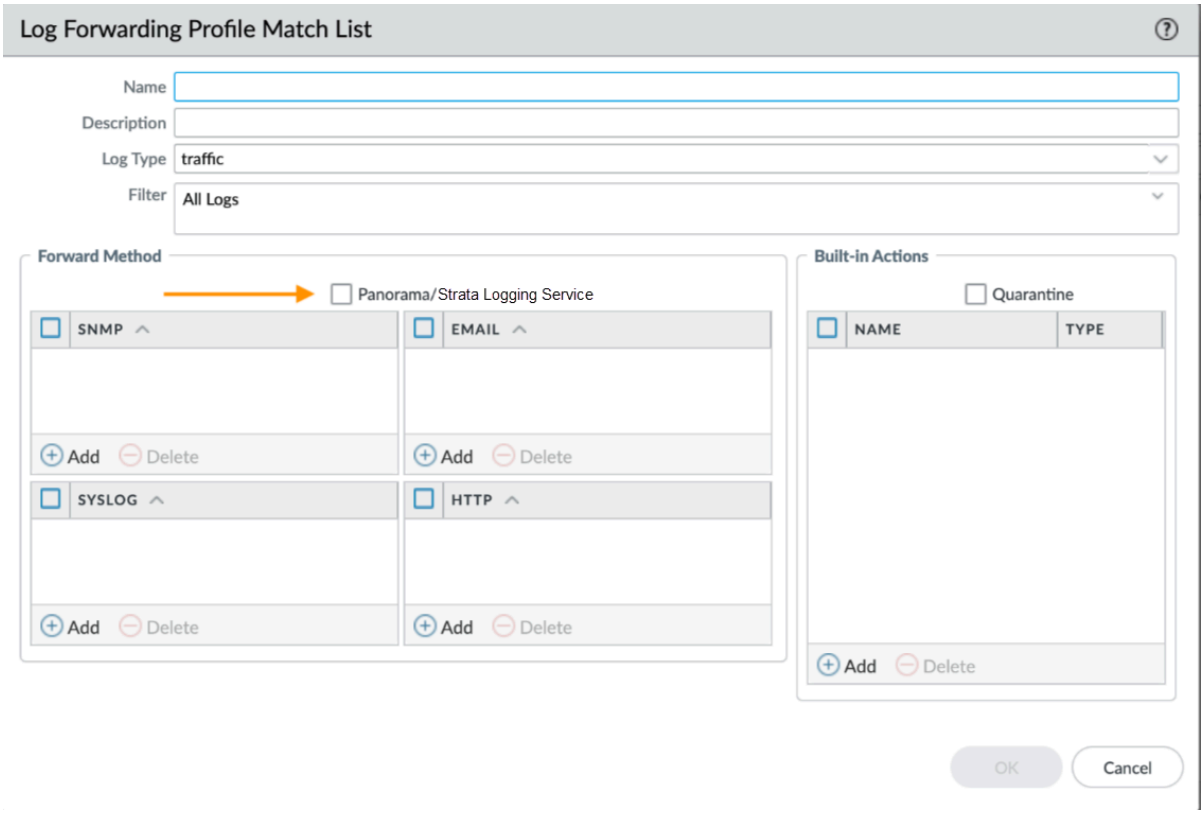
STEP 3 | Klicken Sie auf **Add (Hinzufügen)**, um ein neues Profil für die Übereinstimmungsliste zur Protokollweiterleitung zu erstellen.



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.

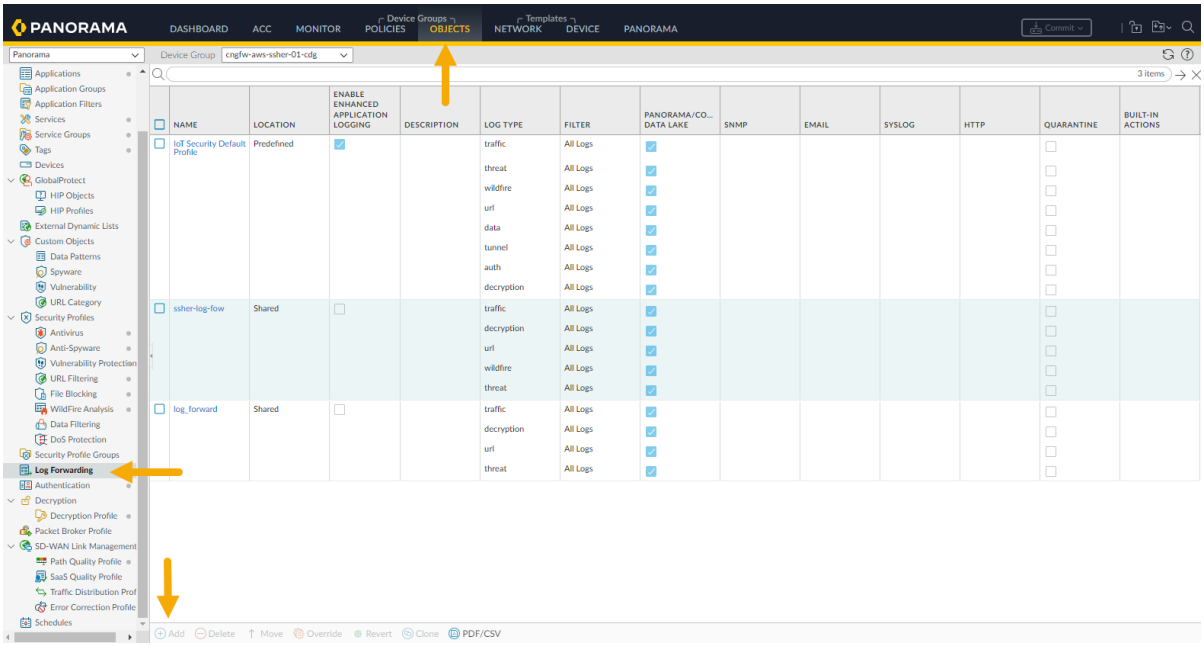
Protokolle ohne den Strata-Protokollierungsdienst weiterleiten

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**.

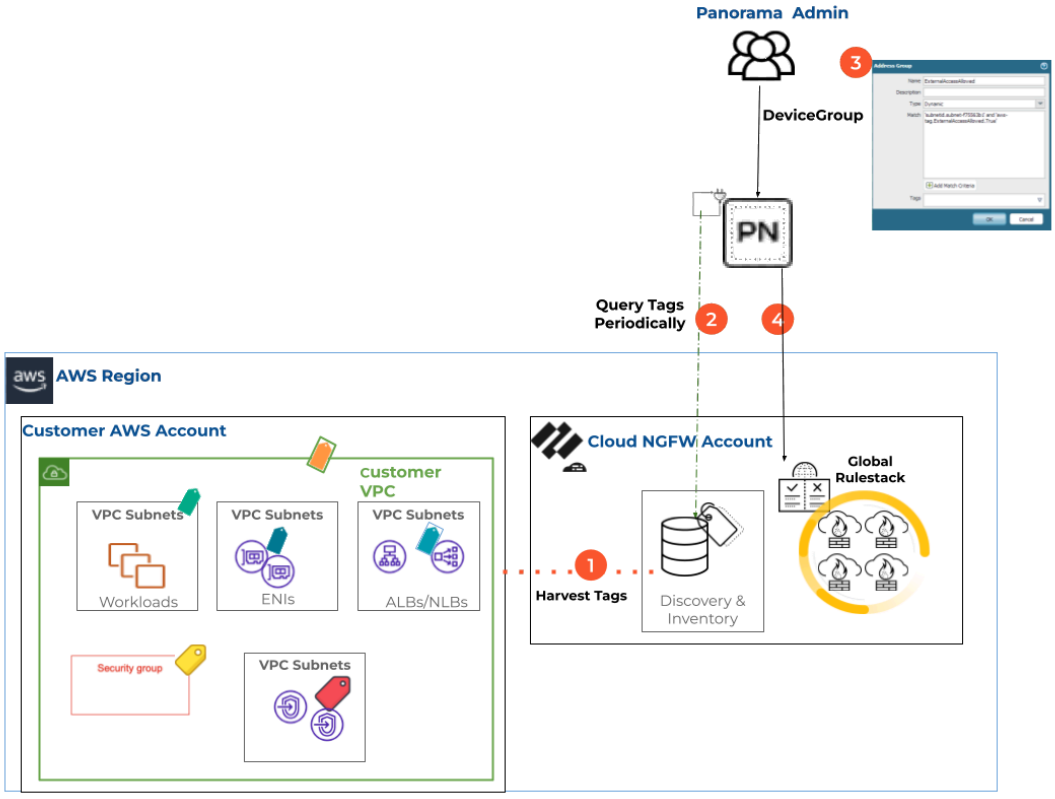
STEP 7 | Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

Tagbasierte Richtlinien

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 den von Ihnen hinzugefügten AWS-Konten 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 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 Richtlinien 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.
- Cloud NGFW-Konsole verwenden AWS-Konten zum Cloud NGFW-Mandanten hinzufügen, um aus diesen Tags zu sammeln.
- Panorama-Plug-in verwenden, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen.
- Dynamic-Address-Group(DAG)-Objekte mit Tags in Gerätegruppen konfigurieren.

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 Richtlinien für Cloud NGFW für AWS-Ressourcen zu aktivieren, müssen Sie Ihre Panorama-Appliance für diese Integration vorbereiten, indem Sie das AWS-Plug-in 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. AWS-Konten zum Cloud NGFW-Mandanten hinzufügen, um aus diesen Tags zu sammeln
2. Panorama-Plug-in verwenden, um Tags abzufragen und sie den Panorama-Gerätegruppen hinzuzufügen.
3. Dynamic-Address-Group(DAG)-Objekte mit Tags in Gerätegruppen konfigurieren.

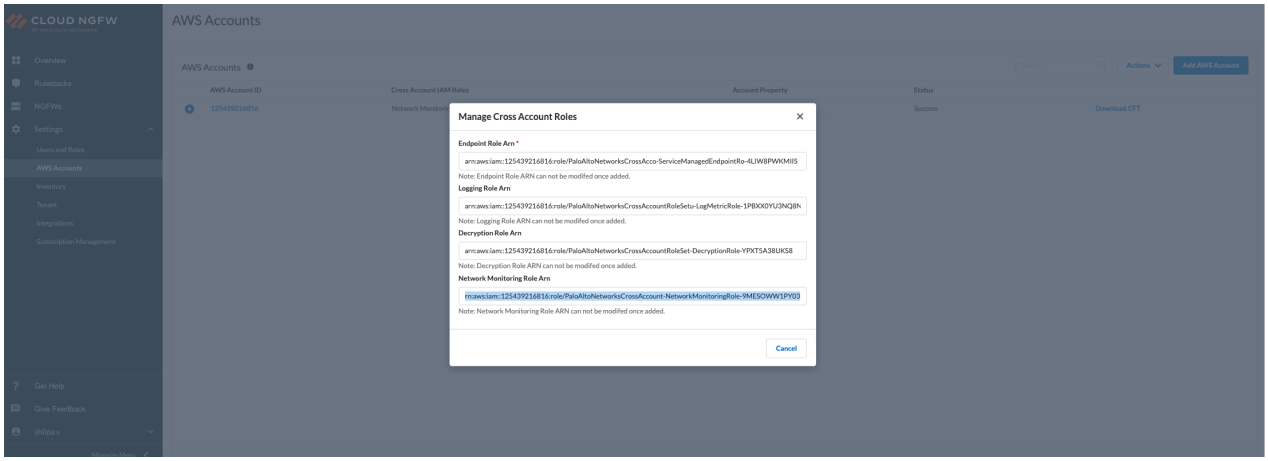
AWS-Konten zum Cloud NGFW-Mandanten hinzufügen, um aus diesen Tags zu sammeln

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.



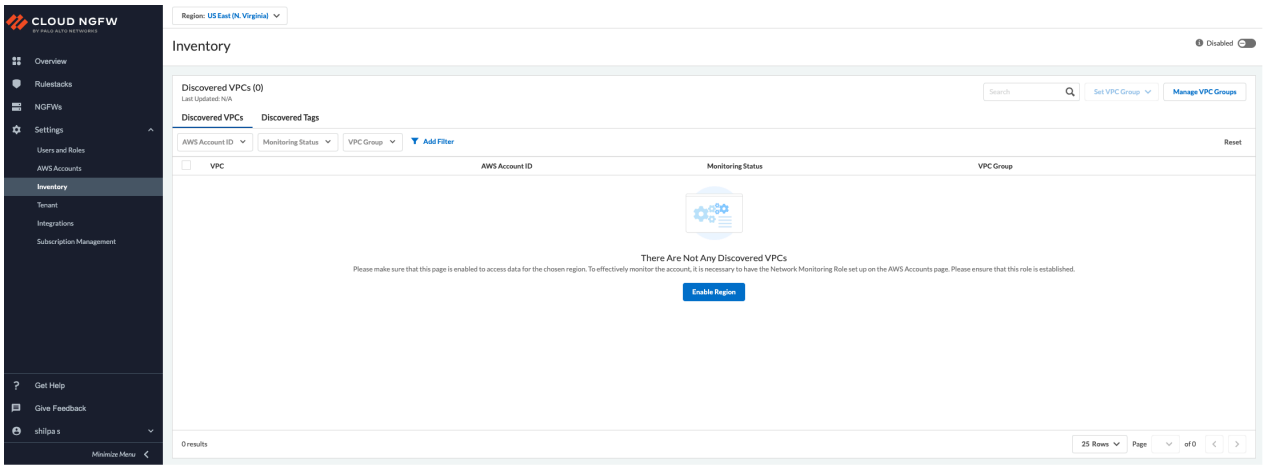
Überwachung aktivieren

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.

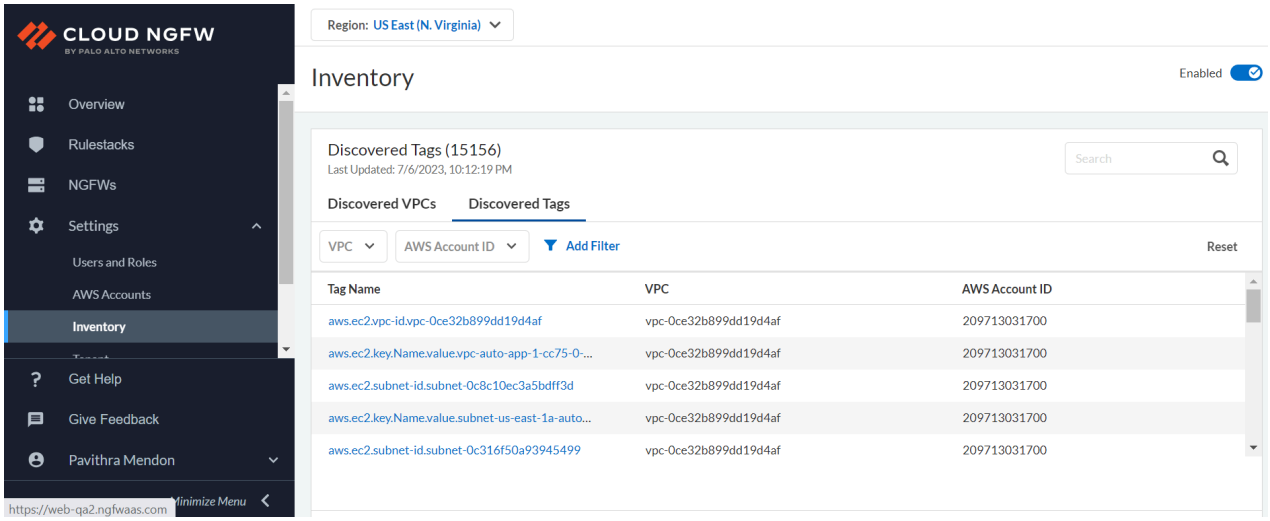
Die Schaltfläche **Enable Region (Region aktivieren)** unter der Registerkarte **Discovered VPCs (Erkannte VPCs)** wird nur angezeigt, wenn Sie Ihr AWS-Konto zum ersten Mal einbinden. Wählen Sie aus der Dropdown-Liste die Option **Region** aus und klicken Sie auf **Enable Region (Region aktivieren)**, 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.

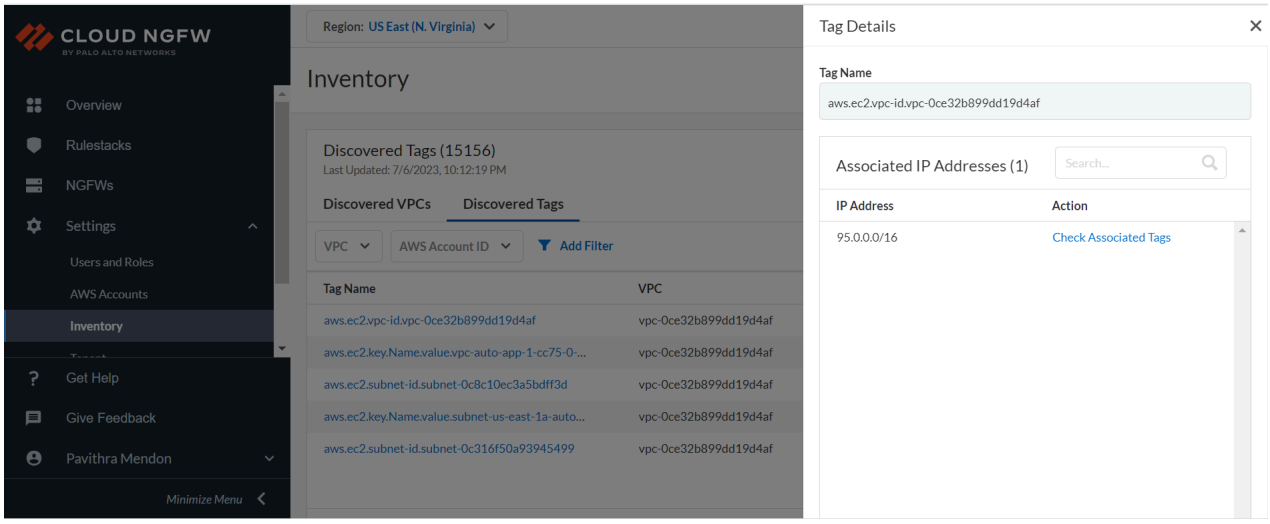


Gesammelte Tags in der Cloud NGFW-Konsole anzeigen

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/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:

1. VPC-Gruppen erstellen und verwalten.
2. Tags mithilfe von Überwachungsdefinitionen und Benachrichtigungsgruppen zu Gerätegruppen hinzufügen.

Installieren und konfigurieren Sie das AWS-Plug-in 5.1.0 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.

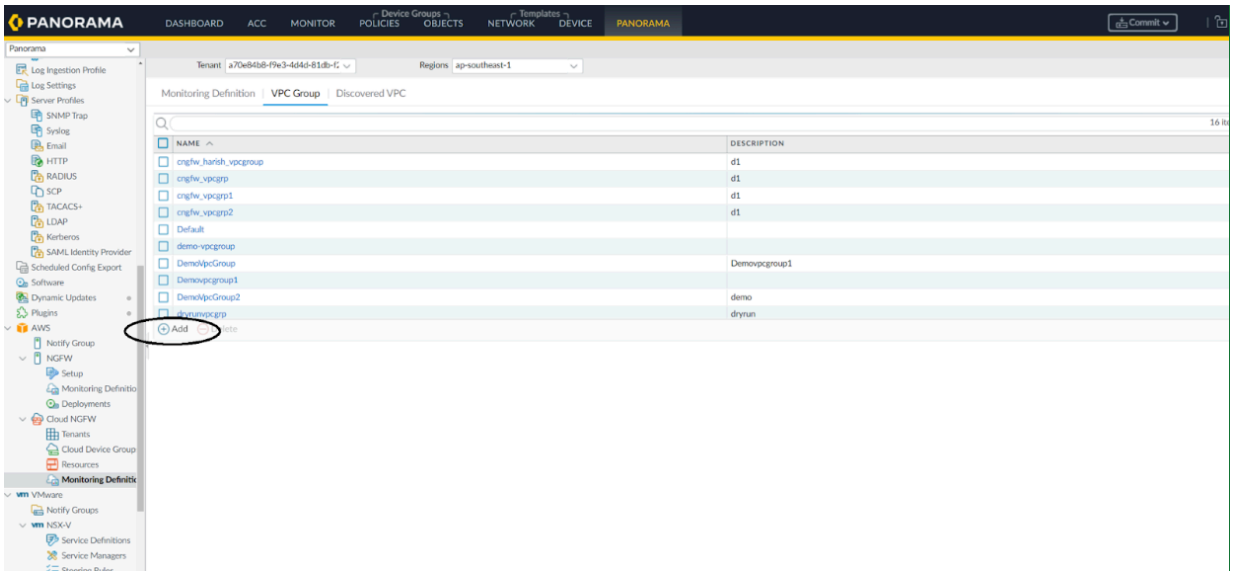
Der Umfang einer in einer Region erstellten VPC-Gruppe gilt nur für diese Region. Beispielsweise kann auf die in Region X erstellte VPC-Gruppe A in Region Y nicht zugegriffen werden.

Alternativ können Sie neue VPC-Gruppen erstellen und diese VPCs mit den folgenden Schritten in andere VPC-Gruppen verschieben:

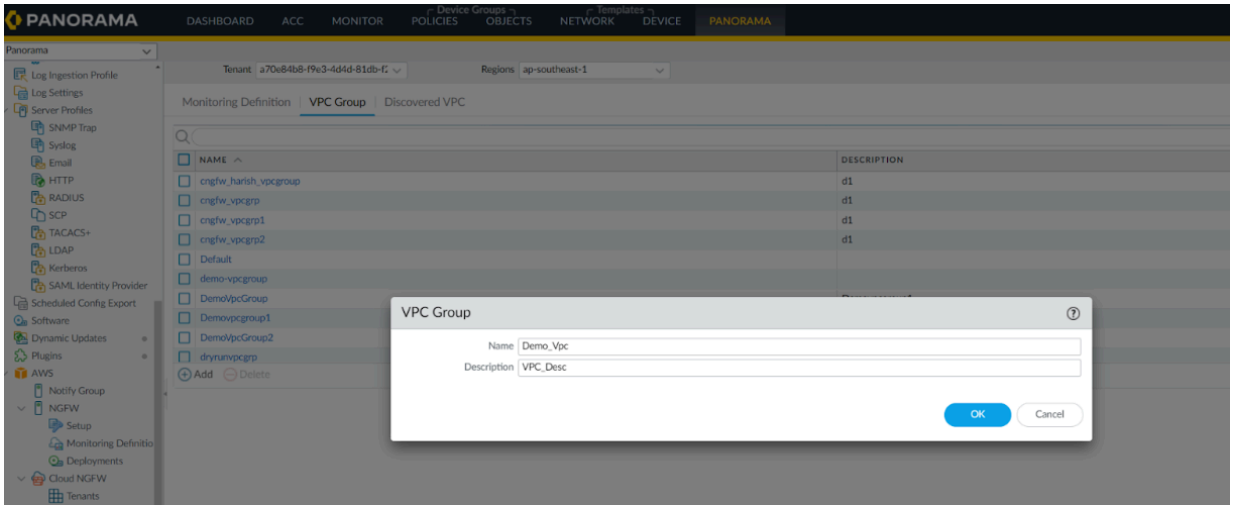
Wenn Sie eine neue, **vom Standard abweichende VPC-Gruppe** auf Panorama erstellen möchten, gehen Sie wie im folgenden Verfahren beschrieben vor:

1. Wechseln Sie in der **Panorama**-Konsole auf die Registerkarte **Panorama** und klicken Sie anschließend auf **AWS**.
2. Wählen Sie den **Mandanten** und die **Region** aus.

3. Wechseln Sie zu **AWS** > **Cloud NGFW** > **Monitoring Definition (Überwachungsdefinition)** > **VPC Group (VPC-Gruppe)** > **Add (Hinzufügen)**.

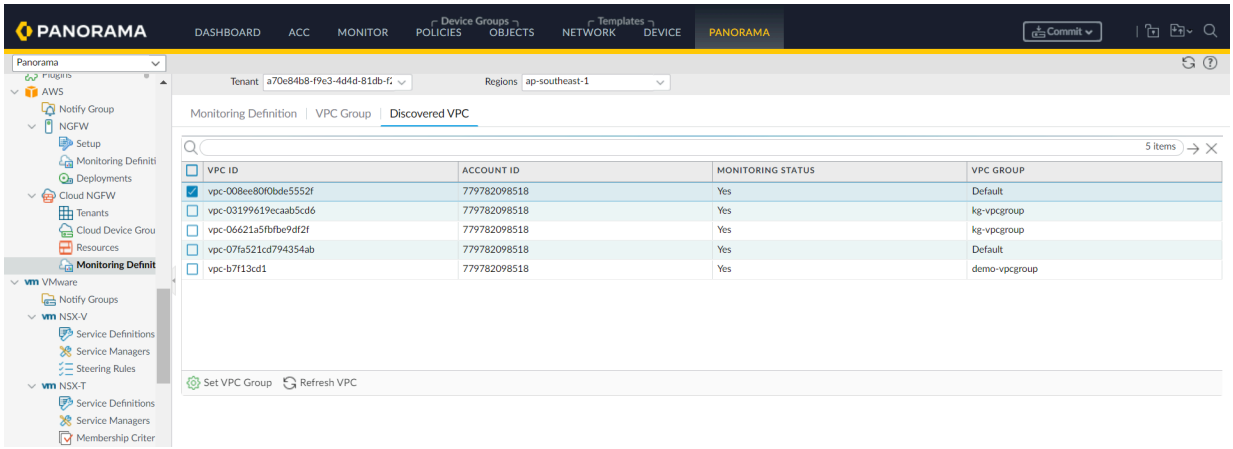


4. Geben Sie den **Namen** und eine **Beschreibung** für die VPC-Gruppe ein.



5. Klicken Sie auf **OK**.

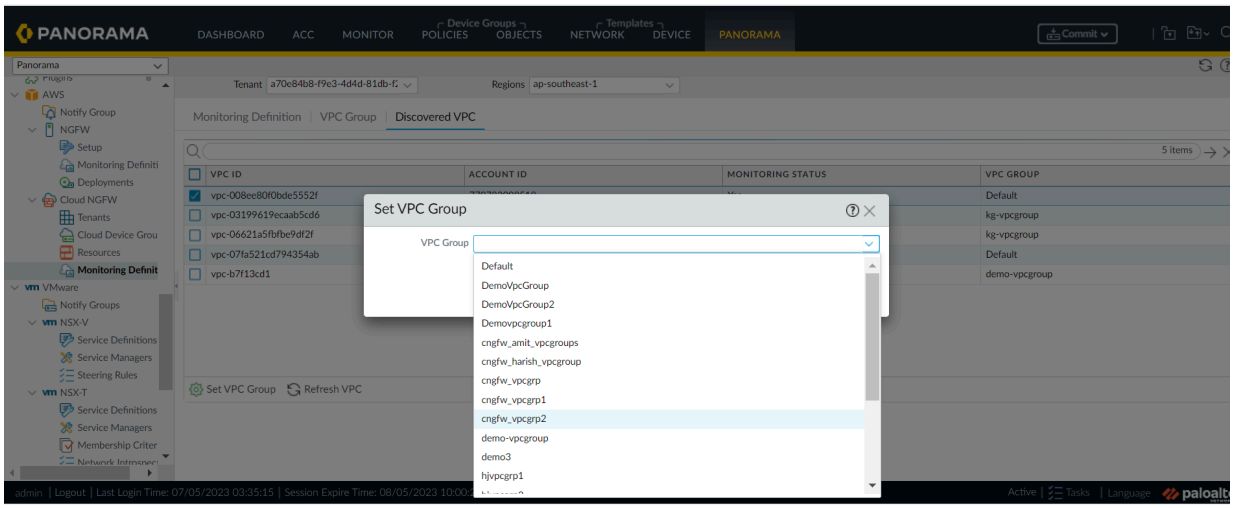
6. Wechseln Sie zu **AWS** > **Cloud NGFW** > **Monitoring Definition (Überwachungsdefinition)** > **Discovered VPC (Erkannte VPC).**



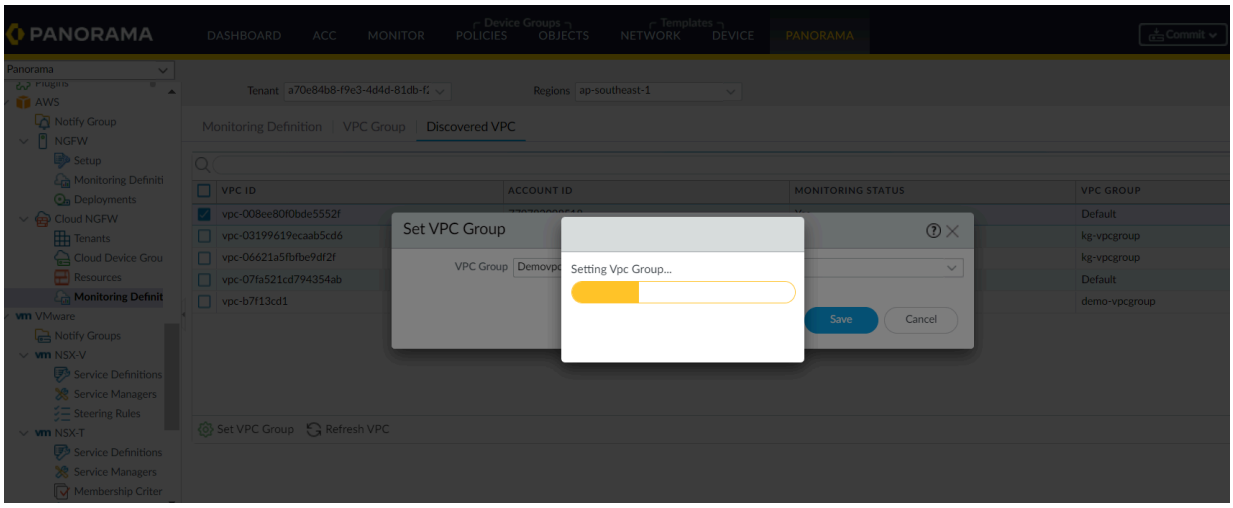
- *Sie können einer **VPC-Gruppe** maximal acht Gerätegruppen zuordnen. Für eine bessere Leistung konfigurieren Sie Überwachungsdefinitionen mit VPC-Gruppen so, dass einer bestimmten VPC-Gruppe (über Benachrichtigungsgruppen) nur acht Gerätegruppen zugeordnet sind.*
- *Die **Standard**-VPC-Gruppe wird 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.*

7. Klicken Sie auf **Set VPC Group (VPC-Gruppe festlegen)**.

8. Wählen Sie eine **VPC-Gruppe** aus.



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



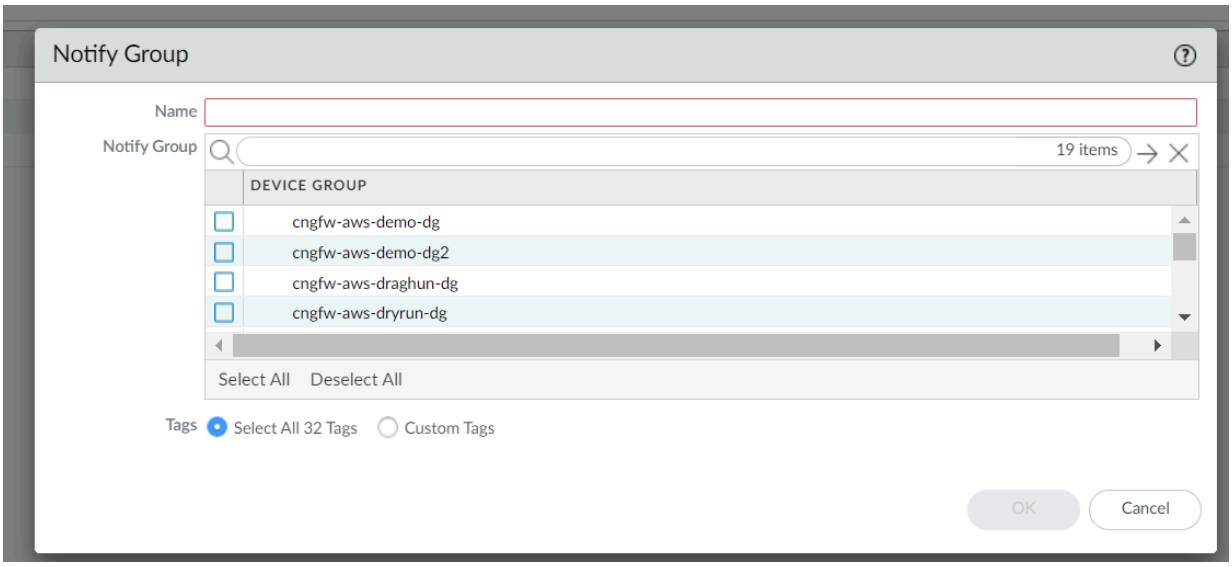
Tags mithilfe von Überwachungsdefinitionen und Gerätegruppen zu Gerätegruppen hinzufügen

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:

1. Wechseln Sie in der **Panorama-Plug-in**-Konsole zu **AWS** > **Notify Group (Benachrichtigungsgruppe)**.

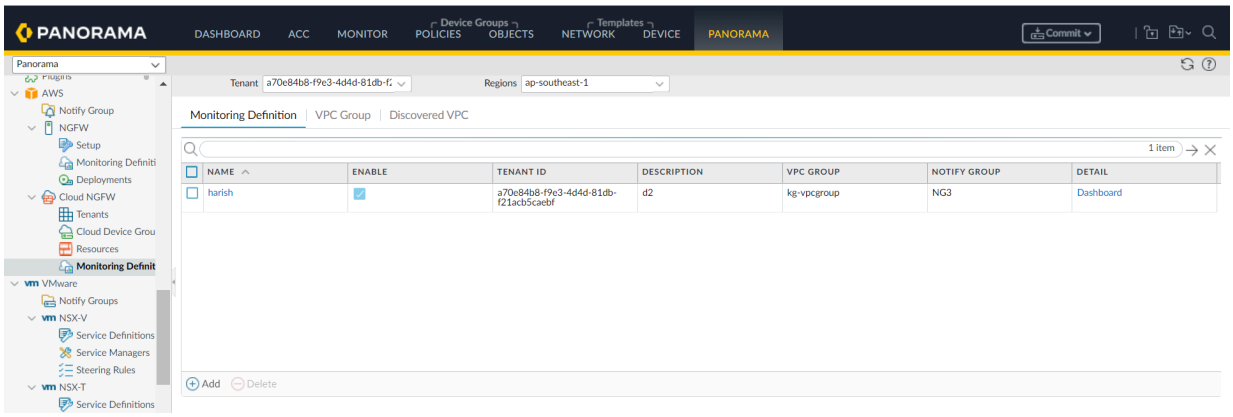
2. Klicken Sie auf **Add (Hinzufügen)**.



3. Geben Sie einen **Namen** ein.
4. Wählen Sie die **Gerätegruppe** und **Tags** aus.
5. Klicken Sie auf **OK**.

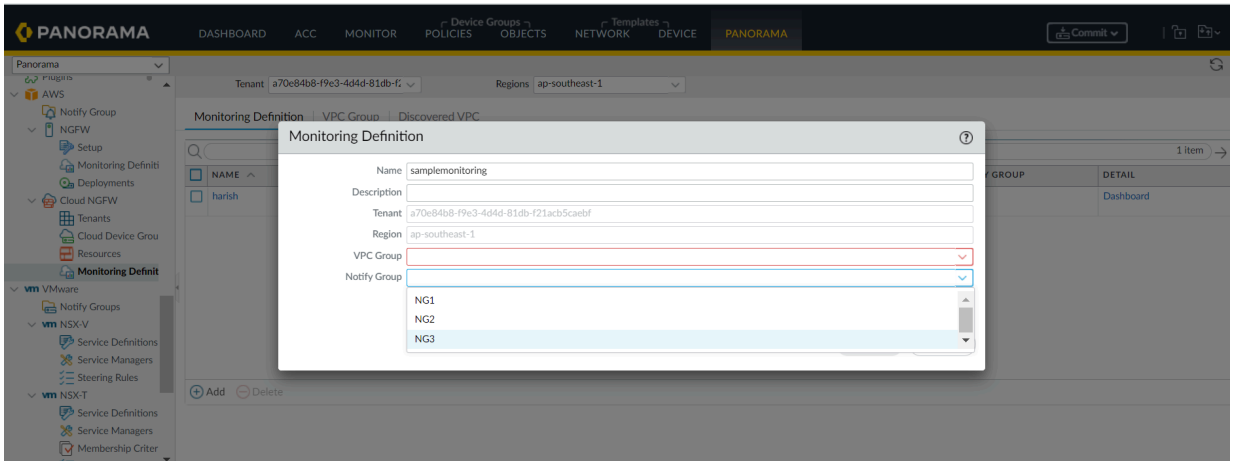
Erstellen Sie eine Cloud-**Überwachungsdefinition**, die die erforderliche **VPC-Gruppe** und **Benachrichtigungsgruppe** für von Cloud NGFW erlernte Tags zuordnet.

1. Wechseln Sie in der **Panorama**-Konsole zu **AWS** > **Cloud NGFW** > **Monitoring Definition (Überwachungsdefinition)**.



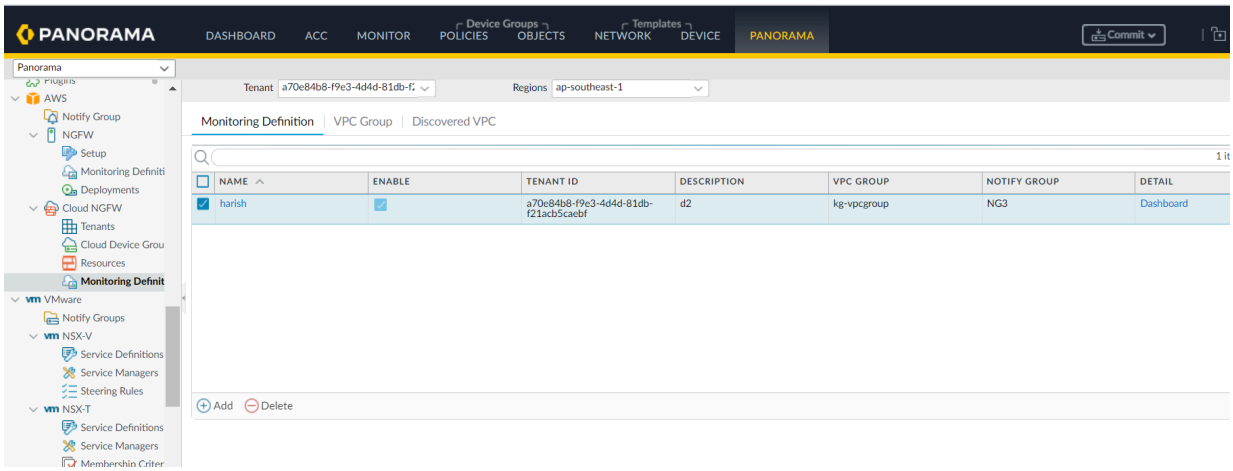
2. Klicken Sie auf **Add (Hinzufügen)**.
3. Geben Sie Ihren **Namen** und eine **Beschreibung** ein.
4. Wählen Sie im Dropdown-Menü **VPC Group (VPC-Gruppe)** die erforderliche VPC-Gruppe aus.

5. Wählen Sie im Dropdown-Menü **Notify Group (Benachrichtigungsgruppe)** die gewünschte Benachrichtigungsgruppe aus.

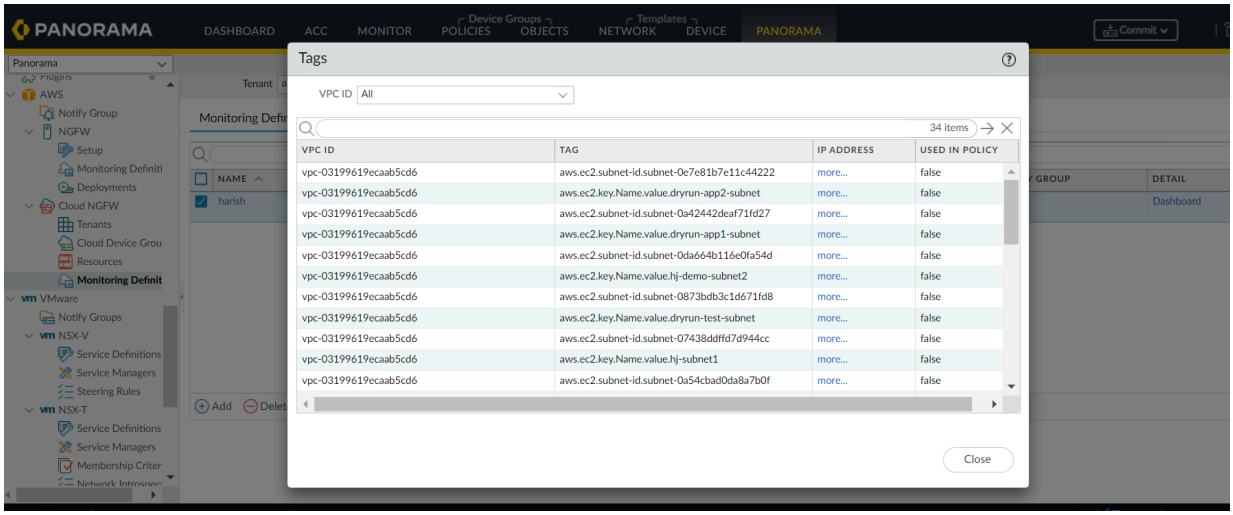


6. Klicken Sie auf **OK**.
7. Führen Sie einen **Commit** aus und übertragen Sie Ihre Änderungen per **Push** an Panorama.

8. 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.



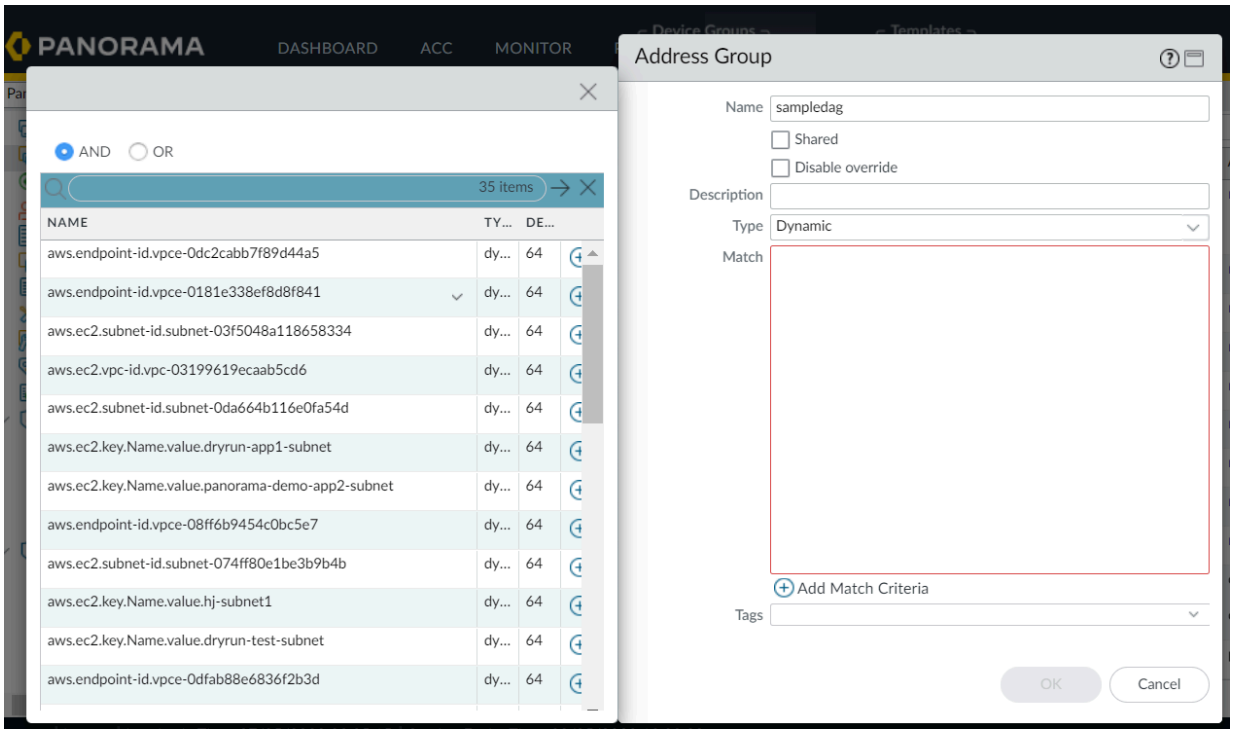
Dynamic-Address-Group(DAG)-Objekte mit Tags in Gerätegruppen konfigurieren

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:

1. Wechseln Sie in der **Panorama**-Konsole auf die Registerkarte **Objects (Objekte)**.
2. Wechseln Sie im linken Bereich zu **Address Groups (Adressgruppen)**.
3. Klicken Sie auf **Add (Hinzufügen)**.
4. Geben Sie den **Namen** Ihrer Adressgruppe ein und wählen Sie den Typ **Dynamic (Dynamisch)** aus.

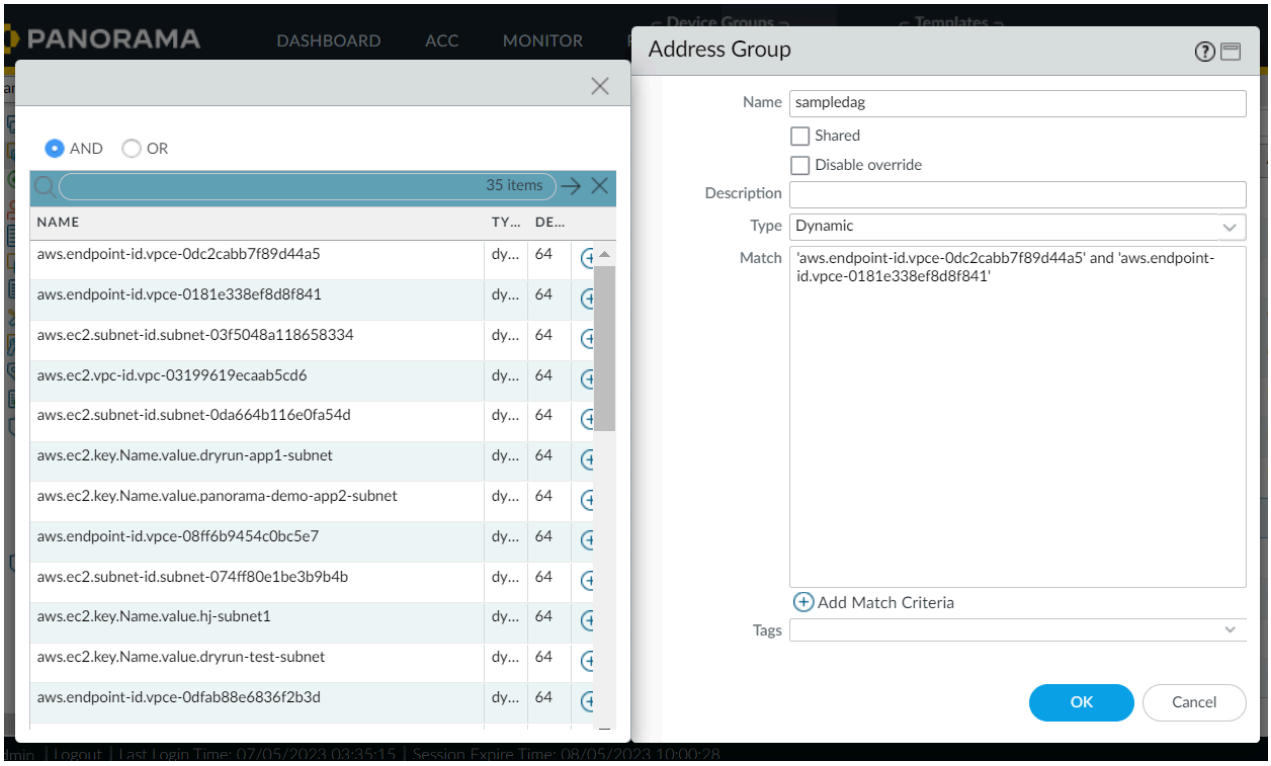
5. Klicken Sie auf **Add match Criteria (Übereinstimmungskriterien hinzufügen)**.



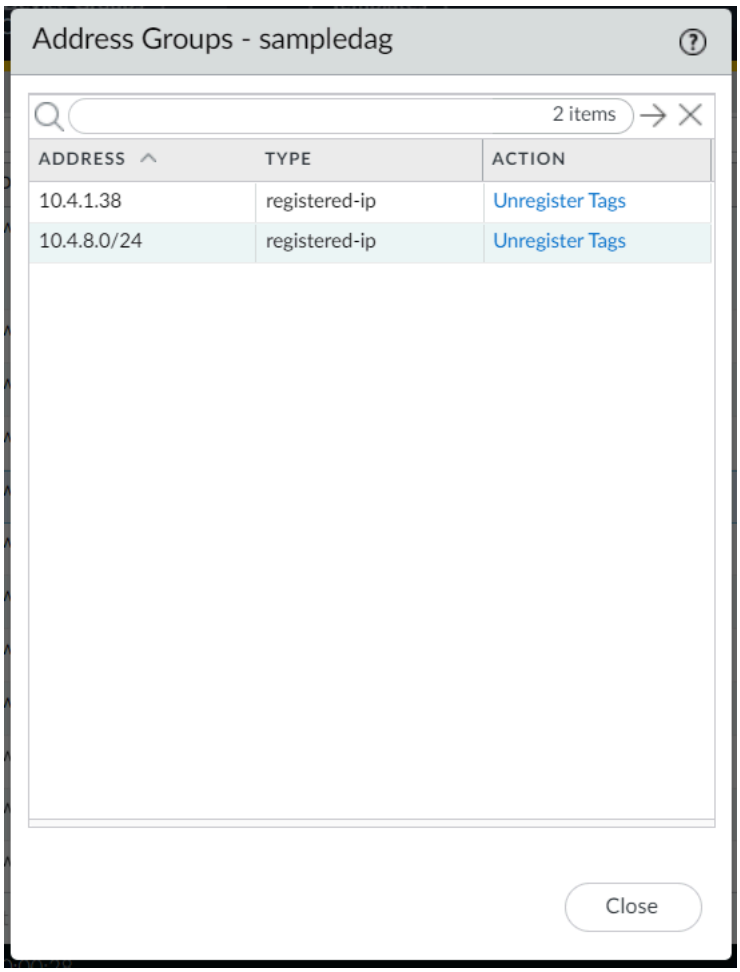
Sie können jetzt **Richtlinien für dynamische Adressgruppen** erstellen, die auf die oben erstellten DAGs für Cloud-Gerätegruppen verweisen.

Sie können Ihrem DAG-Objekt Tags aus verschiedenen Regionen 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.

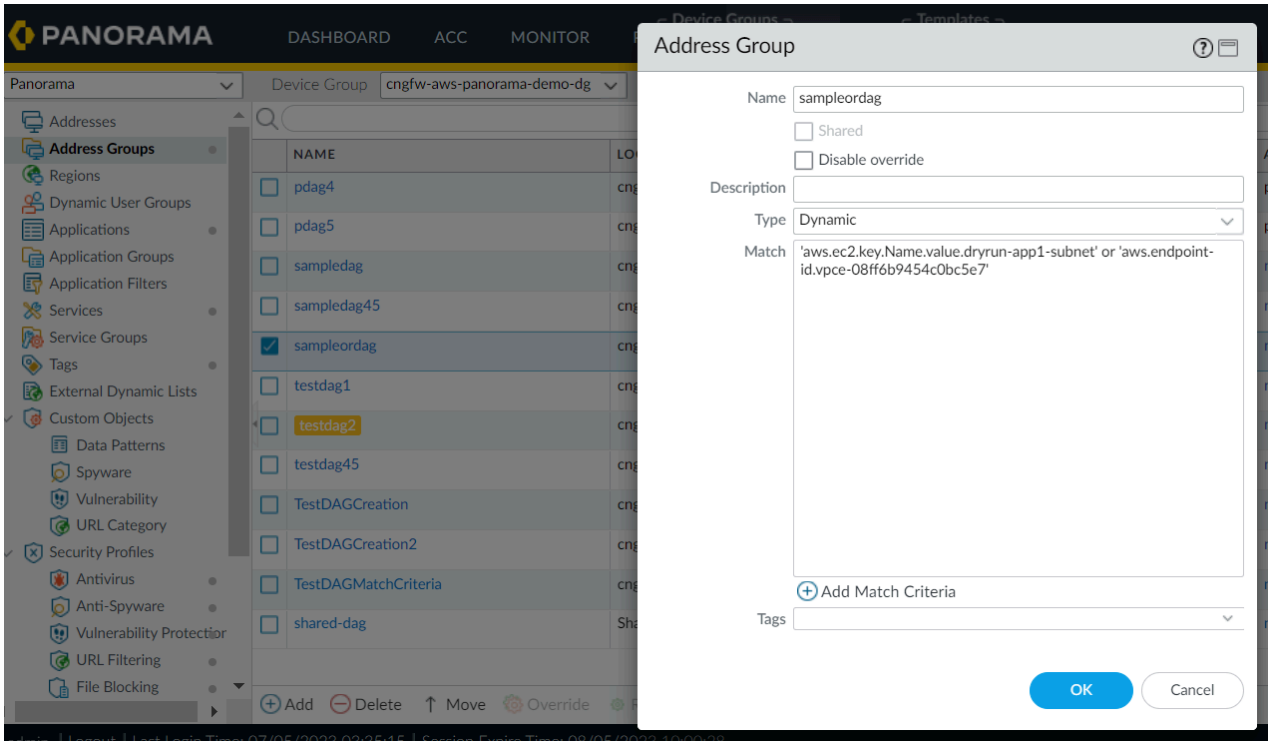
Das nachfolgende Beispiel veranschaulicht, wie DAGs mit dem Operator **AND** erstellt werden:



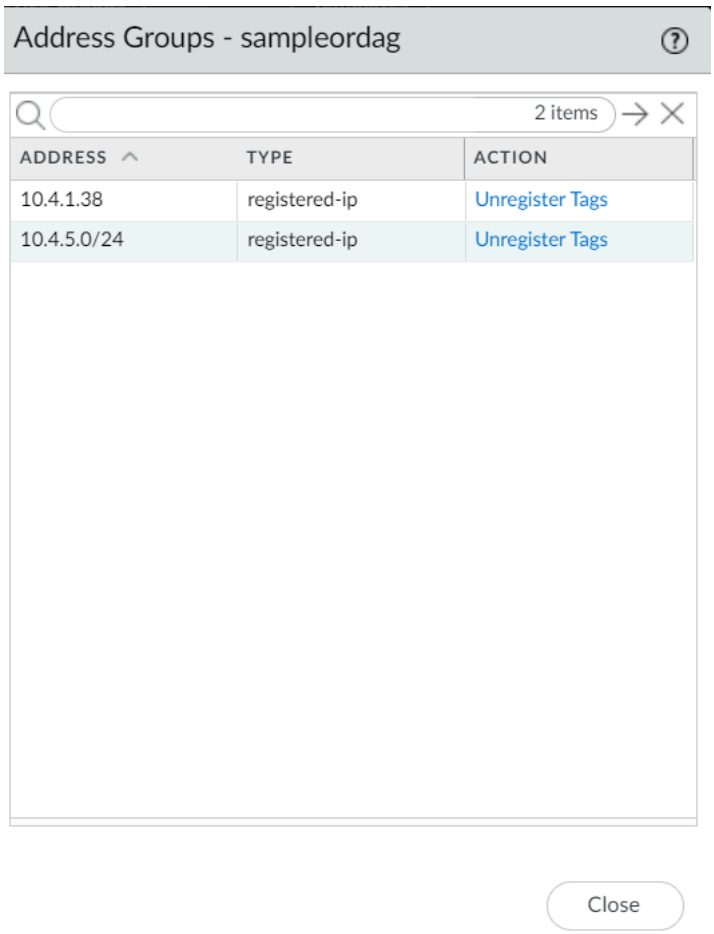
Die Adressgruppe zeigt die Liste der Adressen an, die beiden Übereinstimmungskriterien entsprechen.



Das nachfolgende Beispiel veranschaulicht, wie DAGs mit dem Operator **OR** erstellt werden:



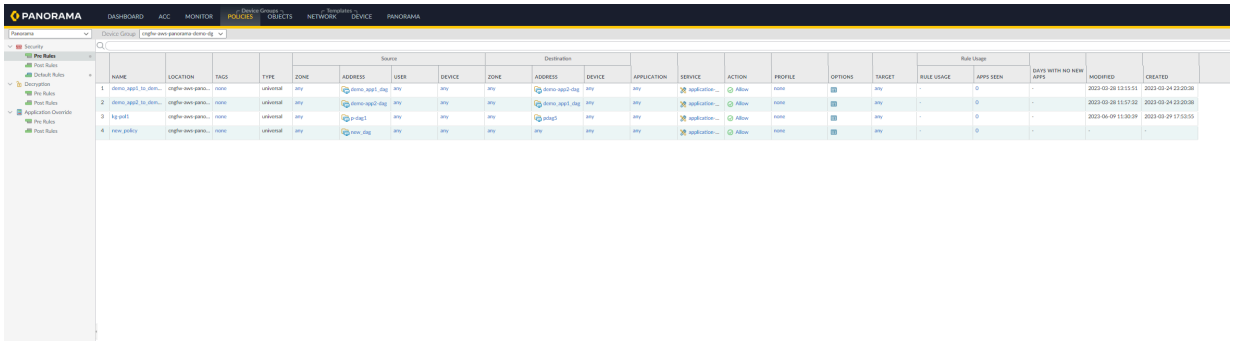
Die Adressgruppe zeigt die Liste der Adressen an, die einem der angegebenen Übereinstimmungskriterien entsprechen.



Im Folgenden sind die Schritte zum Erstellen dynamischer Adressrichtlinien aufgeführt, die auf DAGs für Cloud-Gerätegruppen verweisen:

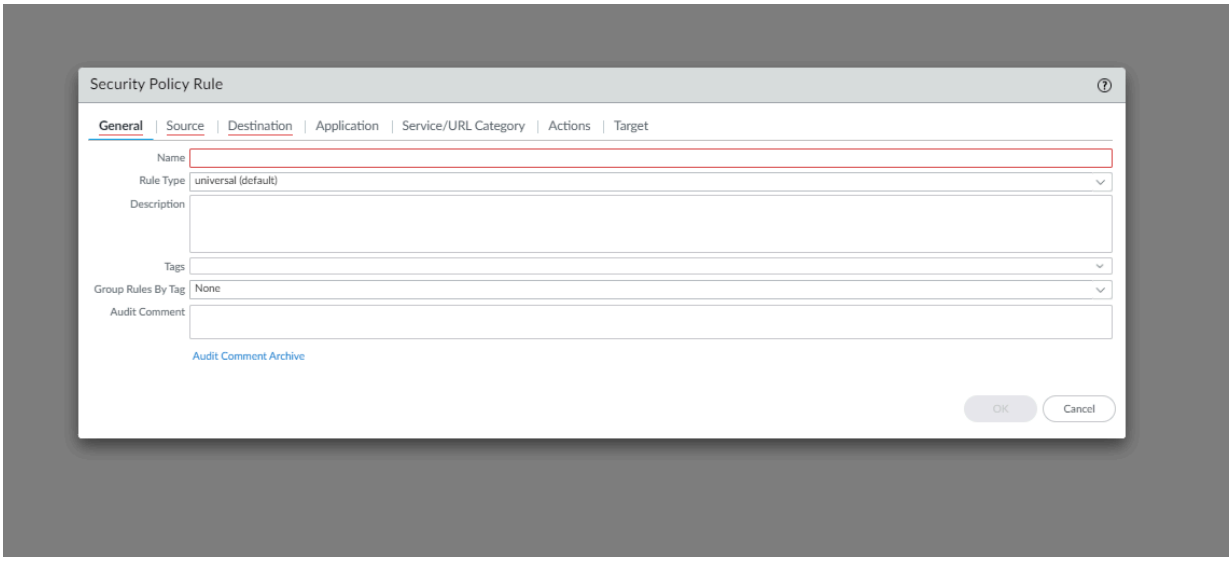
1. Wechseln Sie in der **Panorama**-Konsole zur Registerkarte **Policies (Richtlinien)**.

2. Wechseln Sie zu **Security (Sicherheit)** > **Pre/Post/Default Rules (Vor-/Nach-/Standardregeln)**.

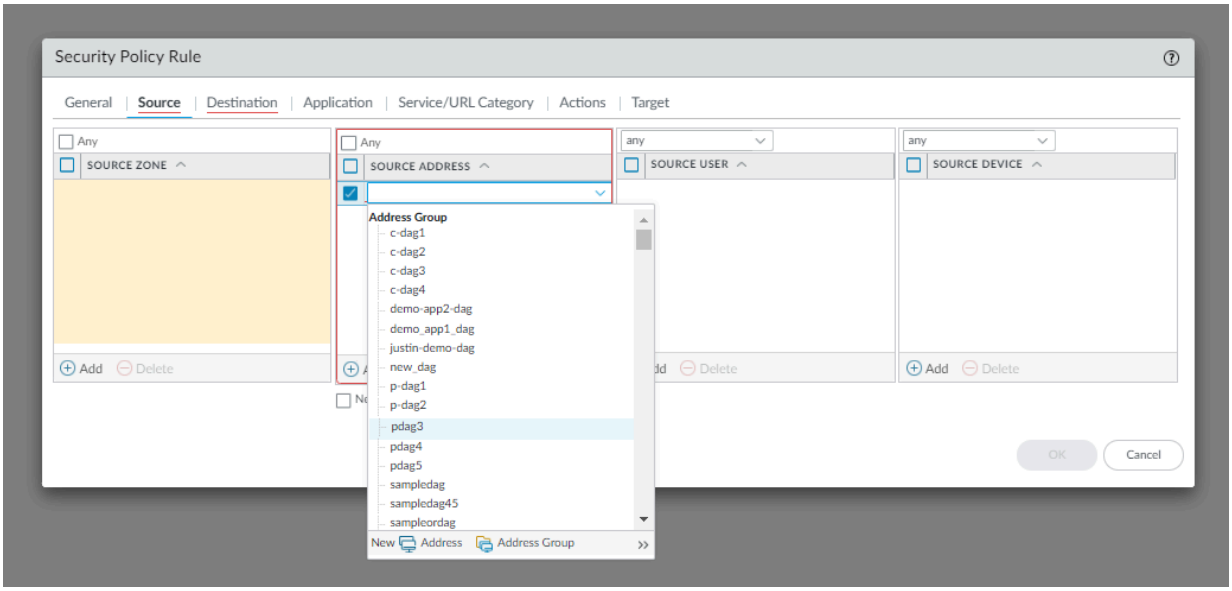


3. Klicken Sie auf **Add (Hinzufügen)**.

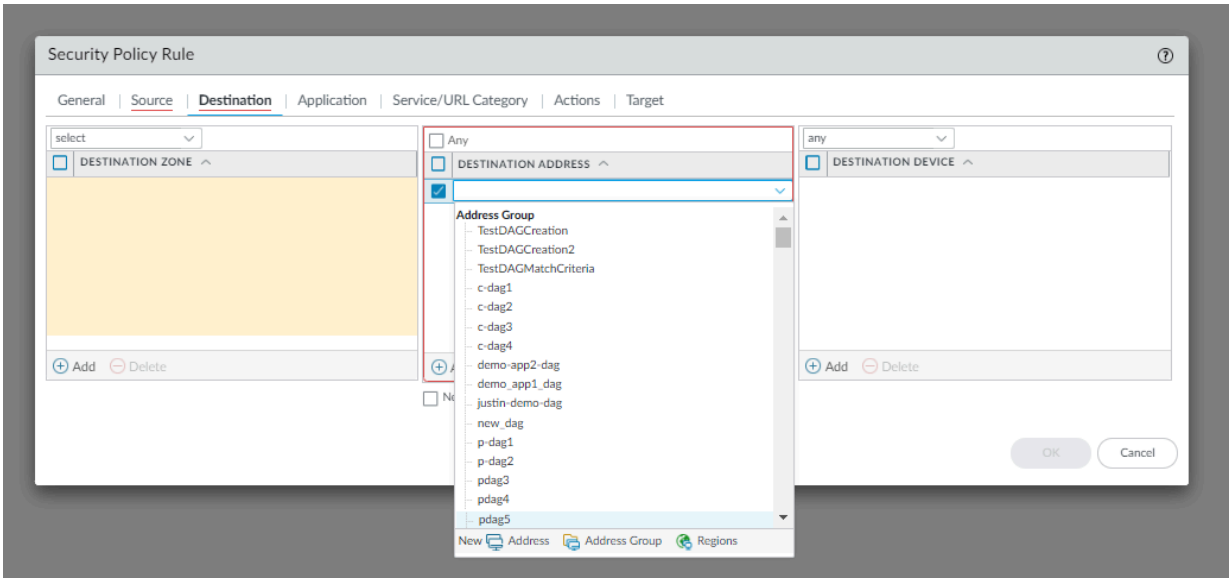
4. Geben Sie im Dialogfeld „Security Policy Rule“ (Sicherheitsrichtlinienregel) einen **Namen** für die Sicherheitsrichtlinienregel ein.



5. Wählen Sie auf der Registerkarte **Source (Quelle)** die DAG für das Feld **Source Address (Quelladresse)** aus und klicken Sie auf **Add (Hinzufügen)**.



6. Wählen Sie auf der Registerkarte **Destination (Ziel)** die DAG für das Feld **Destination Address (Zieladresse)** aus und klicken Sie auf **Add (Hinzufügen)**.

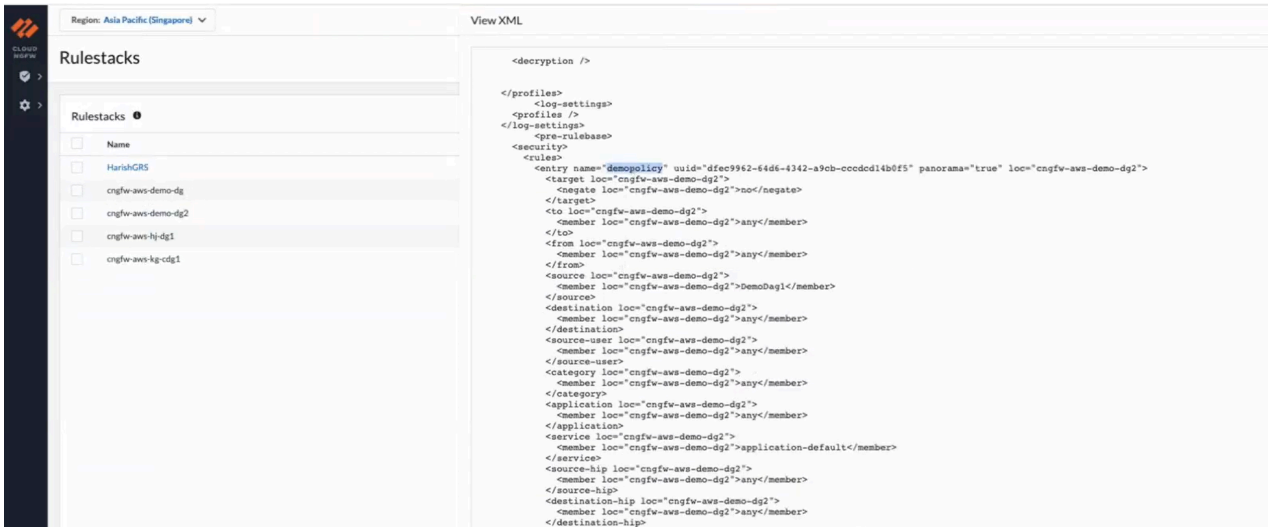


7. Klicken Sie auf **OK**.
8. Führen Sie einen **Commit** aus und übertragen Sie Ihre Änderungen per **Push** an die Cloud NGFW-Gerätegruppe.

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 dynamischen Adressrichtlinien zu überprüfen, die von Panorama an die jeweilige Cloud-Gerätegruppe gesendet wurden. Klicken

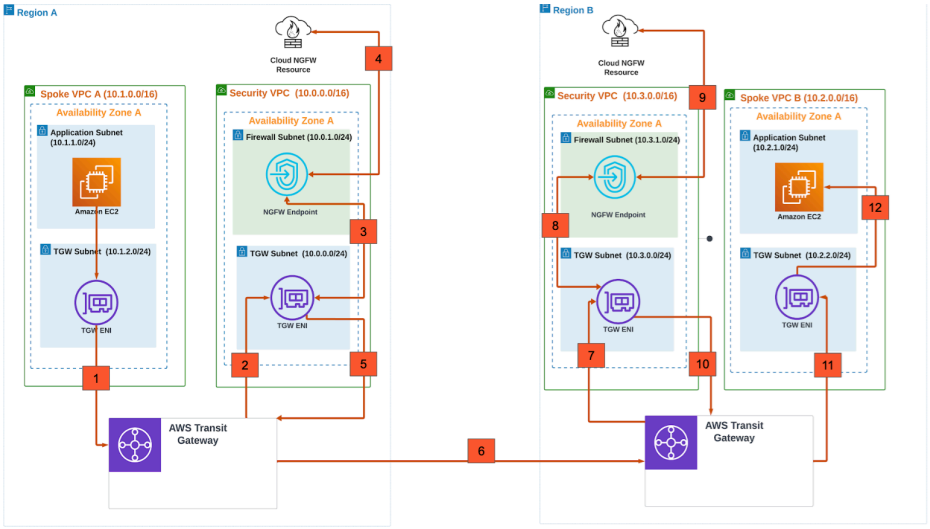
Wechseln Sie zu **View XML (XML anzeigen)**, um Informationen zu dynamischen Adressrichtlinien anzuzeigen, die neu zur Cloud-Gerätegruppe hinzugefügt wurden.



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 lernen muss und diese dann für die Cloud-Gerätegruppe in Region X verwenden möchte, gehen Sie wie folgt vor:

1. Fügen Sie dem Cloud NGFW-Mandanten AWS-Konten hinzu und sammeln Sie Tags daraus.
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.

   Sie werden nur die Tags der Region X sehen können, die zum Konfigurieren Ihrer DAG-Objekte verfügbar sind.
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.
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).
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.
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.

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

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 für die E-DLP-Integration

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

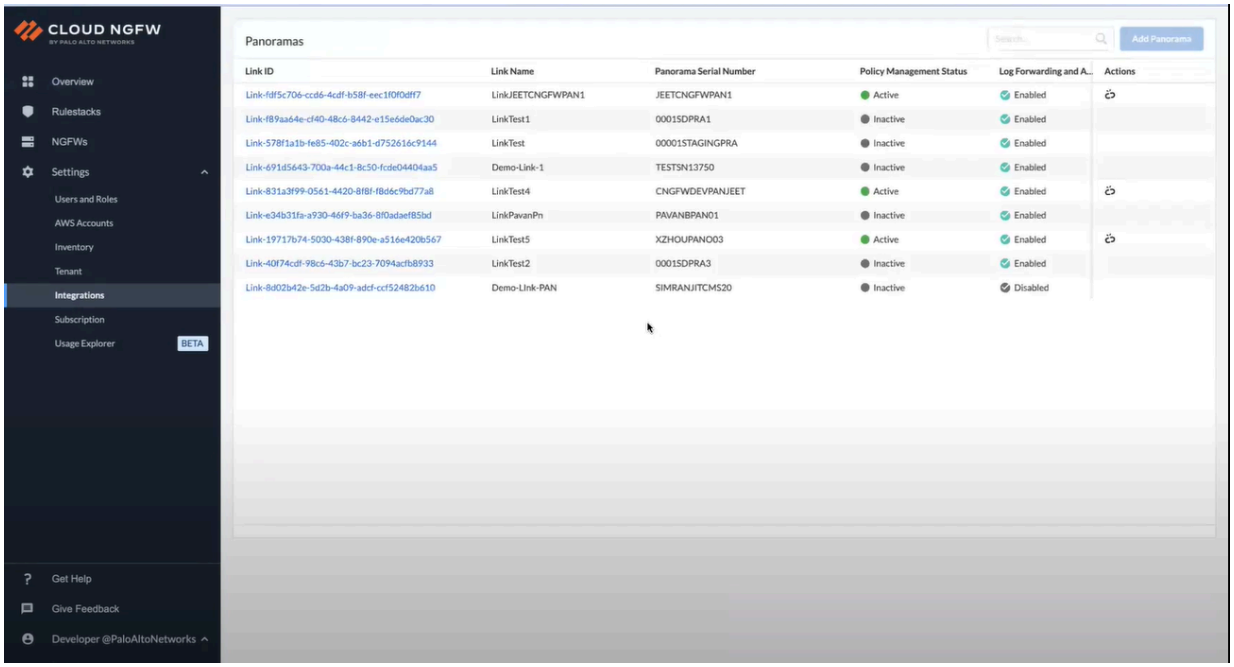
Wenn Sie über einen DLP-Mandanten in Ihrem Customer-Support-Portal(CSP)-Konto verfügen, der in Panorama bereitgestellt wird, verwendet der Cloud NGFW-Dienst diesen DLP-Mandanten, um DLP in Cloud NGFW zu integrieren.

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

Im Folgenden sind die Schritte zum Aktivieren eines neuen DLP-Mandanten in der Cloud NGFW-Konsole aufgeführt:

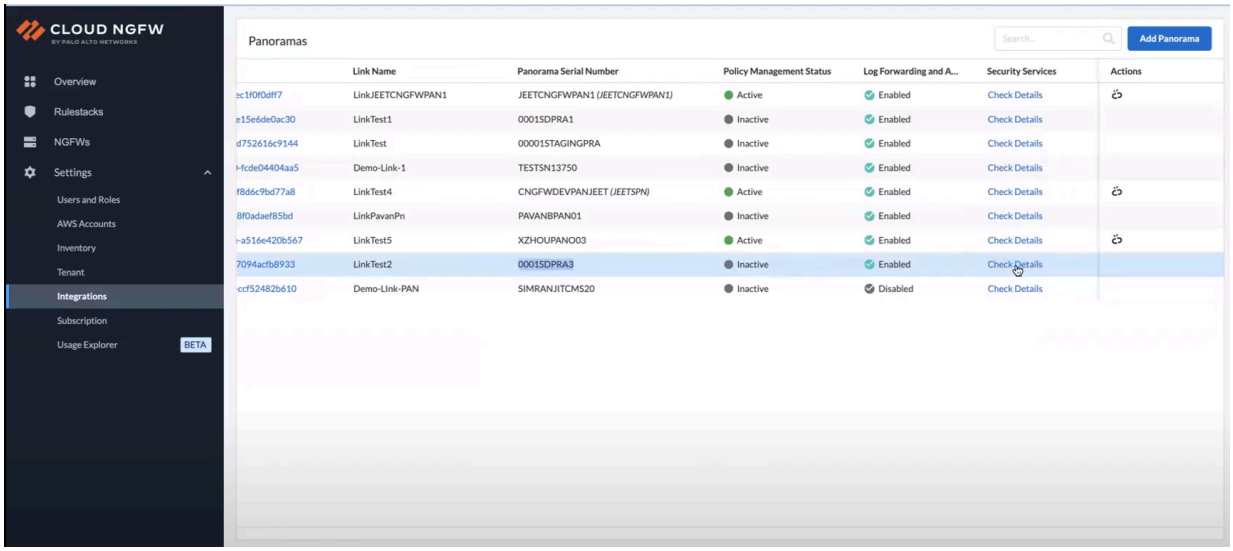
1. Melden Sie sich bei der Cloud NGFW-Konsole an.

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



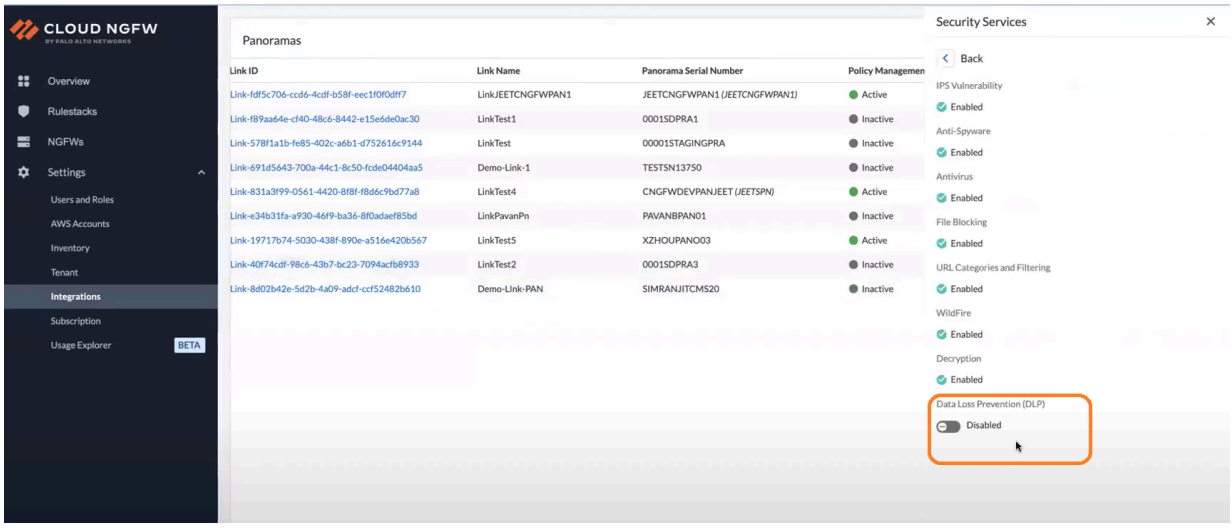
Auf der Seite **Integrations (Integrationen)** werden Informationen über die aktuell verknüpfte Panorama-Instanz angezeigt.

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

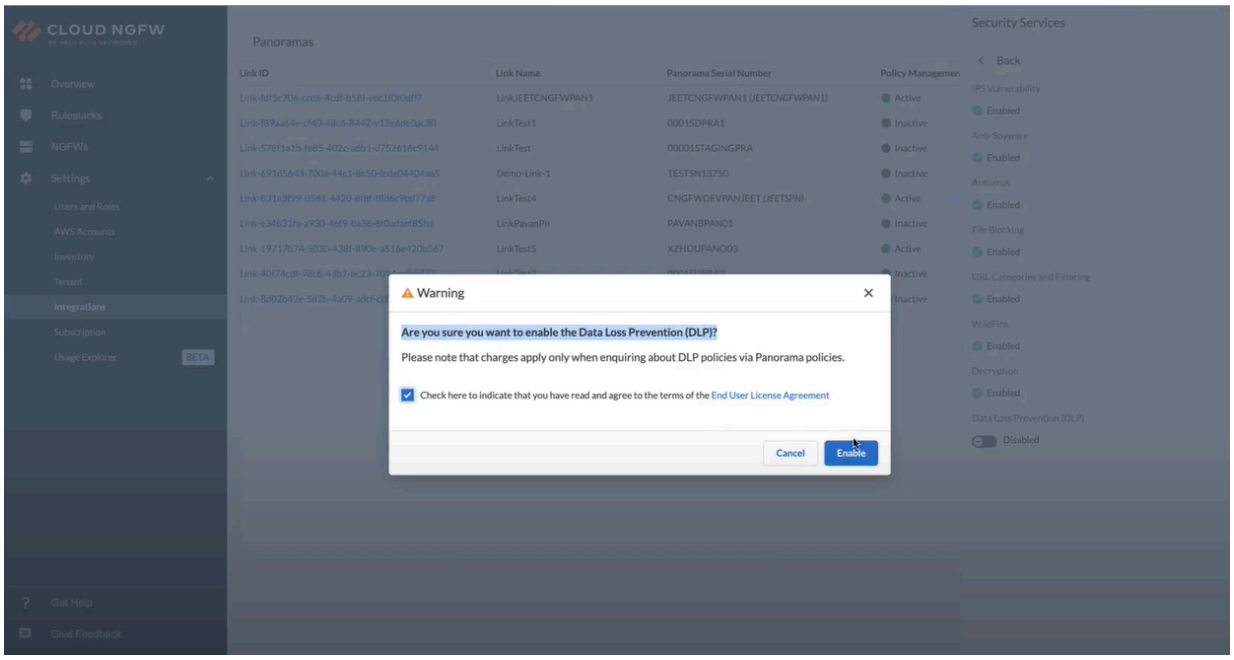


Sie können auch auf die **Verknüpfungs-ID** einer verknüpften Panorama-Instanz und anschließend auf **Check Details (Details prüfen)** klicken.

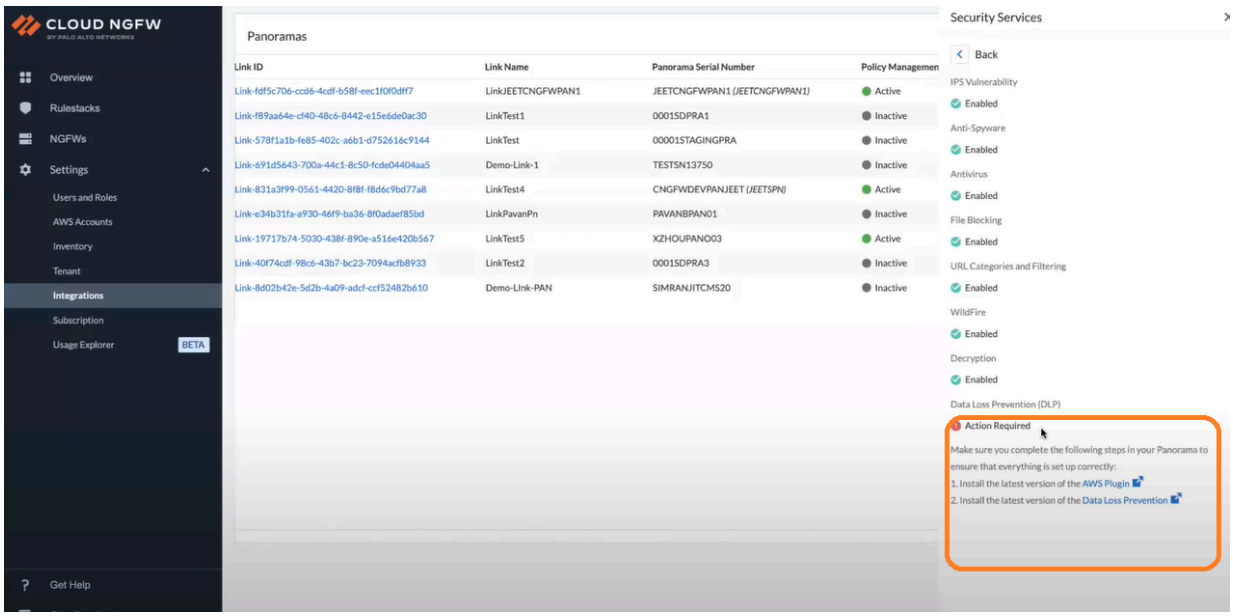
4. Klicken Sie im Fenster **Security Services (Sicherheitsdienste)** auf den Umschalter **Data Loss Prevention (DLP)**.



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



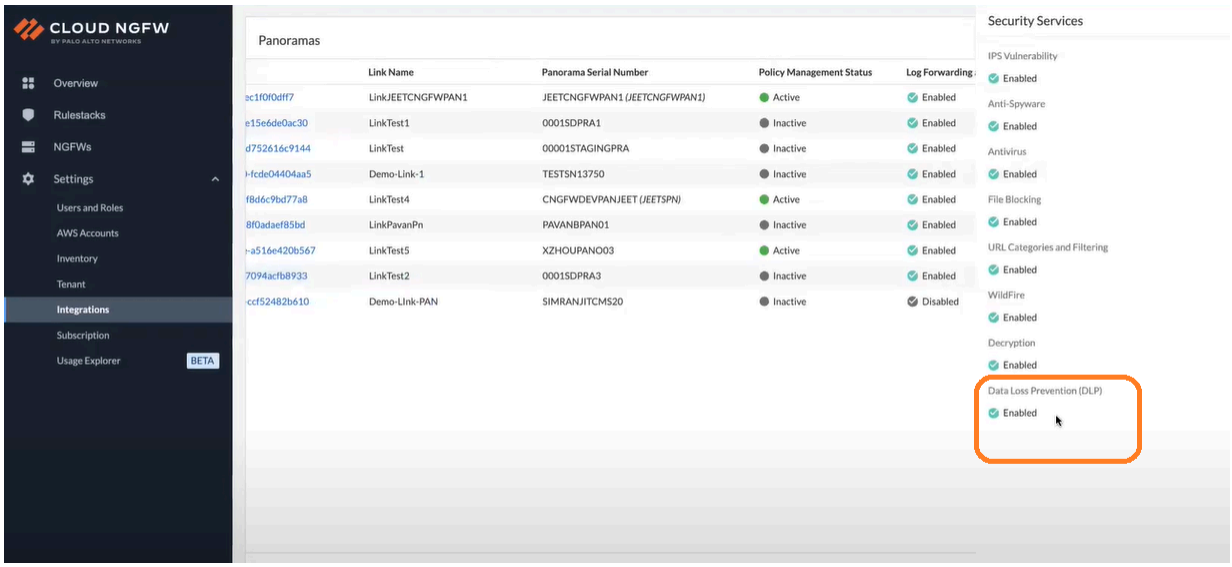
Überprüfen Sie die **erforderliche Maßnahme** in der verknüpften Panorama-Instanz.



6. Stellen Sie sicher, dass die verknüpfte Panorama-Instanz die 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.

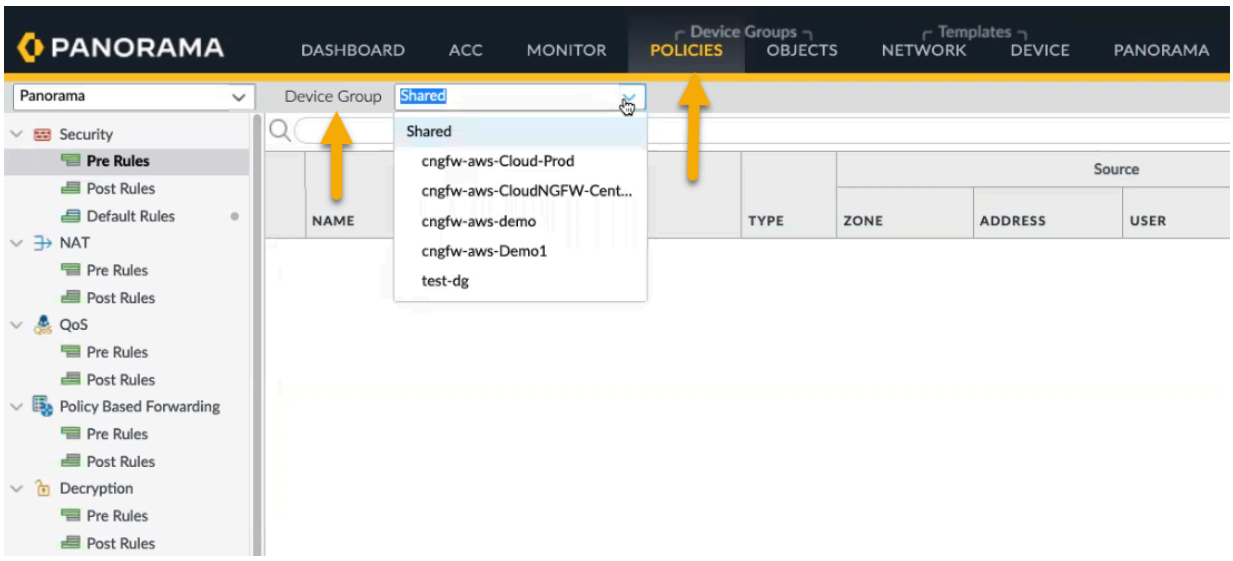
   Wechseln Sie in der Cloud NGFW-Konsole auf die Seite **Integrations (Integrationen)**, wählen Sie die verknüpfte Panorama-Instanz aus und klicken Sie dann in der Spalte **Security Services (Sicherheitsdienste)** auf **Check Details (Details prüfen)**.



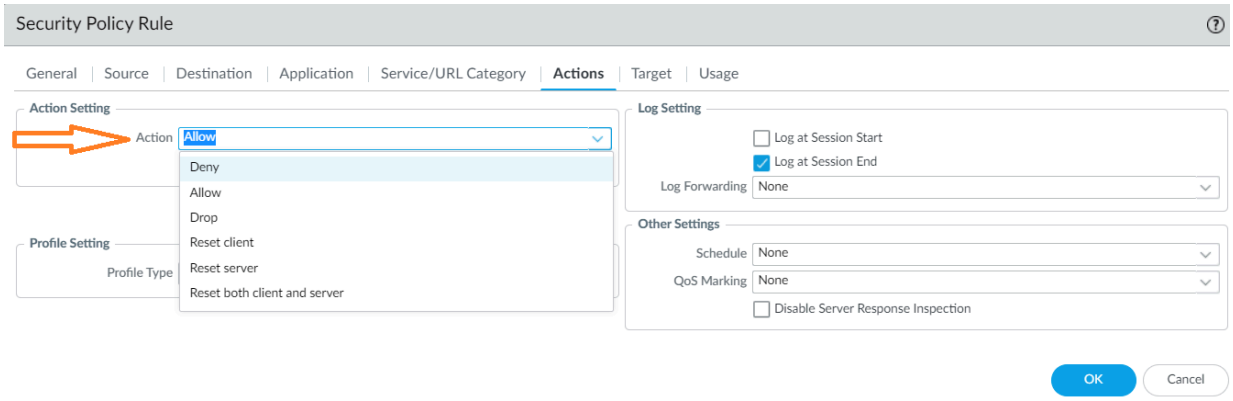
   Jetzt sehen Sie, dass **Data Loss Prevention (DLP)** aktiviert wurde.

   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.

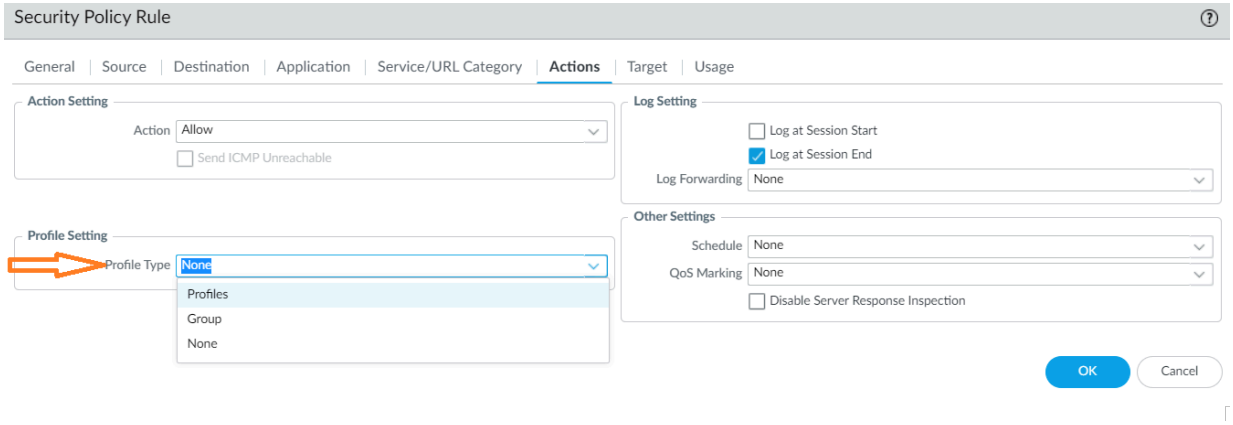
   Sie können ein DLP-Filterprofil zu Ihrer **Sicherheitsrichtlinienregel** für Ihre Firewall in Panorama hinzufügen.



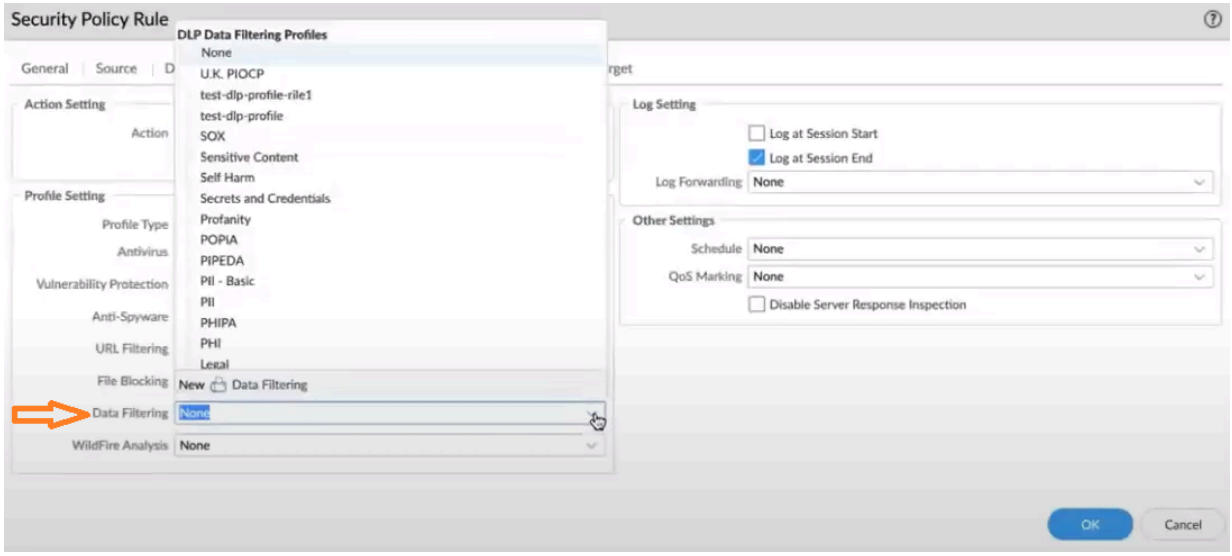
Wechseln Sie im Bildschirm **Security Policy Rule (Sicherheitsrichtlinienregel)** zur Registerkarte **Actions (Aktionen)** und wählen Sie anschließend die auszuführende Aktion aus, z. B. „allow“ (Zulassen) oder „deny“ (Verweigern).



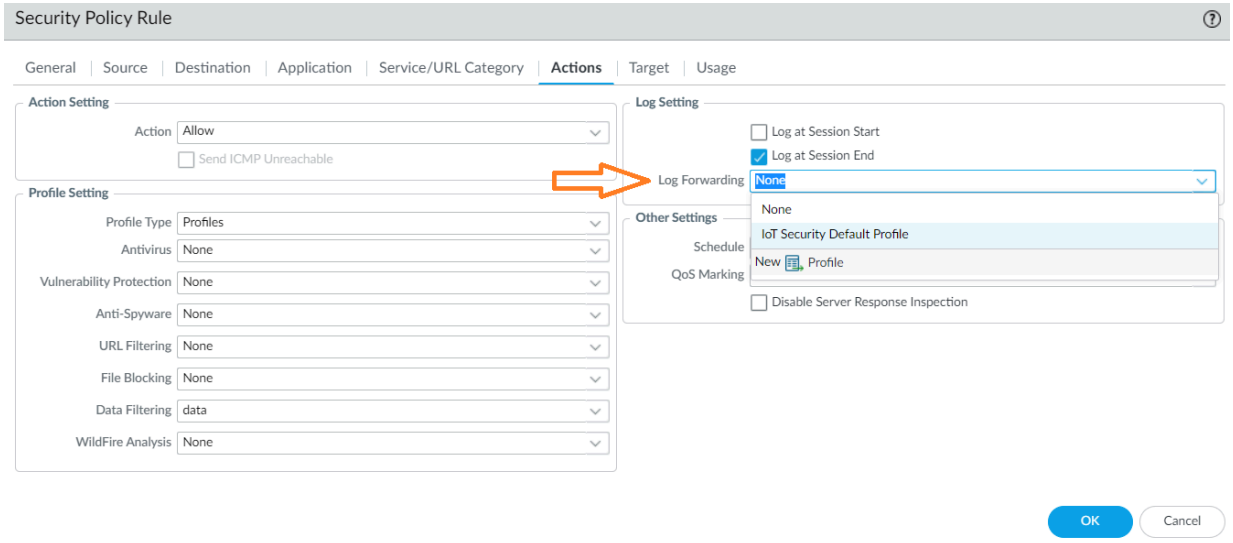
Legen Sie die **Profileinstellung** fest.



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

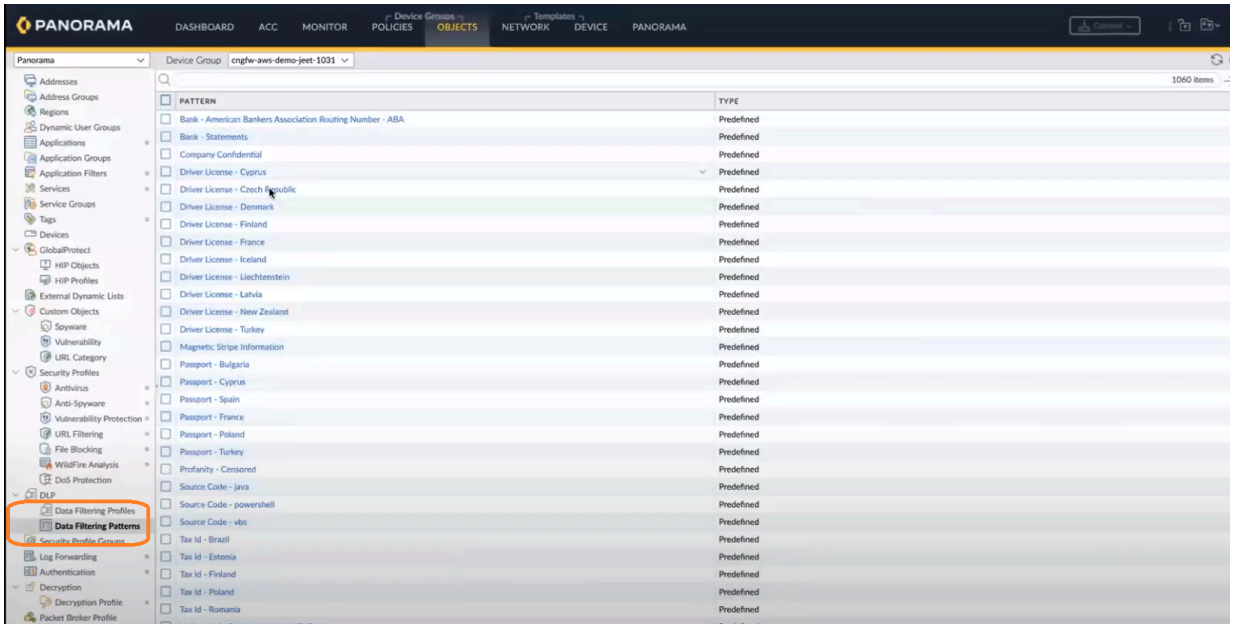


Konfigurieren Sie die **Protokolleinstellung** und andere Einstellungen.



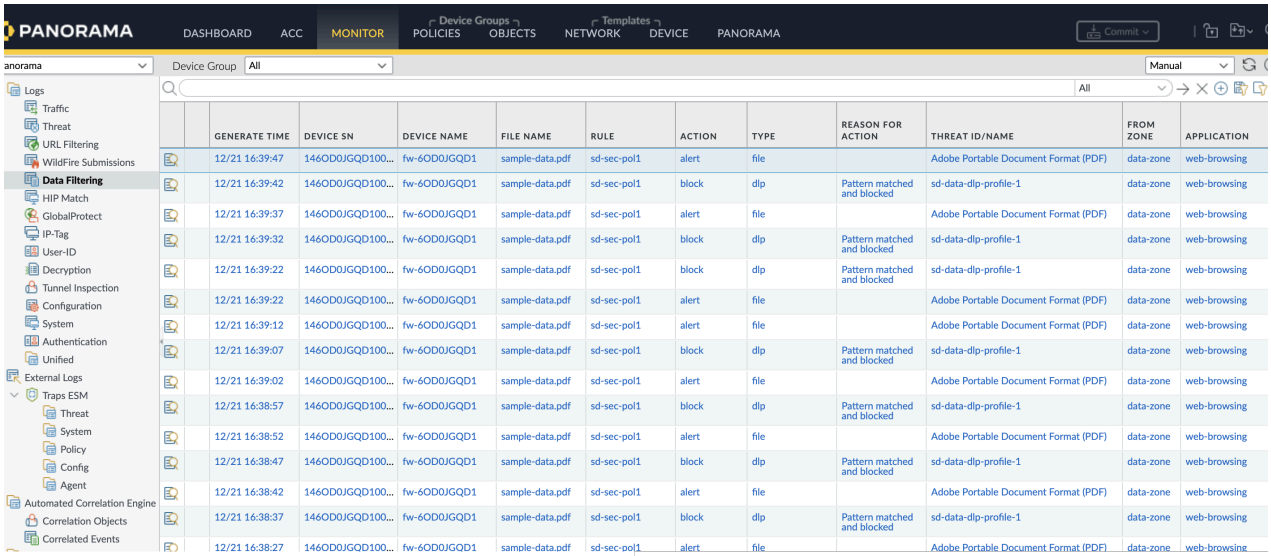
Weitere Informationen finden Sie unter Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden.

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.

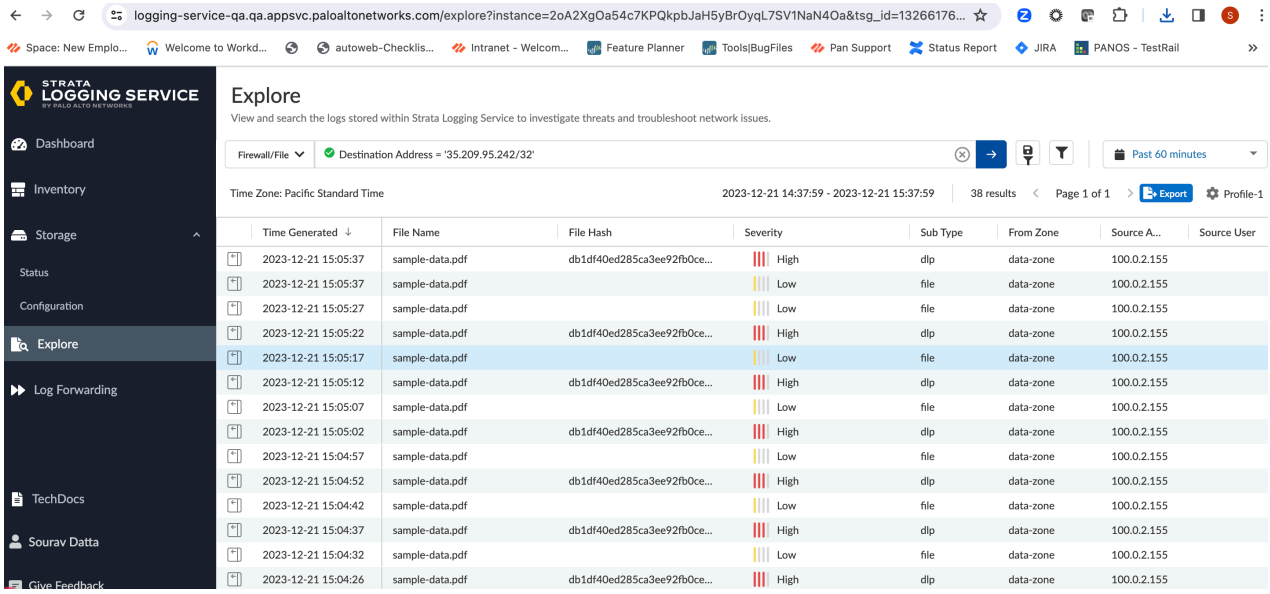


DLP-Protokolldetails überwachen

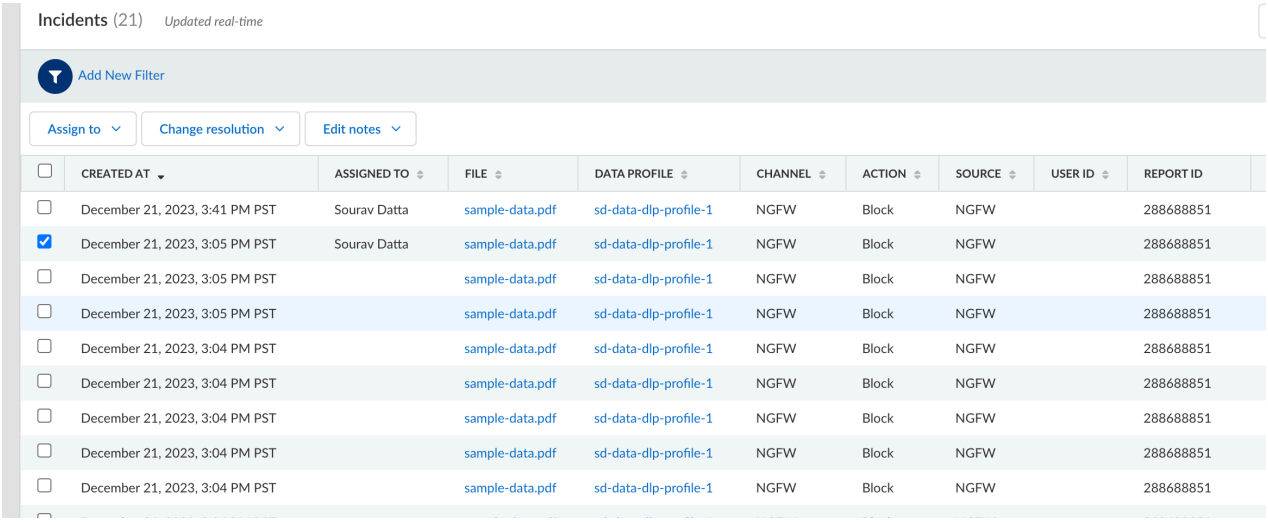
Um Ihre DLP-Protokolle in Panorama anzuzeigen, klicken Sie auf die Registerkarte **Monitor (Überwachen)** und wechseln Sie anschließend zu **Logs (Protokolle)** > **Data Filtering (Datenfilterung)**. Weitere Informationen finden Sie unter Enterprise DLP-Protokolldetails in Panorama anzeigen.



Zum Anzeigen Ihrer CDL-Protokolle 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 Protokolldetails anzeigen in CDL.



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.

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 Benutzeroberfläche 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.

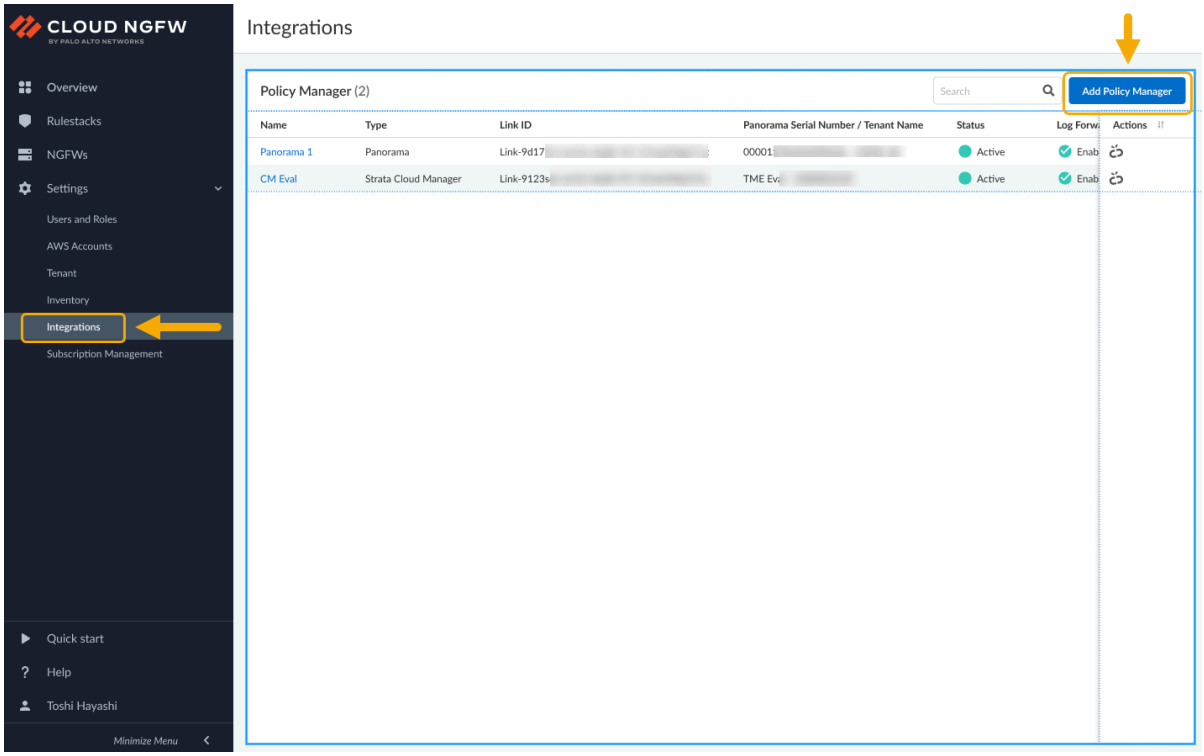
Ihre Cloud NGFW-Ressource mit Strata Cloud Manager für die Richtlinienverwaltung verknüpfen

So integrieren Sie Ihre Cloud NGFW-Ressource in Strata Cloud Manager für die Richtlinienverwaltung:

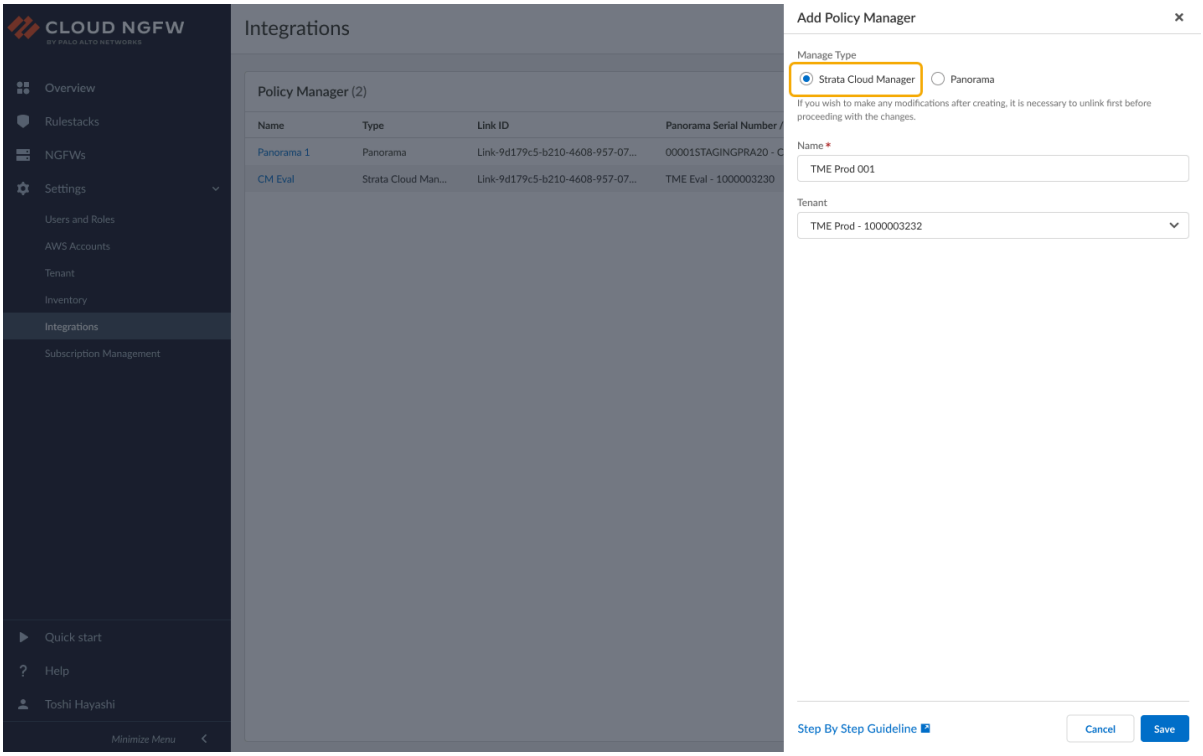
STEP 1 | Melden Sie sich bei der Cloud NGFW-Konsole an.

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.



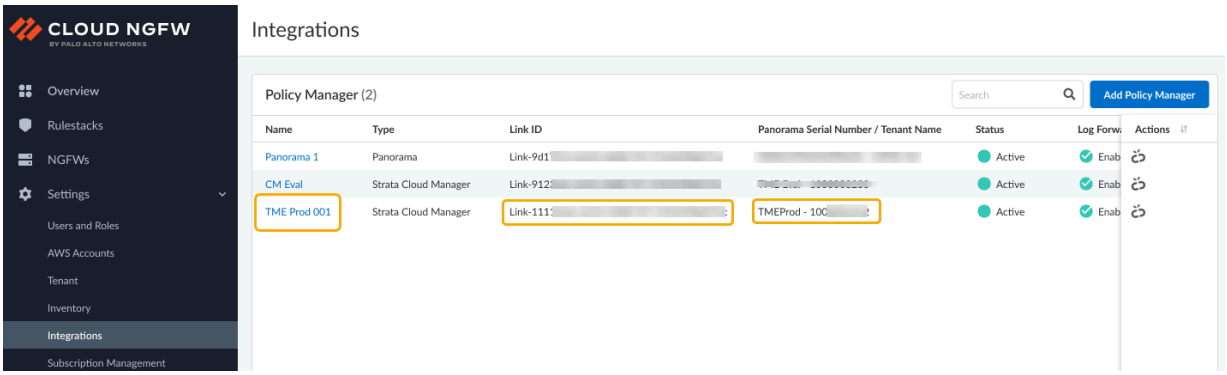
STEP 5 | Geben Sie einen beschreibenden Namen ein.

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.*

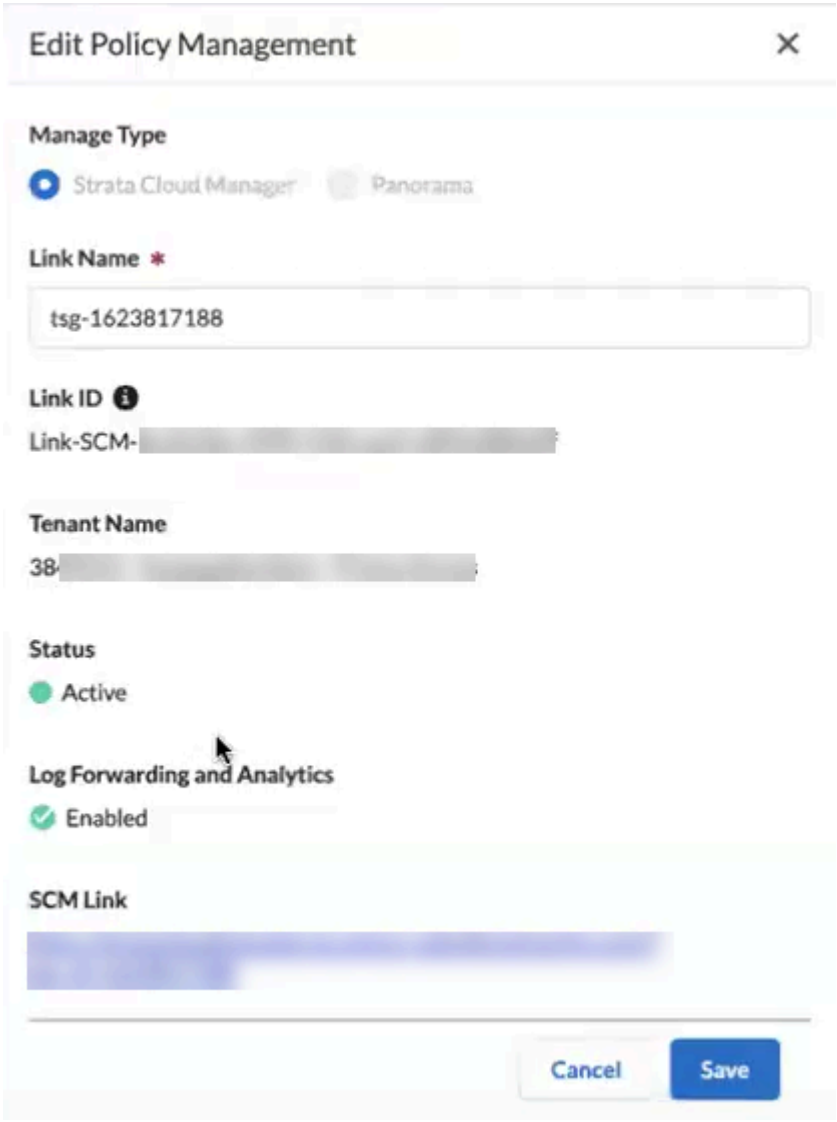
STEP 7 | Klicken Sie auf **Save (Speichern)**. Dadurch wird Ihre Cloud NGFW-Ressource effektiv mit dem SCM-Mandanten verknüpft.

Nach dem Speichern der Konfiguration wird die Seite **Integrations (Integrationen)** aktualisiert, um das neue Richtlinienverwaltungsparadigma zusammen mit der zugeordneten Verknüpfungs-ID und der SCM-Seriennummer/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:



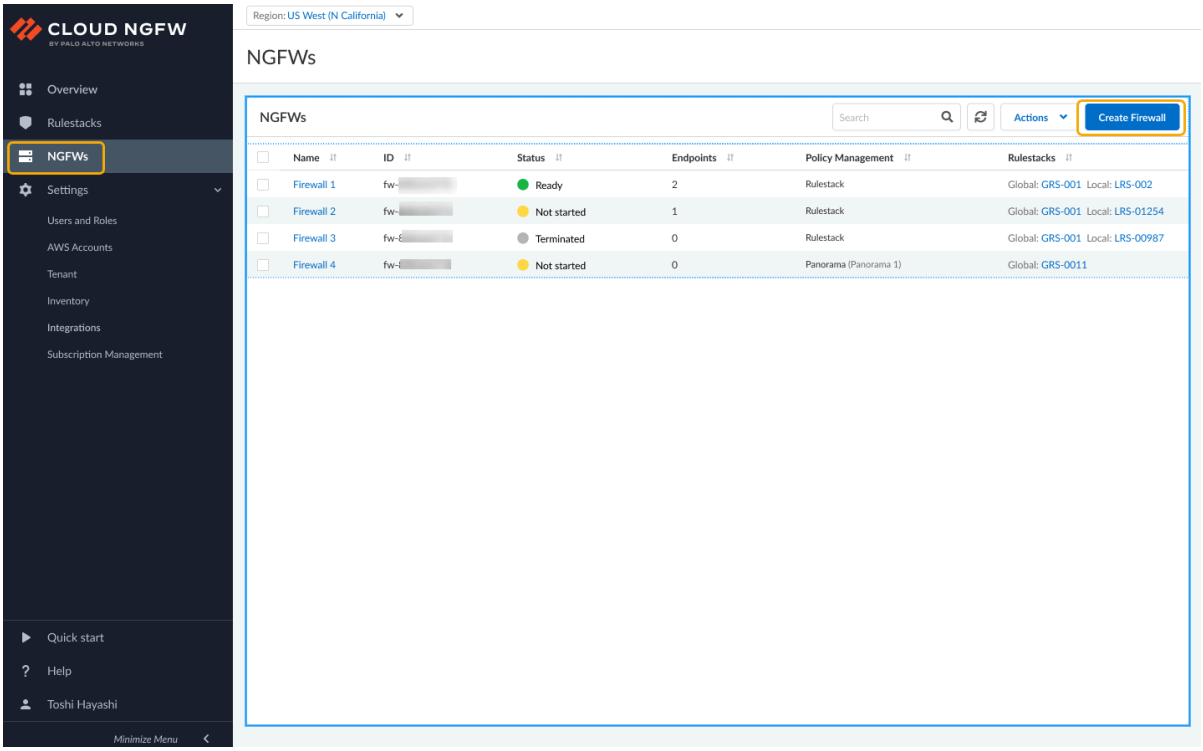
Firewall zur Richtlinienverwaltung des Strata Cloud Managers zuordnen

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.

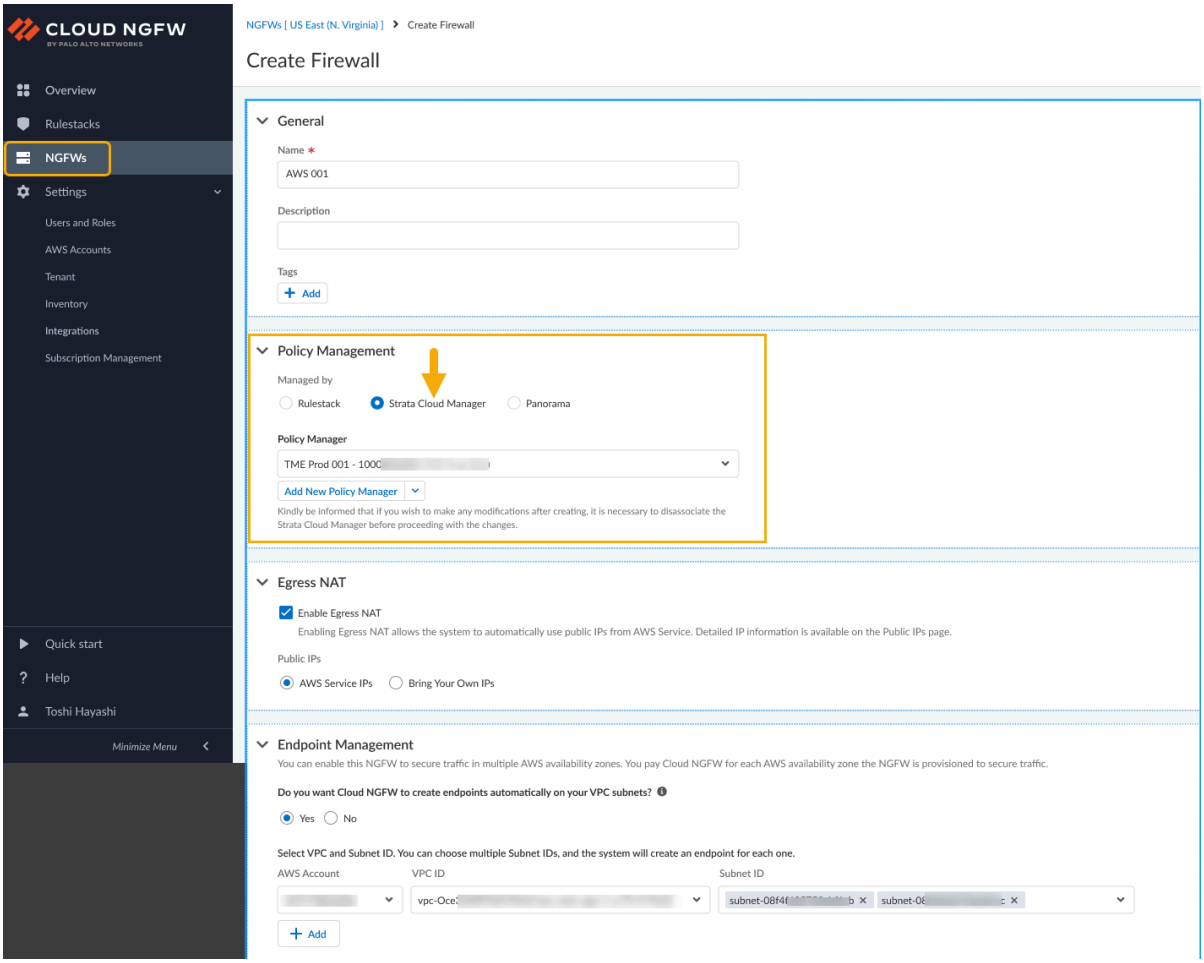
STEP 3 | Klicken Sie auf **Create Firewall (Firewall erstellen)**.



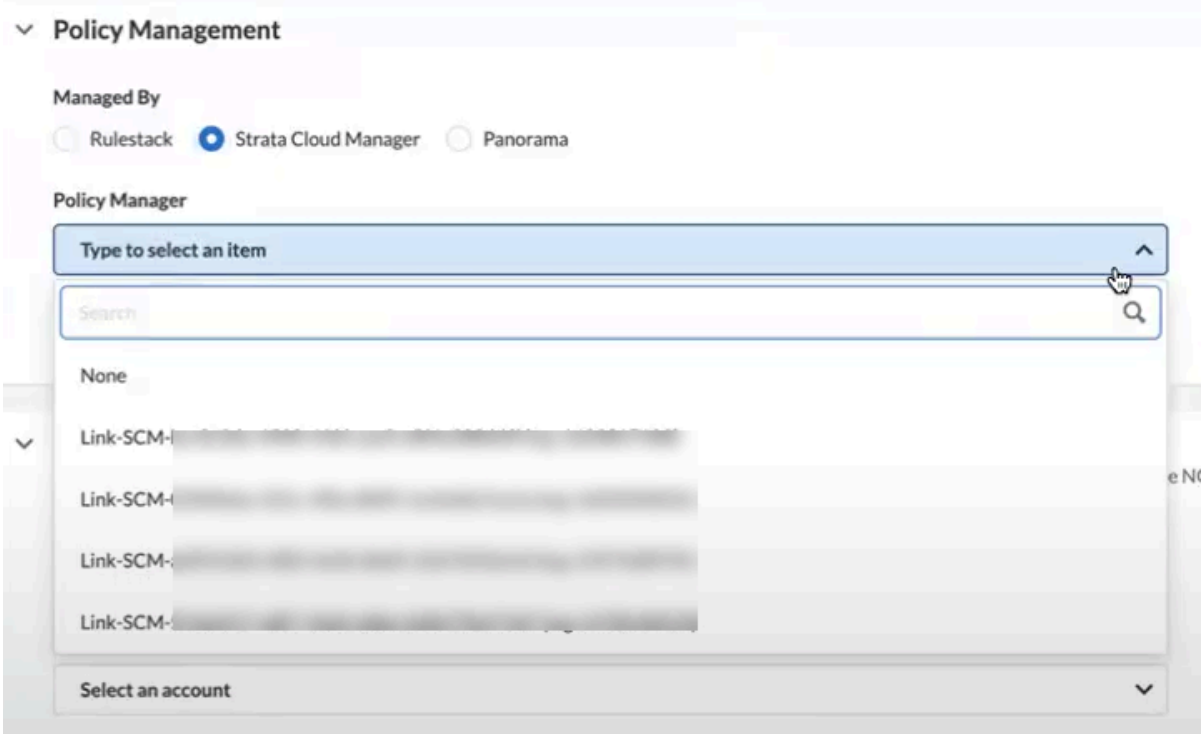
STEP 4 | Geben Sie im Bildschirm **Create Firewall (Firewall erstellen)** einen Namen für die Firewall ein.

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.



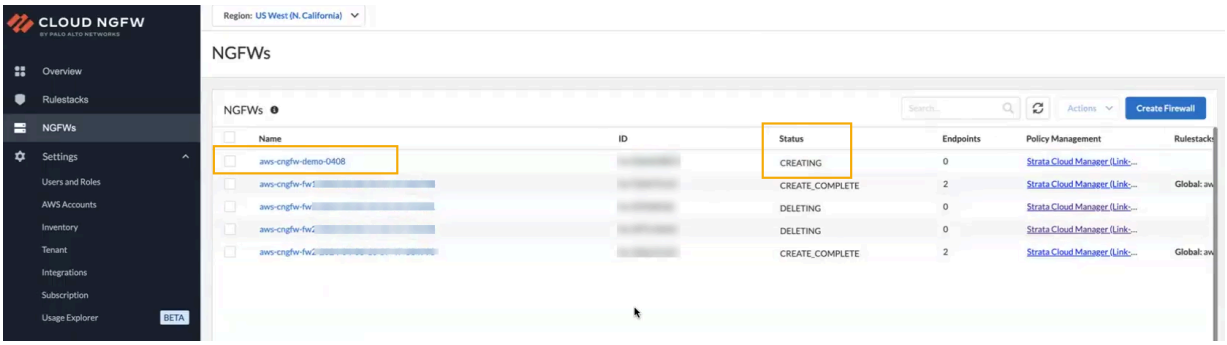
STEP 8 | Konfigurieren Sie **Endpunktverwaltung**, um den Datenverkehr in mehreren AWS-Verfügbarkeitszonen abzusichern.

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*.

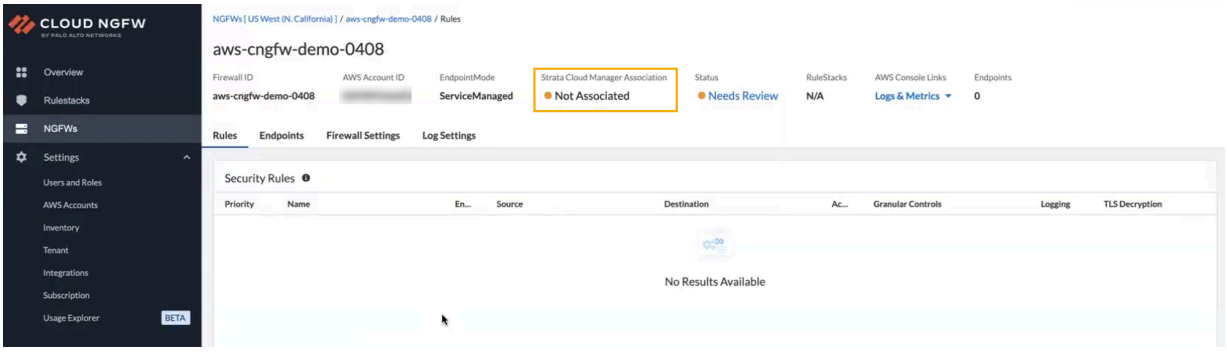
   *Standardmäßig erstellt die Cloud NGFW-Ressource diese Endpunkte nicht automatisch; das Optionsfeld ist auf **No (Nein)** gesetzt.*

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. Beachten Sie, dass beim Erstellen der Firewall nur begrenzte Informationen angezeigt werden:



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.

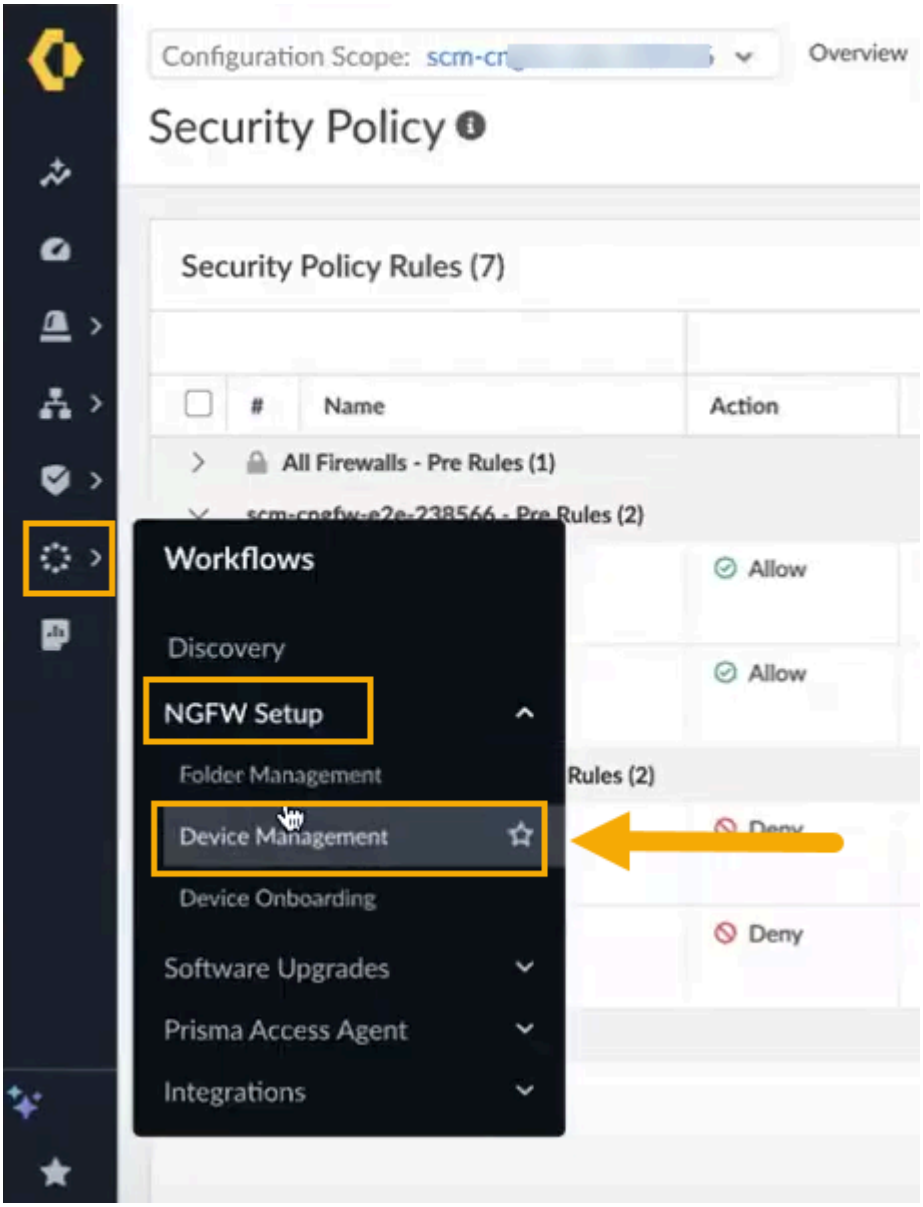
*Wenn Sie sich bei Strata Cloud Manager anmelden, zeigt das Dashboard die Anzahl der Cloud NGFWs unter **NGFW** > **Software** nicht an.*

STEP 1 | Melden Sie sich über den Palo Alto Networks Hub direkt bei der Strata Cloud Manager-App unter stratacloudmanager.paloaltonetworks.com an.

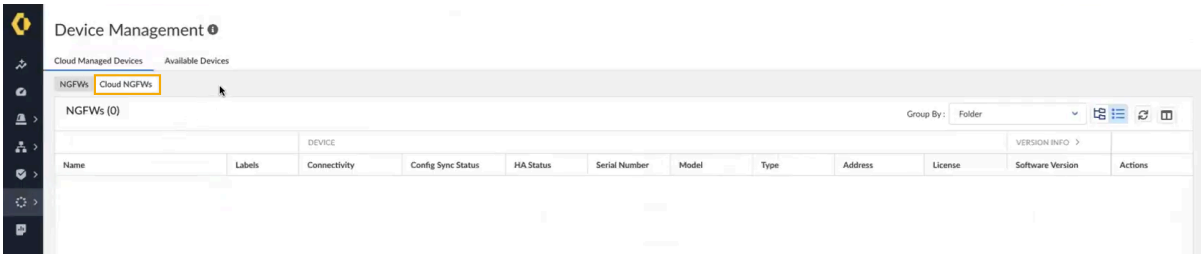
STEP 2 | Suchen Sie in der Strata Cloud Manager-Oberfläche Ihren Cloud NGFW-Mandanten mithilfe der linken Navigationsoption:

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.

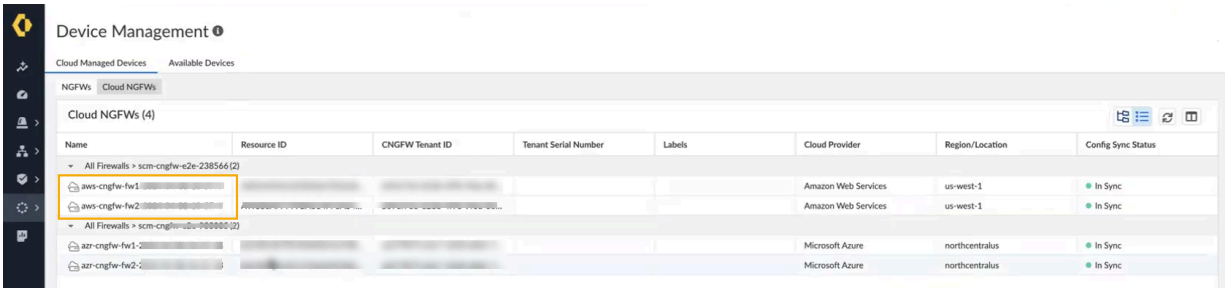
STEP 3 | Wählen Sie **Workflows > NGFW Setup > Device Management (Workflows > NGFW-Setup > Geräteverwaltung)** aus:



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:



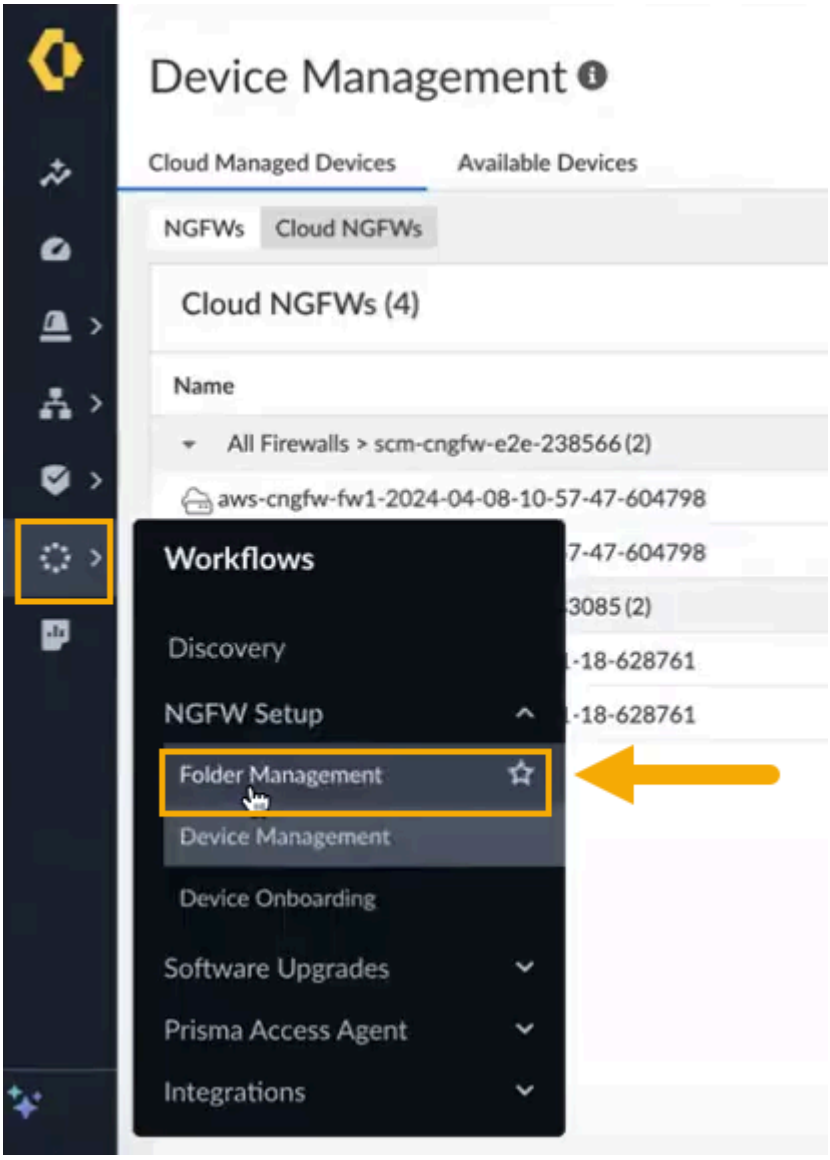
Im Bildschirm **Device Management (Geräteverwaltung)** werden die Cloud NGFW-Ressourcen angezeigt, die derzeit von SCM verwaltet werden:



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/Location (Region/Standort). Die Region, in der sich die Cloud NGFW-Ressource befindet.
- Config Sync Status (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:



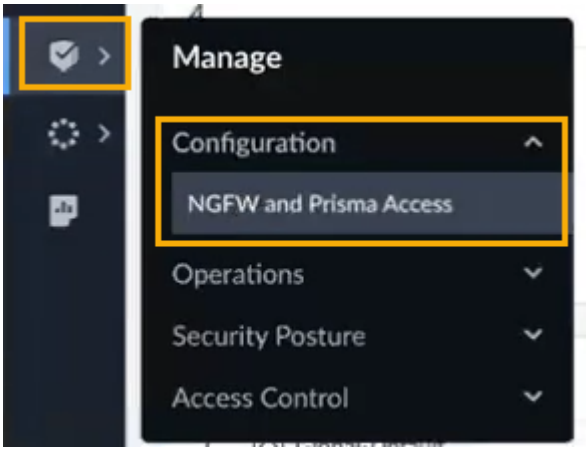
Im Bildschirm **Folder Management (Ordnerverwaltung)** werden die Cloud NGFW-Ressourcen angezeigt, die dem SCM-Mandanten zugeordnet sind:

Informationen zum Erstellen von Ordnern finden Sie unter Ordner für Ihre Cloud NGFW-Ressource mithilfe von Strata Cloud Manager erstellen.

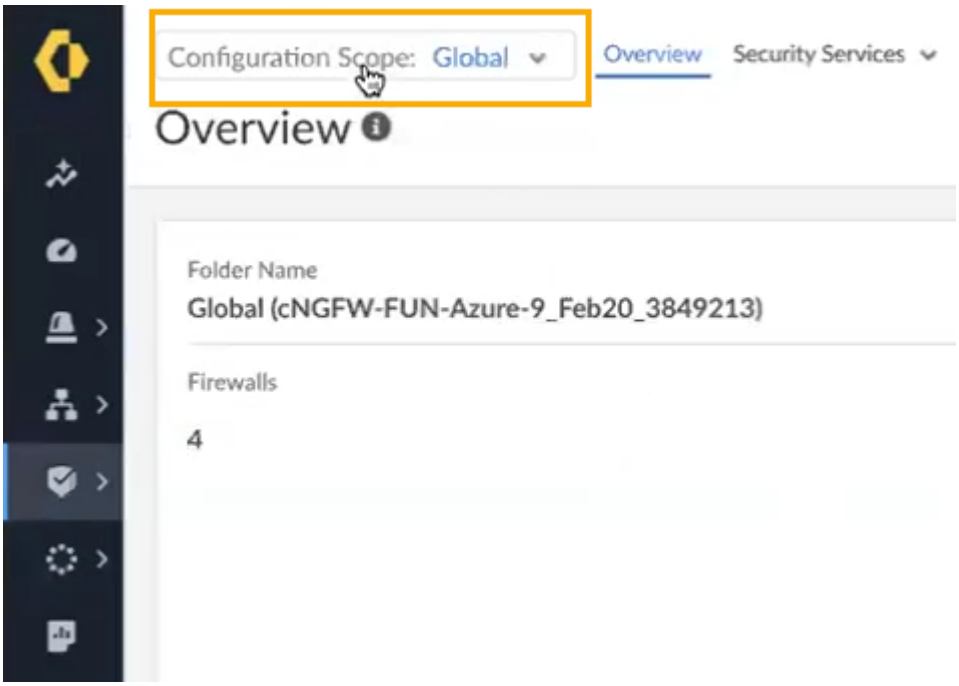
Strata Cloud Manager für die Richtlinienverwaltung in Cloud NGFW verwenden

Sie können Strata Cloud Manager verwenden, um Sicherheitsrichtlinien global auf die Cloud NGFW-Ressourcen anzuwenden, die in einem Ordner enthalten sind.

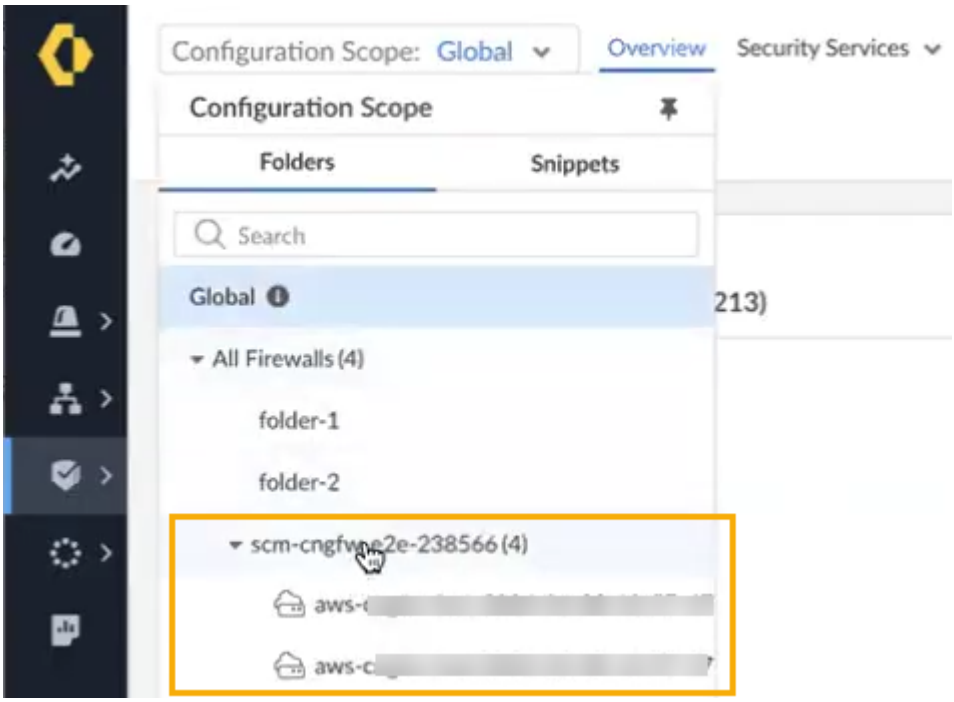
STEP 1 | Wählen Sie in Strata Cloud Manager die Optionen **Manage > Configuration > NGFW and Prisma Access (Verwalten > Konfiguration > NGFW und Prisma Access)** aus.



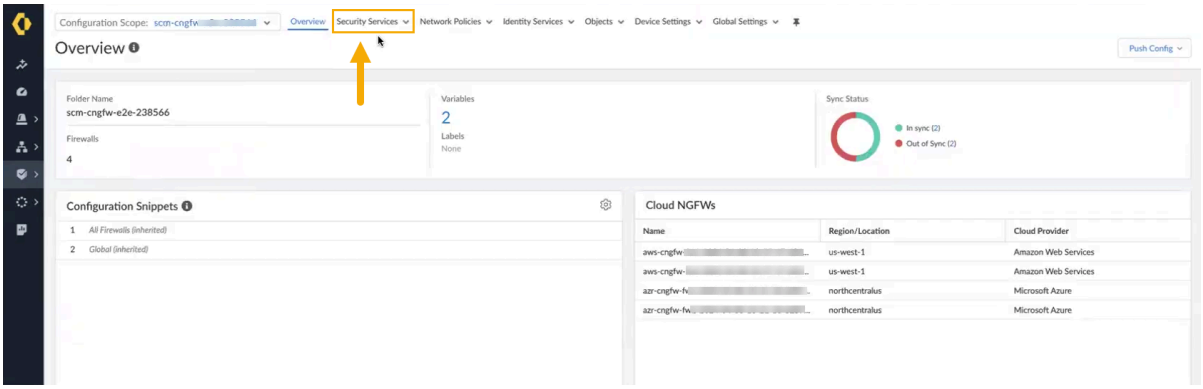
STEP 2 | Wählen Sie **Configuration Scope (Konfigurationsumfang)** aus.



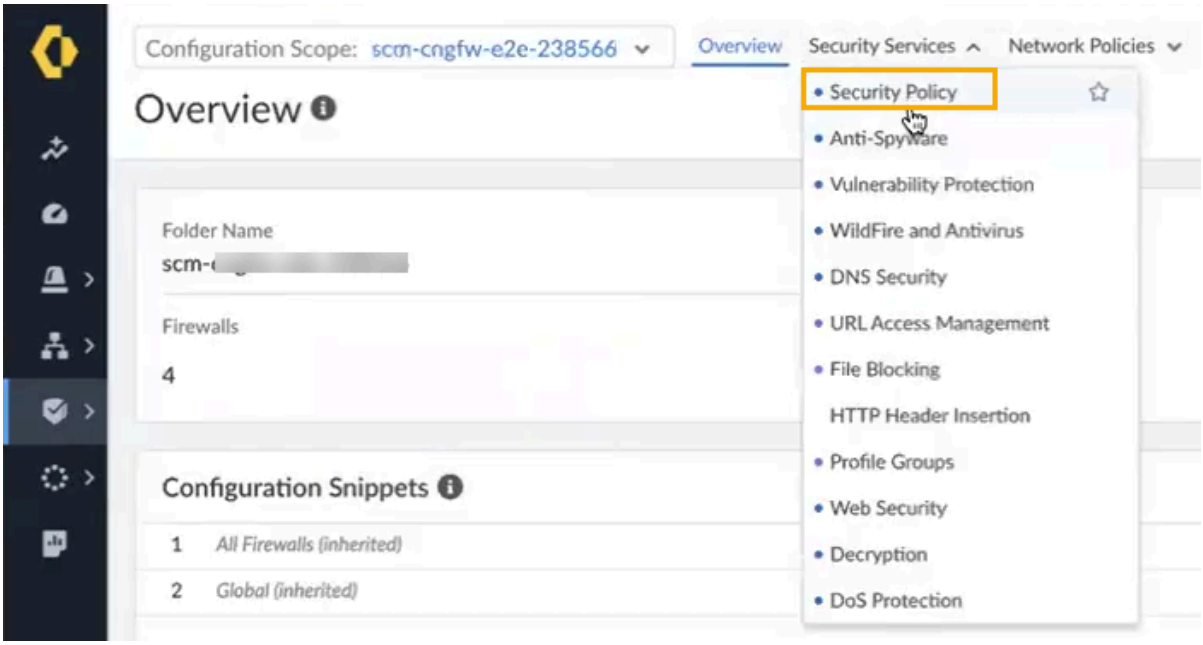
STEP 3 | Suchen Sie in der Dropdown-Liste den Ordner, der die **Cloud NGFW AWS-Ressourcen** enthält:



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

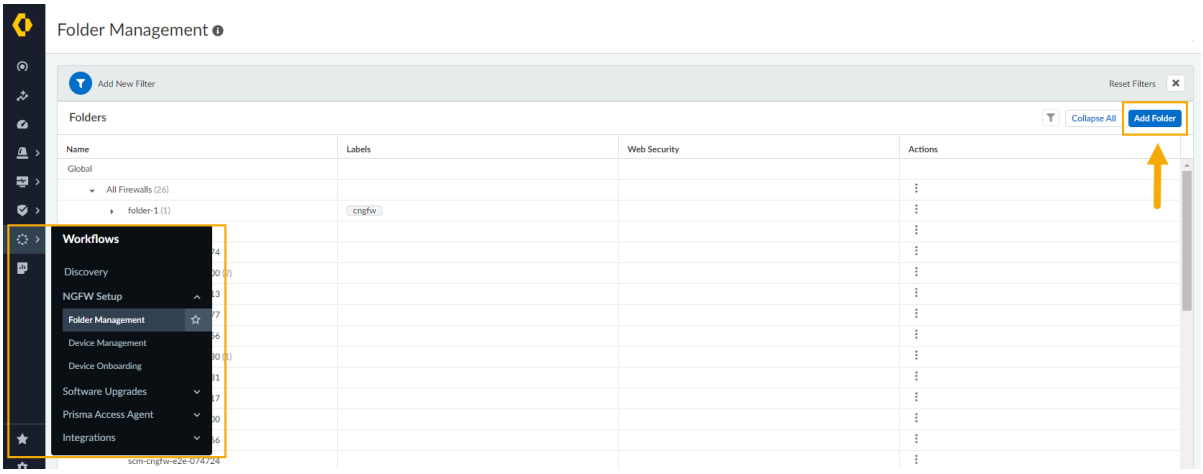
Nachdem Sie das entsprechende Abonnement für die Nutzung des Strata Cloud Manager-Dienstes für Ihre Cloud NGFW-Ressource konfiguriert haben, erstellen Sie einen Ordner, in dem Sie die Ihrer Firewall zugeordneten Daten anzeigen können. Ordner werden verwendet, um Ihre Firewalls oder Bereitstellungstypen (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:

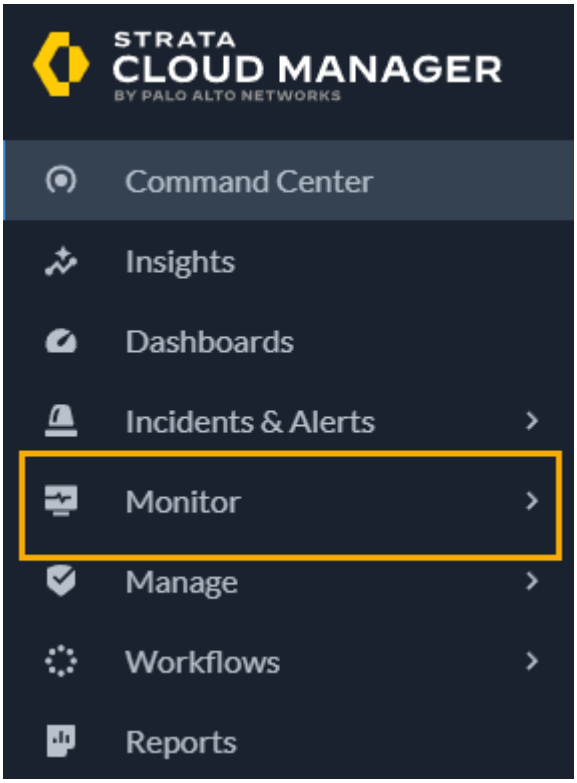
- Produkte und Abonnements, die Sie mit Strata Cloud Manager verwalten.
- Den Zustand und den Konnektivitätsstatus Ihrer Cloud NGFW-Geräte.

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:



Versionsaktualisierungen in Cloud NGFW für AWS

Hier erfahren Sie mehr über die neuesten Funktionen von Cloud NGFW für AWS sowie die bekannten Probleme, an denen das Team arbeitet, um Ihre Erfahrung zu verbessern:

Neuigkeiten

Das ist neu in Cloud NGFW for AWS.

Was ist neu im Juni 2024

Einbindung im Customer Support Portal	Diese Version von Cloud NGFW für AWS verbessert das Einbindungserlebnis durch die Integration der Registrierung Ihres Cloud NGFW-Mandanten beim Customer Support Portal von Palo Alto Networks. Weitere Informationen finden Sie unter Ihren Cloud NGFW-Mandanten bei einem Palo Alto Networks Supportkonto registrieren.

Automatisierte Einbindung von Konten	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. Weitere Informationen finden Sie unter Automatisierte Einbindung von Konten konfigurieren.

Was ist neu im Mai 2024

Richtlinienverwaltung in Cloud NGFW mit Strata Cloud Manager	Sie können Ihre Cloud NGFW-Ressource jetzt 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 Benutzeroberfläche 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. Mit dieser ersten Version können Sie Ressourcen mithilfe der Cloud NGFW-Konsole erstellen und diese Ressourcen anschließend beim Strata Cloud Manager für eine zentrale Richtlinienverwaltung registrieren. Sie werden Strata Cloud Manager zur Überwachung und Fehlerbehebung verwenden. Weitere Informationen finden Sie unter „Ihre Cloud NGFW-Ressource mit Strata Cloud Manager verknüpfen“. Weitere Informationen finden Sie unter Strata Cloud Manager für die Richtlinienverwaltung.
Cloud NGFW-Metriken	Mithilfe der Cloud NGFW-Metriken verfügen Sie jetzt über eine verbesserte Betriebstransparenz Ihrer Cloud NGFW-Ressourcen. Cloud NGFW veröffentlicht jetzt Metriken in AWS CloudWatch, damit Sie den Zustand, die Leistung und die Nutzungsmuster Ihrer Cloud NGFW überwachen können. Mit diesen zusätzlichen Metriken können Sie den Gesamtzustand Ihrer Cloud NGFW-Ressourcen bewerten, Leistungsengpässe identifizieren und Anomalien erkennen. Weitere Informationen finden Sie unter Datenverkehrsprotokollfelder in Cloud NGFW für AWS.
Zonen-ID anzeigen	Cloud NGFW für AWS verbessert die Multi-VPC-Funktionalität, da Sie jetzt beim Erstellen der Firewall-Ressourcen Verfügbarkeitszonennamen angeben können. AWS ordnet die ID der physischen Verfügbarkeitszonen *nach dem Zufallsprinzip* den Namen der Verfügbarkeitszonen für jedes AWS-Konto zu. Zuvor mussten Sie den Namen der Verfügbarkeitszone für eine bestimmte Verfügbarkeitszonen-ID in Ihrem/Ihren AWS-Konto(s) in der Cloud NGFW-Konsole manuell ermitteln und diese Informationen dann zum Erstellen von Cloud NGFW-Ressourcen verwenden. Mit dieser

	Erweiterung können Sie in Cloud NGFW beim Erstellen einer neuen Firewall-Ressource entweder die ID oder den Namen der Verfügbarkeitszone angeben. Weitere Informationen finden Sie unter NGFW-Ressource in AWS erstellen.
Abonnementverbesserungen	Cloud NGFW für AWS verbessert die auf der Seite **Subscription (Abonnement)** angezeigten Informationen durch die zusätzliche Anzeige des Status Ihres Credit-Abonnements. Auf dieser Seite wird jetzt angezeigt, ob Ihr Abonnement *abgelaufen*, *aktiv*oder *inaktiv* ist.
Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar: • Asien-Pazifik (Osaka) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.

Was ist neu im März 2024

Fortschrittliche Bedrohungsabwehr	Cloud NGFW für AWS verwendet jetzt Advanced Threat Prevention, um unbekannten Command-and-Control-Datenverkehr und Zero-Day-Injection-Angriffe zu blockieren. Weitere Informationen finden Sie unter Advanced Threat Prevention.
Verbesserungen bei Single-Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA)	Der Zugriff auf die Cloud NGFW-Konsole wurde mit Single-Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) integriert, um Komfort und Sicherheit zu vereinen. Sie können jetzt auch dieselbe E-Mail-Adresse für die Registrierung bei mehreren Cloud NGFW-Mandanten verwenden. Auf der Cloud NGFW-Anmeldeseite können Sie jetzt eines bzw. einen der vielen von Ihnen verwendeten Cloud NGFW-Konten/-Mandanten auswählen. Weitere Informationen finden Sie unter Cloud NGFW für AWS abonnieren und Benutzer zu Cloud NGFW für AWS einladen.
Unterstützung des Schnellstarts von AWS Marketplace SaaS	Cloud NGFW ist jetzt in AWS Marketplace SaaS Quick Launch integriert, um das AWS Marketplace-Abonnement einfach, schnell und sicher zu machen, indem Schritt-für-Schritt-Anleitungen mithilfe einer vorkonfigurierten AWS CloudFormation-Vorlage angeboten werden. Weitere Informationen finden Sie unter Cloud NGFW für AWS abonnieren.
Verbesserungen der AWS CloudFormation-Registry	Die CloudFormation-Registry von Cloud NGFW wurde jetzt mit den neuesten Funktionen in Firewall- und Regelstapelressourcen sowie integriertem Abruf programmgesteuerter Zugriffstoken aktualisiert. Weitere Informationen finden Sie unter Cloud NGFW-Ressourcen für Ihre AWS CFT bereitstellen.

Enterprise Data Loss Prevention	Mit Enterprise Data Loss Prevention (E-DLP) können Sie vertrauliche Informationen vor unbefugtem Zugriff, Missbrauch, Extraktion oder Weitergabe schützen. Sie können E-DLP jetzt in Cloud NGFW für AWS integrieren und die Panorama-Schnittstelle verwenden, um Ihren Sicherheitsrichtlinienregeln Datenfilterungsprofile hinzuzufügen. Weitere Informationen finden Sie unter E-DLP-Integration mit CNGFW für AWS.
Tagbasierte Richtlinien – Verbesserungen	Sie können Ihren Cloud-Gerätegruppen jetzt IP-Tags aus zwei verschiedenen Regionen hinzufügen. Sammeln Sie Ihre Tags aus einer AWS-Region und setzen Sie dann Sicherheitsrichtlinien für Ihre Firewall in der anderen Region durch. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.
Metriken zur Nutzung von Cloud NGFW-Regeln	Sie können jetzt die Panorama-Konsole verwenden, um die Regelnutzung für Betriebs- und Fehlerbehebungsaufgaben zu verfolgen und zu überwachen, einschließlich der Anzahl der Regeltreffer und der auf den Cloud NGFW-Ressourcen angezeigten Anwendungen. Weitere Informationen finden Sie unter Regelnutzung in Cloud NGFW für AWS. *Um diese Funktion zu nutzen, müssen Sie ein Upgrade auf Version 5.2.0 des AWS-Plug-ins durchführen.*
Cloud NGFW-Integration mit AWS Cloud WAN	Mit AWS Cloud WAN können Sie jetzt ein einheitliches Netzwerk aufbauen, das Cloud- und lokale Umgebungen verbindet und Ihnen die Weiterleitung des Datenverkehrs zwischen folgenden Bereichen ermöglicht: • VPCs im selben Segment in derselben Region (isolierte Anhänge) • VPCs in verschiedenen Segmenten in derselben Region • VPCs im selben Segment über verschiedene Regionen hinweg (isolierte Anhänge) • VPCs in verschiedenen Segmenten über verschiedene Regionen hinweg Weitere Informationen finden Sie unter Cloud NGFW-Integration mit AWS Cloud WAN.

Was ist neu im Dezember 2023

Blogs, Artikel usw. zu Cloud NGFW für AWS.	Richtlinien für den Preisschätzer für Cloud NGFW für AWS

Was ist neu im November 2023

Videos zu Cloud NGFW für AWS	AWS Reinvent 2023 – Wie Unternehmen Anwendungen mit AWS und Palo Alto Networks absichern (HYB205) Network Security Bytes – Cloud NGFW für AWS

Was ist neu im Oktober 2023

Blogs, Artikel usw. zu Cloud NGFW für AWS.	Cloud NGFW für AWS-Bereitstellungsarchitekturen

Was ist neu im September 2023

Blogs, Artikel usw. zu Cloud NGFW für AWS.	Cloud NGFW für AWS lässt sich in Panorama integrieren Cloud NGFW für AWS – Handbuch zur Ausfallsicherheit

Was ist neu im August 2023

Mehrere Panorama-Instanzen für Cloud NGFW-Mandanten	Sie können jetzt mehrere Panorama-Appliances zusammen mit ihrer Strata-Protokollierungsdienst-Instanz mit Ihrem Cloud NGFW-Mandanten verknüpfen. Anschließend können Sie die NGFW-Ressource eines Mandanten einer dieser Verknüpfungen für die Richtlinien- und Protokollverwaltung zuordnen. Weitere Informationen finden Sie unter Mehrere Panorama-Instanzen mit Ihrem Cloud NGFW-Mandanten verwenden.
Cloud NGFW für AWS ist jetzt mit Premium-Support erhältlich	Premium-Support ist jetzt ohne zusätzliche Kosten in Cloud NGFW für AWS enthalten. Der Premium-Support von Palo Alto Networks erweitert Ihre internen Ressourcen durch technische Experten, die Ihnen zur Unterstützung Ihrer Sicherheitsinfrastruktur von Palo Alto Networks zur Verfügung stehen. Diese Supportebene bietet Zugriff auf Security Assurance, damit Sie bei Sicherheitsvorfällen Sicherheitsexperten hinzuziehen können. Weitere Informationen finden Sie unter Premium-Support.
Dynamische Dimensionierung des Strata-Protokollierungsdienstes für Cloud NGFW für AWS	Sie können jetzt den Strata-Protokollierungsdienst verwenden, um Abfragen zur Erkundung bzw. für den Protokoll-Viewer durchzuführen und Protokolle anzuzeigen, die von einer bestimmten Cloud NGFW für AWS-Ressource generiert wurden. Der Strata-Protokollierungsdienst zeigt außerdem wichtige Metriken für Ihre Cloud NGFWs auf einer speziellen **Cloud NGFW-Inventarseite für den Strata-Protokollierungsdienst** an, um die Erfassungsrate,

	Speichernutzung und den Verbindungsstatus besser überwachen zu können. Bei Verwendung mit Cloud NGFW für AWS wird der Strata-Protokollierungsdienst jetzt automatisch zusammen mit den Cloud NGFW für AWS-Ressourcen skaliert. Mit zunehmendem Datenverkehrsdurchsatz auf diesen Cloud NGFW-Ressourcen steigt auch Ihr verfügbarer Speicher für den Strata-Protokollierungsdienst, sodass Sie sich keine Gedanken über manuelle Anpassungen machen müssen, um Ihre Protokolldaten speichern zu können.
Usage Explorer (Vorschau)	Diese Version wurde um den Usage Explorer in der Cloud NGFW-Konsole für AWS ergänzt. Über das Usage Explorer-Dashboard können Sie den Cloud NGFW-Verbrauch und dessen Korrelation mit Credits anzeigen, die dem Mandanten zugeordnet sind. Weitere Informationen finden Sie unter Cloud NGFW für AWS Usage Explorer.
Preis- und Abrechnungsänderungen	Cloud NGFW für AWS ändert das Preismodell, um mehr Flexibilität für die aggregierte Cloud NGFW-Mandantennutzung zu bieten. Dieses basiert auf den Bereitstellungsstunden aller NGFWs, der von ihnen abgesicherten Datenverkehrsmenge und der Anzahl der von ihnen pro Stunde verwendeten Sicherheitsfunktionen. Weitere Informationen finden Sie auf der Seite Preise.

Was ist neu im Juli 2023

Cloud NGFW-Protokolle und -Aktivitäten in Panorama filtern	Auf der Registerkarte **Monitor (Überwachen)** in Panorama können Sie jetzt mithilfe von Filtern das Protokoll einer einzelnen Cloud-Gerätegruppe anzeigen oder Protokolle und Aktivitäten für alle Cloud-Gerätegruppen anzeigen. Ausführlichere Informationen finden Sie unter Cloud NGFW-Protokolle und -Aktivitäten anzeigen.
Tagbasierte Richtlinien	Wenn Sie AWS-Assets (wie etwa EC2-Instanzen) in der öffentlichen AWS-Cloud bereitstellen oder beenden, können Sie die Sicherheitsrichtlinie für Ihre Palo Alto Networks Cloud NGFW-Ressourcen automatisch aktualisieren, sodass Sie den Datenverkehr zu diesen AWS-Assets absichern können. Weitere Informationen finden Sie unter Tagbasierte Richtlinien.
WildFire	Cloud NGFW kann Ihren VPC-Datenverkehr jetzt vor dateibasierten Bedrohungen schützen, indem Dateien, ausführbare Dateien und bösartige Skripts (wie JScript und PowerShell) in Ihrem VPC-Datenverkehr erkannt und zur Malware-Analyse an den Cloud-Dienst WildFire™ (WF) weitergeleitet werden.

Was ist neu im Juni 2023

Verknüpfung der Unterstützung für die Panorama-Integration aufheben	Sie können jetzt die Verknüpfung der Panorama-Appliance mit einer Cloud NGFW-Ressource automatisch aufheben, ohne ein Support-Ticket zu öffnen. Weitere Informationen finden Sie unter Verknüpfung von Cloud NGFW mit Palo Alto Networks Management aufheben.
Video zu Cloud NGFW für AWS	So löschen Sie eine Cloud NGFW-Ressource

Was ist neu im Mai 2023

Unterstützung von Panorama	Sie können jetzt einen Cloud NGFW für AWS-Mandanten in eine Palo Alto Networks Appliance integrieren, um einen gemeinsamen Satz von Sicherheitsregeln zentral auf Cloud NGFW-Ressourcen neben Ihren physischen und virtuellen Firewall-Appliances zu verwalten. Weitere Informationen finden Sie unter Panorama-Integration.
Video zu Cloud NGFW für AWS	Cloud NGFW für AWS-Integration mit Panorama

Was ist neu im April 2023

Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • af-south-1 (Kapstadt) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.

Was ist neu im März 2023

Rolle des Mandanten-Readers	Als Cloud NGFW-Mandantenadministrator (TenantAdministrator) können Sie jetzt andere Benutzer in der Rolle „TenantReader“ (Mandanten-Reader) einladen. Ein Benutzer mit dieser Rolle kann alle Aspekte des Cloud NGFW-Mandanten anzeigen und beschreiben, wie z. B. • NGFW-Ressourcen und -Einstellungen • Globale und lokale Regelstapel • Alle Mandantenbenutzer und Mandanteneinstellungen

Video zu Cloud NGFW für AWS	Datenverkehrsfluss von Multi-VPC-NGFW-Ressourcen

Was ist neu im Februar 2023

Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • ap-south-1 (Hongkong) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.
Video zu Cloud NGFW für AWS	Intelligente Feeds auf einem S3-Bucket hosten

Was ist neu im Januar 2023

Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • me-south-1 (Bahrain) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.

Was ist neu im Dezember 2022

Multi-VPC Cloud NGFW-Ressource	Sie können dieselbe Cloud NGFW-Ressource für mehrere virtuelle private Clouds (VPCs) in den eingebundenen AWS-Konten Ihrer Mandanten gemeinsam nutzen. Sie können Endpunkte für eine NGFW-Ressource in verschiedenen VPCs erstellen und den Datenverkehr zur Überprüfung an die NGFW-Ressource weiterleiten. Mehr zu dieser Funktion finden Sie auf der Seite Dokumentation und in einem ausführlichen Blog.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	Neu: Erweiterte Cloud NGFW-Skalierbarkeit über mehrere AWS-VPCs hinweg
Video zu Cloud NGFW für AWS	Multi-VPC Cloud NGFW-Ressource

Was ist neu im November 2022

Mehrere AWS-Konten im Cloud NGFW-Mandanten	Sie können mehrere AWS-Konten in denselben Cloud NGFW-Mandanten einbinden und in diesen Konten Cloud NGFW-Ressourcen erstellen. Weitere Informationen finden Sie unter Mehrere AWS-Konten hinzufügen.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	Cloud NGFW für AWS – Häufig gestellte Fragen (aktualisiert)
Video zu Cloud NGFW für AWS	AWS re:Invent 2022 – Avalon Healthcare Solutions sichert Bereitstellung mit Palo Alto Networks ab (PRT241)

Was ist neu im Oktober 2022

Blogs, Artikel usw. zu Cloud NGFW für AWS.	Interaktiver Preisschätzer macht Cloud NGFW für AWS noch einfacher
Video zu Cloud NGFW für AWS	AWS Firewall Manager-Unterstützung für Palo Alto Networks Cloud NGFW | Amazon Web Services

Was ist neu im September 2022

Videos zu Cloud NGFW für AWS	AWS Summit SF 2022 – Zentrale Verwaltung von Palo Alto Networks Cloud NGFW mit AWS Firewall Manager

Was ist neu im August 2022

Vereinfachtes Cloud NGFW-Abonnement und einfachere Einbindung von Konten	Sie können jetzt mit wenigen Klicks und minimalen Kontextwechseln zwischen der AWS Marketplace- und der Cloud NGFW-Konsole Cloud NGFW für AWS abonnieren und Ihre AWS-Konten einbinden. Weitere Informationen zu dieser Funktion finden Sie auf der Seite Dokumentation und in den AWS-Videos.
Blogs, Artikel usw. zu Cloud NGFW für AWS	Herausragende Netzwerksicherheit für AWS jetzt weltweit einfacher erhältlich
Video zu Cloud NGFW für AWS	Cloud NGFW für AWS bereitstellen, Schritt 1: Cloud NGFW abonnieren (aktualisiert)

Was ist neu im Juli 2022

Cloud NGFW für AWS Credits	Sie können jetzt zu einem Ein-, Zwei- oder Dreijahresvertrag wechseln, indem Sie die SaaS-Vertragsauflistung für **Palo Alto Networks Cloud NGFW für AWS Credits** abonnieren und eine bestimmte Anzahl an Credits erwerben. Dieses Abonnement ordnet Cloud NGFW für AWS Credits Ihrem vorhandenen Cloud NGFW-Mandanten zu. Mit Cloud NGFW für AWS Credits können Sie Cloud NGFW-Ressourcen in Ihrem Mandanten bis zu einer bestimmten Kapazität zu geringeren Kosten nutzen, bis Ihr Vertrag abläuft, während Sie gleichzeitig die Möglichkeit behalten, Ihre Cloud NGFW-Nutzung jederzeit zu erweitern.
Eingehende Entschlüsselung	Sie können jetzt Cloud NGFW für AWS verwenden, um eingehende SSL/TLS-Sitzungen Ihres VPC-Eingangsdatenverkehrs zu entschlüsseln, zu überprüfen und zu schützen. Weitere Informationen finden Sie unter Eingehende Entschlüsselung in Cloud NGFW für AWS einrichten.
Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • ap-northeast-1 (Tokio) • ap-northeast-2 (Seoul) • ap-northeast-3 (Osaka) • ap-south-1 (Mumbai) • sa-east-1 (São Paulo) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.
Videos zu Cloud NGFW für AWS	AWS re:Inforce 2022 – Aufbau einer skalierbaren und abgesicherten globalen Netzwerkinfrastruktur mit AWS (NIS205) AWS re:Inforce 2022 – Integriert und automatisiert: Absicherung jeder Phase der Cloud-Einführung (GRC306)

Was ist neu im Juni 2022

Überwachungsprotokolle in Cloud NGFW	Sie können jetzt Cloud NGFW-Überwachungsprotokolle in Ihrem Cloudwatch-Konto anzeigen. Bitte lesen Sie in der Dokumentation nach, um mehr über diese Funktion zu erfahren.
XFF-Unterstützung in der Cloud NGFW-Richtlinie	Sie können Cloud NGFW-Ressourcen jetzt aktivieren, um die Quell-IP-Adresse im X-Forwarded-For (XFF) HTTP-Header-Feld zu verwenden und die Richtlinie zu erzwingen. Weitere Informationen finden Sie in der Dokumentation.

Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • eu-west-3 (Paris) • eu-north-1 (Stockholm) • eu-south-1 (Mailand) • ap-southeast-1 (Singapur) • ap-southeast-2 (Sydney) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	Bevorstehende Neuerungen für Cloud NGFW – Live: Antworten auf häufig gestellte Fragen
Video zu Cloud NGFW für AWS	Cloud NGFW für AWS – Integration in Splunk

Was ist neu im Mai 2022

Terraform-Unterstützung für Cloud NGFW für AWS	Mit dem neuen cloudngfwaws-Anbieter können Sie den Aufbau Ihrer Sicherheitsinfrastruktur und die Aufrechterhaltung der Netzwerksicherheit Ihrer AWS-VPCs mithilfe von Cloud NGFW-Regelstapeln automatisieren. Weitere Informationen zum Terraform-Anbieter finden Sie unter Terraform-Unterstützung für Cloud NGFW für AWS und im ausführlichen Blog.
Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in den folgenden AWS-Regionen verfügbar. • us-east-2 (Ohio) • ca-central-1 (Kanada) • eu-west-1 (Irland) • eu-west-2 (London) • eu-central-1 (Frankfurt) Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.
CloudFormation-Unterstützung für Cloud NGFW für AWS	Wir haben CloudFormation-Ressourcentypen als öffentliche Erweiterung in der AWS CloudFormation-Registry veröffentlicht. Sie können diese Cloud NGFW-Ressourcen jetzt direkt zu Ihren CloudFormation-Vorlagen hinzufügen, und zwar auf die gleiche Weise, wie Sie von AWS bereitgestellte Ressourcen verwenden. Mit diesen Ressourcentypen können Sie Cloud NGFW-Komponenten mithilfe von IaC-Workflows (Infrastructure as Code) bereitstellen und verwalten.

	Weitere Informationen zur AWS CloudFormation-Unterstützung für Cloud NGFW finden Sie unter Cloud NGFW-Ressourcen für Ihre AWS CFT bereitstellen.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	• Das Entwicklerhandbuch für Cloud NGFW für AWS • Aktualisiert – Cloud NGFW für AWS – Häufig gestellte Fragen
Videos zu Cloud NGFW für AWS	• Interaktive Produkttour • AWS Routing Loop – Gateway Load Balancer und FWaaS • Cloud NGFW-Integration in AWS Firewall Manager • Cloud NGFW für AWS – Entdecken Sie, was sich dahinter verbirgt

Was ist neu im April 2022

Einführung der kostenlosen Testversion von Cloud NGFW für AWS	Sie können jetzt Cloud NGFW für AWS direkt über den AWS Marketplace testen und kaufen. Mit der kostenlosen Testversion können Sie zwei NGFW-Ressourcen mit vollem Funktionsumfang nutzen, um 100 GB Datenverkehr sieben Tage lang kostenlos abzusichern. Legen Sie noch heute los! Um praktische Erfahrungen mit Cloud NGFW zu sammeln, abonnieren Sie es über den AWS Marketplace. Weitere Informationen zur kostenlosen Testversion von Cloud NGFW finden Sie unter Kostenlose Testversion von Cloud NGFW für AWS.
Zusätzliche Unterstützung für AWS-Regionen	Cloud NGFW für AWS ist jetzt in der AWS-Region „us-west-2 (Oregon)“ verfügbar. Eine vollständige Liste der unterstützten Regionen finden Sie unter Unterstützte Regionen und Zonen in Cloud NGFW für AWS.
Programmgesteuerter Zugriff auf Cloud NGFW für AWS	Sie können jetzt Cloud NGFW-Ressourcen mithilfe der REST APIs programmgesteuert erstellen und verwalten. Sie können 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. Weitere Informationen zum programmgesteuerten Zugriff auf Cloud NGFW für AWS finden Sie unter Programmgesteuerten Zugriff aktivieren und im Handbuch zur NGFW für AWS-REST API.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	Cloud NGFW für AWS – Digitaler Kurs
Videos zu Cloud NGFW für AWS	Einführungsveranstaltung zu Cloud NGFW für AWS (On-Demand)

Was ist neu im März 2022

Einführung in Cloud NGFW für AWS	Cloud NGFW für AWS ist ein vollständig verwalteter Dienst auf der AWS-Plattform, der auf den Software-Firewalls von Palo Alto Networks beruht. Mit Cloud NGFW für AWS kann die Bereitstellung der Funktionen und Infrastruktur der Palo Alto Next-Generation Firewall in einem Schritt erfolgen. Cloud NGFW für AWS ist ein regionaler Service. Derzeit ist er in den Regionen Ost-USA (Nord-Virginia) und West-USA (Kalifornien) verfügbar. Weitere Informationen finden Sie in den Ankündigungen zu Cloud NGFW für AWS im Palo Alto Networks-Blog und im technischen Blog auf der Live-Community-Seite. Bitte melden Sie sich über die AWS Marketplace-Seite an, um praktische Erfahrungen mit diesem Dienst zu sammeln. Weitere Informationen zu Cloud NGFW, ihren Funktionen und Preisen finden Sie in der technischen Dokumentation, in der Video-Playlist und auf den Seiten mit häufig gestellten Fragen.
AWS Firewall Manager unterstützt Cloud NGFW	Sie können AWS Firewall Manager verwenden, um die Bereitstellung von Cloud NGFWs von Palo Alto Networks zu orchestrieren und eine zentralisierte Transparenz zu erhalten. AWS Firewall Manager fügt Cloud NGFWs von Palo Alto Networks automatisch und konsistent ohne manuellen Eingriff zu neuen Konten und VPCs hinzu. Diese Integration reduziert den erforderlichen Aufwand für die Überwachung neuer Konten, fügt Firewall-Schutz hinzu und bietet Einblick in nicht konforme Konfigurationen in allen Konten in Ihrem Unternehmen. Weitere Informationen finden Sie in der Ankündigung zu AWS Firewall Manager, auf der AWS Firewall Manager-Dokumentationsseite und im Blog von Jeff Barr zur Integration.
Blogs, Artikel usw. zu Cloud NGFW für AWS.	• Cloud NGFW für AWS – Ankündigungsblog • Cloud NGFW für AWS – Technischer Blog • Cloud NGFW und AWS Firewall Manager – Blog von Jeff Barr • Cloud NGFW für AWS – Häufig gestellte Fragen • Cloud NGFW für AWS-Bereitstellungsarchitekturen • Cloud NGFW für AWS – E-Book
Videos zu Cloud NGFW für AWS	• Einführung in Cloud NGFW für AWS • Bereitstellungsschritt 1: Cloud NGFW abonnieren • Bereitstellungsschritt 2: Sicherheitsleitlinie definieren • Bereitstellungsschritt 3: Cloud NGFW-Ressource erstellen • Zentralisiertes Bereitstellungsmodell (Ost-West-Datenverkehrsschutz) • Verteiltes Bereitstellungsmodell (Schutz für ausgehenden Datenverkehr)

	• Verteiltes Bereitstellungsmodell (Schutz für eingehenden Datenverkehr) • Verteiltes Bereitstellungsmodell (Schutz des Datenverkehrs zwischen Subnetzen) • App-ID in Cloud NGFW • Intelligence Feed (EDL) in Cloud NGFW • Rollen und Berechtigungen in Cloud NGFW • Sicherheitsprofile in Cloud NGFW • Ausgehende TLS-Entschlüsselung in Cloud NGFW

Bekannte Probleme bei Cloud NGFW für AWS

Die folgenden bekannten Probleme wurden in Cloud NGFW für AWS erkannt.

ID	Beschreibung
DIT-40616	In manchen Fällen kann das Validieren und anschließende Übernehmen einer Regelstapeländerung dazu führen, dass Ihre Cloud NGFW-Ressource eine falsche Konfiguration anwendet. Dieses Problem kann auch dazu führen, dass eine automatisch skalierte Firewall beim Hochfahren eine falsche Konfigurationsdatei anwendet. Um dieses Problem zu beheben, empfiehlt Palo Alto Networks, dass Sie nicht auf **Validate (Prüfen)** klicken, wenn Sie eine Änderung an Ihrem Regelstapel vornehmen. Führen Sie stattdessen ein Commit für die Änderung ohne Validierung durch.
FWAAS-1501	Cloud NGFW löst mithilfe des nativen AWS Route 53 Resolver FQDNs auf, die Sie in Ihren Regeln konfigurieren. Der AWS Route 53 Resolver kann einen FQDN in eine IP-Adresse auflösen. Das unterscheidet sich von dem, was Sie möglicherweise sehen, wenn Sie den Route 53 Resolver in Ihren VPCs verwenden.
FWAAS-2589	Wenn Sie ein AWS-Konto in Ihren Cloud NGFW-Mandanten einbinden, wählen Sie einen dieser beiden Endpunkterstellungsmodi aus: kundenverwaltet und dienstverwaltet. In Cloud NGFW können Sie nach Abschluss des Kontoeinbindungsprozesses den Modus nicht mehr wechseln.
FWAAS-3009	Mit Cloud NGFW können Sie einen S3-Bucket als Protokollierungsziel für die NGFW-Ressourcen verwenden. In AWS-Regionen außerhalb der USA erwartet Cloud NGFW, dass Sie die S3-Buckets verwenden, die in derselben AWS-Region erstellt wurden, in der Sie die NGFW-Ressourcen bereitstellen.
FWAAS-5817	Die Panorama-Benutzeroberfläche zeigt keine Fehlermeldung an, wenn der Push des Cloud-Managers oder des Cloud NGFW-Dienstes fehlschlägt. Sie erfahren erst dann von einem Push-Fehler, wenn der Firewall-**Commit** fehlschlägt.
FWAAS-5823	Beim Erstellen einer neuen Cloud-Gerätegruppe können Sie nicht auswählen, welche Zertifikate für *Forward Trust* oder *Forward Untrust* verwendet werden.
FWAAS-6380	Wird eine Änderung ohne Commit per Push an eine Cloud-Gerätegruppe übertragen, kann eine Fehlermeldung angezeigt werden. Führen Sie vor dem Übertragen per Push einen Commit für Ihre Änderungen durch.
FWAAS-6540	Eine vorhandene Gerätegruppe ermöglicht Ihnen fälschlicherweise, nach der Erstellung einen anderen Vorlagenstapel anzuwenden. Sie können nicht mehreren Mandanten verschiedene Vorlagenstapel für die gleiche Gerätegruppe zuordnen.
FWAAS-6542	Bei Anwendung auf eine andere Gerätegruppe schlägt die Aktualisierung des Vorlagenstapels fehl.

ID	Beschreibung
FWAAS-6961	Beim Panorama AWS-Plug-in für den Cloud NGFW-Dienst kann der zum ersten Mal mit Panorama verknüpfte Mandant unter der Registerkarte „Discovered VPC“ (Erkannte VPC) keine VPCs sehen. Problemumgehung: Der zum ersten Mal verknüpfte Mandant muss unter der Registerkarte **Discover VPC (VPC erkennen)** auf die Schaltfläche **Refresh VPC (VPC aktualisieren)** klicken, um eine Liste der VPCs abzurufen.
FWAAS-7721	In einer skalierten Umgebung stürzt die Benutzeroberfläche des AWS-Plug-ins ab, wenn die IP-Adressen-zu-Tags-Nutzlast im Dashboard **Monitoring Definition (Überwachungsdefinition)** angezeigt wird. **Problemumgehung**: Verwenden Sie die Befehlszeilenschnittstelle von Panorama, um den folgenden Befehl auszuführen: `show plugins aws details-dashboard`.
FWAAS-7766	Auf der Seite **Discovered VPC (Erkannte VPC)** in der Cloud NGFW-Benutzeroberfläche wird der Grund für den Fehler nicht angezeigt, wenn der Überwachungsstatus für ein erkanntes VPC „Failed“ (Fehlgeschlagen) lautet.
FWAAS-10971	Beim Ausgeben des Befehls **reset** mit ungültigen Firewall-Ressourcen-IDs werden die Regelnutzungszähler nicht zurückgesetzt. Dies ist ein erwartetes Verhalten.

Cloud NGFW für AWS – behobene Probleme

Die folgenden Probleme wurden in dieser Version von Cloud NGFW für AWS behoben.

ID	Beschreibung
FWAAS-3009	Mit Cloud NGFW können Sie einen S3-Bucket als Protokollierungsziel für die NGFW-Ressourcen verwenden. In AWS-Regionen außerhalb der USA erwartet Cloud NGFW, dass Sie die S3-Buckets verwenden, die in derselben AWS-Region erstellt wurden, in der Sie die NGFW-Ressourcen bereitstellen.
FWAAS-5842	Es ist nicht möglich, einzelne Cloud-Gerätegruppenprotokolle, die an CDL gesendet wurden, über die Registerkarte **Monitor (Überwachen)** in Panorama anzuzeigen. Es werden Protokolle für alle Cloud-Gerätegruppen angezeigt.
FWAAS-6536	Cloud NGFW zeigt nicht alle Cloud-Gerätegruppen an, wenn Sie **All (Alle)** auf der Seite **Tenants (Mandanten)** auswählen. Wenn Sie einen einzelnen Mandanten auswählen, werden alle Cloud-Gerätegruppen in der Liste angezeigt.
FWAAS-6633	Möglicherweise wird ein Firewall-Commit nach der ersten Konfigurationsübertragung per Push für die Cloud-Gerätegruppe von Panorama nicht ausgelöst. **Problemumgehung**: Wiederholen Sie die Konfigurationsübertragung per Push für die Cloud-Gerätegruppe von Panorama.
FWAAS-8622	Der Regelstapel von Cloud NGFW für AWS kann im Zustand vor dem Commit hängen bleiben, wenn die Schaltfläche **Validate (Prüfen)** vor dem ersten Commit ausgewählt wird. **Problemumgehung**: Validieren Sie die Änderungen an Ihrer Regelstapelkonfiguration nicht. Wählen Sie stattdessen **Commit** ohne Validierung aus.

