paloalto
TECHDOCS

Erste Schritte in Cloud NGFW für AWS

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 5, 2024

Table of Contents

Einführung in Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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 eines 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 zugeordneten Objekte und Sicherheitsprofile. Um einen Regelstapel zu verwenden, verknüpfen Sie ihn mit einer oder mehreren NGFW-Ressourcen. Cloud NGFW bietet zwei Typen von Regelstapeln.

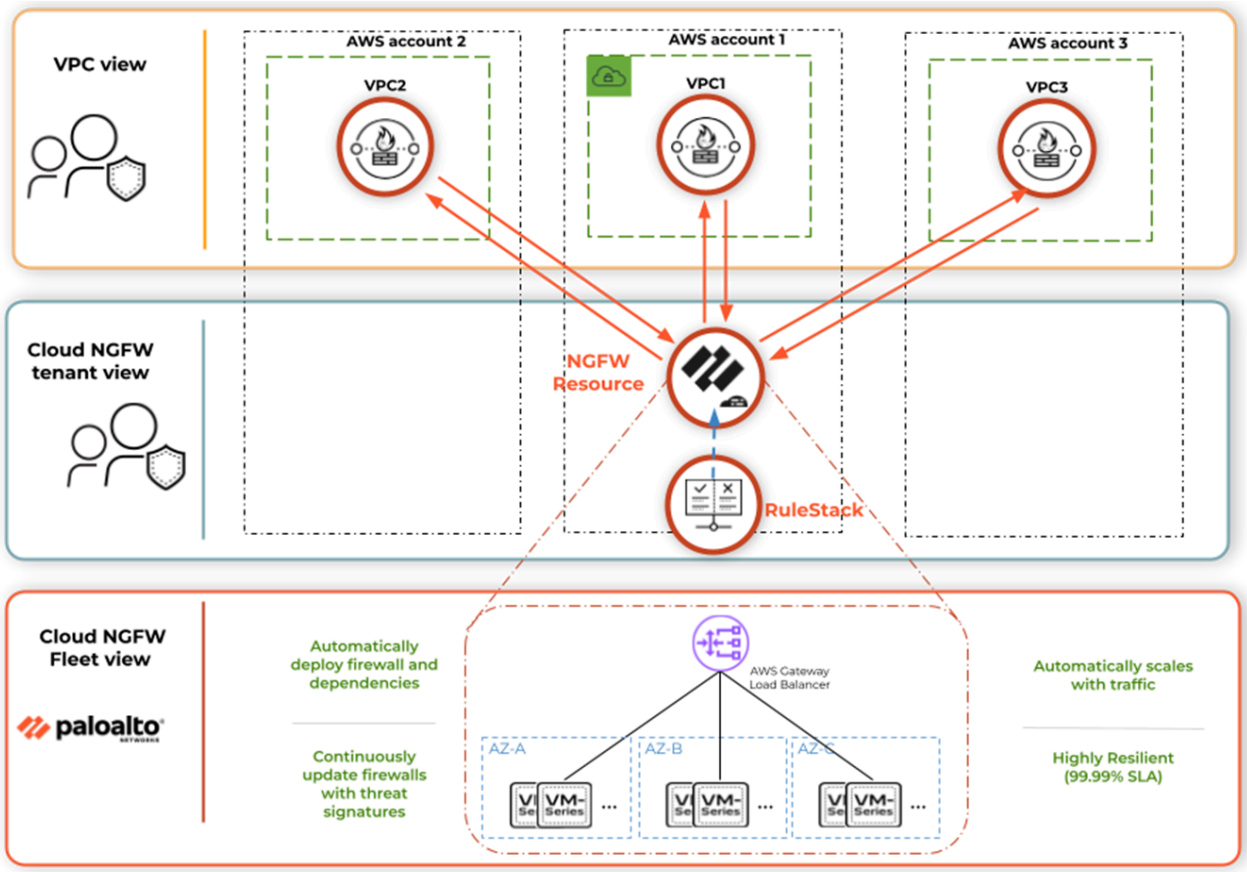
  Cloud NGFW unterstützt zwei Typen von Regelstapeln:

  - **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.

Informationen zu Cloud NGFW-Endpunkten

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. Weitere Informationen finden Sie unter Datenverkehr zu Cloud NGFW leiten.

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. Fügen Sie Ihr AWS-Konto dem Cloud NGFW-Mandanten hinzu. 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 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 und auch die VPC-Endpunkte zu erstellen
4. **VPC-Routingtabellen aktualisieren**– Nach der Bereitstellung Ihrer Cloud NGFW-Ressource müssen Sie den Datenverkehr zu Cloud NGFW leiten, um weitere Informationen zu erhalten. Durch die Aktualisierung Ihrer VPC-Routingtabellen wird der Datenverkehr zur Überprüfung und Durchsetzung an die NGFW-Firewall-Ressource geleitet.

Cloud NGFW-Anwendungsfälle

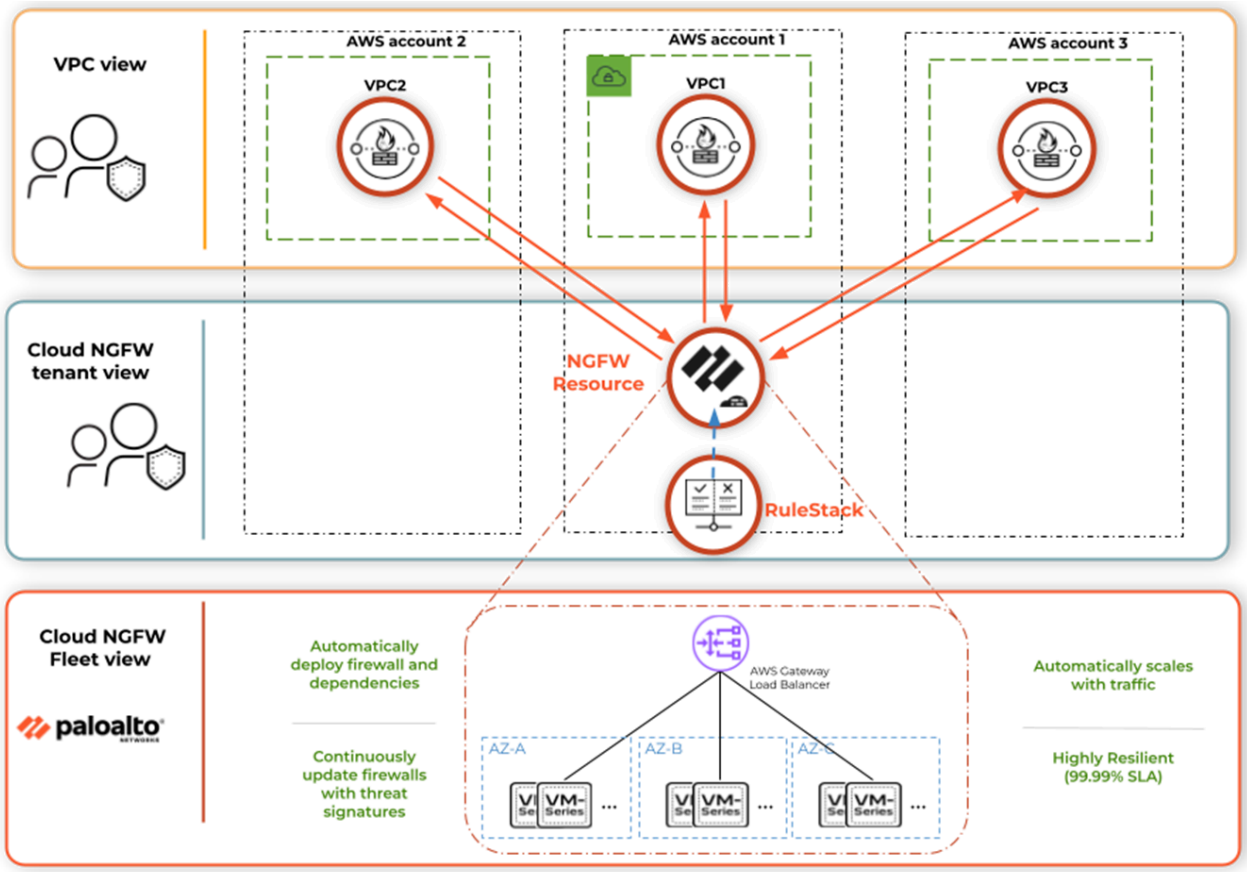
Cloud NGFW bietet Ihnen Tools und Funktionen zum Sichern von eingehendem Datenverkehr, ausgehendem Datenverkehr und Ost-West-Datenverkehr.

- **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 innerhalb Ihrer Anwendungs-VPC entsteht. Leiten Sie diesen Datenverkehr an Ziele außerhalb der AWS-Region. 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 stellen Sie den Datenverkehr zwischen Quelle und Ziel in zwei verschiedenen Anwendungs-VPCs oder in zwei verschiedenen Subnetzen in denselben VPCs bereit. Cloud NGFW kann die Verbreitung von Malware in Ihrer AWS-Umgebung stoppen.

Cloud NGFW-Ressource und NGFW-Endpunkte

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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 Routentabellen finden Sie unter Datenverkehr zu Cloud NGFW leiten.

Unterstützte Cloud NGFW-Verwaltungs- und Bereitstellungsfunktionen

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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

Unterstützte Funktionen zur Verwaltung von Sicherheitsrichtlinien

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

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlini	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
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	• SCM-Konsole
Protokolltypen	Cloud NGFW generiert mit Zeitstempeln versehene 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	• Verkehrs-Protokolle • Bedrohungsprotokolle • Entschlüsselungsprotokolle • Auditierungslog	• Verkehrs-Protokolle • Bedrohungsprotokolle • URL-Filterungs-Protokolle • Entschlüsselungsprotokolle	• Protokoll-Viewer • Verkehrs-Protokolle • Bedrohungsprotokolle • URL-Filterungs-Protokolle • Entschlüsselungsprotokolle

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlini	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	zeichnet Informationen für einen separaten Ereignistyp auf. Beispielsweise generiert Cloud NGFW ein Bedrohungsprotokoll, um Datenverkehr aufzuzeichnen, der mit einer Spyware-, Sicherheitslücken- oder Virensignatur übereinstimmt.			
Protokollziele	Cloud NGFW kann die generierten Protokolle an AWS-Ziele und den Strata-Protokollierungsdienst 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 • Strata-Protokollierungsdienst • Protokolle vom Strata-Protokollierungsdienst an einen Syslog-Server weiterleiten • Protokolle vom Strata-Protokollierungsdienst an einen	• Amazon Simple Storage Service(S3)-Bucket • Amazon CloudWatch-Protokollgruppe • Amazon Kinesis Data Firehose • Strata-Protokollierungsdienst • Protokolle vom Strata-Protokollierungsdienst an einen Syslog-Server weiterleiten • Protokolle vom Strata-Protokollierungsdienst an einen

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlini	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
			HTTPS-Server weiterleiten	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 im Strata-Protokollierungsdienst erkunden • Protokolle in Panorama überwachen • Application Command Center (ACC) in Panorama überwachen	• Protokolle in Amazon Destinations erkunden • Protokolle im Strata-Protokollierungsdienst erkunden • Activity Insights in Strata Cloud Manager • Command Center in Strata Cloud Manager
Berichte	Erstellen Sie vordefinierte und benutzerdefinierte Berichte zu Anwendungen, Bedrohungen und URL-Aktivitäten Ihres VPC-Datenverkehrs.	-	• Geplante und benutzerdefinierte Berichte	• Geplante und benutzerdefinierte Berichte
Richtlinienanalyse und -optimierung	Die Überwachung der Regelnutzung hilft Ihnen zu bewerten, ob Ihre Richtlinienumsetzung weiterhin Ihren Durchsetzungsanforderungen entspricht. Die Richtlinienanalyse analysiert Ihre	-	• Regelnutzung • Richtlinienoptimierer	• Regelnutzung • Richtlinienoptimierer

Verwaltung, Visualisierung und Protokollierung von Sicherheitsrichtlini	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	Cloud NGFW-Regeln und empfiehlt mögliche Konsolidierungen oder Entfernung spezifischer Regeln, um Ihren gewünschten Sicherheitsstatus zu erreichen. Sie überprüft auch Anomalien wie Schatten, Redundanzen, Verallgemeinerungen, Korrelationen und Konsolidierungen in Ihrem Regelsatz.			
Paketerfassung	Palo Alto Networks Firewall zum Durchführen einer benutzerdefinierten Paketerfassung oder einer Bedrohungspaketerfassung.	-	-	-

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
Sicherheitsrichtlinie	Die Sicherheitsrichtlinie schützt Ihren VPC-Datenverkehr vor Bedrohungen und Störungen.	• Lokaler Regelstapel • Globaler Regelstapel	• Sicherheitsrichtlinien • Vor-Regeln • Nach-Regeln • Standardregeln	• Sicherheitsrichtlinien • Vor-Regeln • Nach-Regeln • Standardregeln

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.			
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	• IPv4-Netzmaske • IPv4-Bereiche • IPv4-Platzhaltermaske • FQDNs
Adressgruppen	Sie können bestimmte Quell- oder Zieladressen gruppieren, für die die gleiche Richtliniendurchsetzung erforderlich ist.	-	• Adressgruppen	• Adressgruppen
Regionen	Sie können Datenverkehr von (oder zu) IP-Adressen basierend	• Länder	• Vordefinierte Regionen • Benutzerdefinierte Regionen	• Regionen

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	auf ihrem geografischen Standort, 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	• Port und Protokoll	• Dienste	• Dienste

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.			
Dienstgruppen	Sie können Dienste mit denselben Sicherheitseinstellungen in Dienstgruppen zusammenfassen, um die Anzahl der Regeln in der Sicherheitsrichtlinie zu reduzieren.	-	• Dienstgruppen	• Dienstgruppen
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,	• Intelligenz-Feeds • Integrierte Feeds • EDL-Hosting-Dienst-Feeds	• Externe dynamische Listen • Integrierte EDL • EDL-Hosting-Dienst-Listen	• Externe dynamische Listen • Integrierte EDL • EDL-Hosting-Dienst-Listen

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.			
Anwendungen	Sie können Ihren VPC-Datenverkehr mithilfe des App-ID™-Verkehrsklassifizierungssystems von Palo Alto Networks präzise steuern. Dieses System basiert auf Anwendungssignaturen, um die Anwendungen in Ihrem Netzwerk genau zu identifizieren.	• APP-IDs	• APP-IDs • Benutzerdefinierte Anwendungssignaturen	• APP-IDs • Benutzerdefinierte Anwendungssignaturen

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
Anwendungsgruppe	Sie können eine Reihe von App-IDs gruppieren, für die die gleiche Richtliniendurchsetzung erforderlich ist.	-	• Anwendungsgruppen	• 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 entsprechen, automatisch	-	• Anwendungsfilter	• Anwendungsfilter

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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	• 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	-	• Tags	• Tags

Richtlinien und Richtlinienobjekte	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	Richtlinienregeln anwenden.			
Dynamische Benutzergruppe	Ermöglicht Ihnen, eine Liste von Benutzern aus der 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 Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
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.	• 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	• Verwalten: Zertifikatverwaltung *Das Cloud-Zertifikat wird von Cloud NGFW noch nicht unterstützt.*

Zertifikate und Entschlüsselung	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	Entschlüsseln von verschlüsseltem Text. Jedes Zertifikat enthält außerdem eine digitale Signatur zur Authentifizierung der Identität des Ausstellers.		• Abrufen eines Zertifikats von einer externen Zertifizierungsstelle (CA) • Online-Certificate-Status-Protocol(OCSP)-Responder • Vertrauenswürdige Standardzertifizierungsstellen • Zertifikatprofil	
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,	• 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	• Verwaltung der Entschlüsselung

Zertifikate und Entschlüsselung	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	die benötigt werden, um als vertrauenswürdige dritte Partei für eine Sitzung zu fungieren.			

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
Schutz vor IPS-Sicherheitslücken	Der Sicherheitslückenschutz schützt vor eingehenden Bedrohungen, bei denen ein Angreifer versucht, eine Sicherheitslücke im System auszunutzen, um in Ihr Netzwerk einzudringen. Die Sicherheitslücken im System können in Form von Pufferüberläufen, der Ausführung illegalen Codes usw. auftreten.	• Best Practices	• Standardprofil • Strenges Profil • Benutzerdefiniertes Profil (Bedrohungsausnahmen) • Benutzerdefinierte Signaturen für Sicherheitslücken • Signaturen für Snort/Suricata	• Schutz vor Sicherheitslücken
Anti Spyware	Anti-Spyware erkennt und blockiert ausgehende Bedrohungen, insbesondere Command-and-Control(C2)-Aktivitäten, die (nach einem Cyberangriff)	• Best Practices	• Standardprofil • Strenges Profil • Benutzerdefiniertes Profil (Bedrohungsausnahmen) • Benutzerdefinierte Signaturen für Spyware	• Anti Spyware

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.		• 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 keinen tatsächlichen Anwendungsfall gibt.	• Best Practices und Anpassungen	• Basisprofil • Strenges Profil • Benutzerdefiniertes Profil	• Dateiblockade
Antivirus	Antivirus erkennt und schützt vor Malware, die in komprimierten	• Best Practices	• Standardprofil	• Anti-Virus

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	Dateien, ausführbaren Dateien, PDF-Dateien sowie HTML- und JavaScript-Viren in Ihrem VPC-Datenverkehr versteckt ist		• 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.	-	WildFire-Analyse	WildFire-Analyse
URL Filtering	Die URL-Filterung analysiert den VPC-Datenverkehr und steuert die URLs,	• Zugriffskontrolle für von Palo Alto Networks verwaltete URL-Kategorien	• Zugriffskontrolle für von Palo Alto Networks verwaltete URL-Kategorien	• Zugriffskontrolle für von Palo Alto Networks verwaltete URL-Kategorien

Sicherheitsdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	auf die Ihre VPC-Workloads zugreifen (sowohl im Klartext- als auch im verschlüsselten 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.	• Benutzerdefinierte URL-Kategorien	und benutzerdefinierte URL-Kategorien • Cloud-Inline-Kategorisierung	und benutzerdefinierte URL-Kategorien • 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.	-	DNS Security	DNS Security
Datenfilterung und Enterprise DLP	Bei der Datenfilterung werden vertrauliche Informationen in Ihrem VPC-Datenverkehr erkannt – etwa Kreditkarten- oder Sozialversicherungsnummern oder interne	-	• Vordefinierte Muster, reguläre Ausdrücke und Dateieigenschaften • Enterprise DLP	*DLP auf SCM wird derzeit nicht unterstützt.*

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

Sicherheitszonen und Schutz	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
Sicherheitszonen	Sicherheitszonen sind eine logische Möglichkeit, Schnittstellen auf der Firewall und Cloud NGFW-Endpunkte zu	-	Private und öffentliche Zonen	-

Sicherheitszonen und Schutz	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	gruppieren, um den VPC-Datenverkehr zu steuern und zu protokollieren.			
Zonenschutz	Der Zonenschutz verteidigt Netzwerksicherheitszonen vor Flood-Angriffen, Reconnaissance-Versuchen und paketbasierten Angriffen.	-	Zonenschutz	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
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	• 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	*XFF auf SCM wird derzeit nicht unterstützt.*

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.			
NAT	Die Firewalls von Palo Alto Networks können Ziel-NAT für Ihren eingehenden VPC-Datenverkehr und Quell-NAT für Ihren ausgehenden VPC-Datenverkehr erzwingen.	Ausgangs-NAT	Ausgangs-NAT	-
DNS-Proxy	Wenn Sie Cloud NGFW als DNS-Proxy konfigurieren, übernimmt der Dienst die Aufgabe eines Vermittlers zwischen Clients und Servern und eines DNS-	-	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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 Priorität	-	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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.	-	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
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/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	-	-	-

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	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) über die private Standleitung und den gesamten übrigen Datenverkehr über die Internetverbindung zu senden. Oder Sie können aus Leistungsgründen festlegen, dass geschäftskritische Anwendungen			

Netzwerkdienste	Beschreibung	Native Richtlinienverwaltu (Regelstapel)	Panorama-Richtlinienverwaltu (Cloud-Gerätegruppen)	Strata Cloud Manager (SCM) für die Richtlinienverwaltu
	über die Standleitung geroutet werden, während der gesamte übrige Datenverkehr, z. B. das Surfen im Internet, über die günstigere Verbindung gesendet wird.			

Erste Schritte im AWS Marketplace

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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.

  Sie können dann dem Cloud NGFW-Mandanten mehrere weitere AWS-Konten hinzufügen, anschließend Cloud NGFW-Ressourcen (auch NGFWs genannt) erstellen und sie VPCs in ihren AWS-Konten zuordnen. Erstellen Sie Sicherheitsrichtlinienregeln für diese NGFWs und überwachen Sie die Nutzung der Cloud NGFW-Mandanten, um Messdatensätze an den AWS Marketplace Metering Service zu senden. 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 den AWS Firewall Manager nicht mehr mit diesem Cloud NGFW-Mandanten verwenden.

- **Erste Schritte mit einem AWS Firewall Manager-Administratorkonto** – Wenn Sie derzeit den 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 können Sie den Richtlinien-Workflow von AWS Firewall Manager verwenden, 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.

Erste Schritte über ein AWS-Mitgliedskonto

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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.

Erstellen Sie ein Cloud NGFW-PAYG-SaaS-Abonnement, 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
- Multi-Mandanten-Benutzer eines einzelnen Benutzers, der auf mehreren Mandanten unterstützt wird
- Mehrere AWS-Konten 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 definieren Sie die unten beschriebenen Parameter in einer CloudFormation-Vorlage (CFT), um die Erstkonfiguration abzuschließen.

- **Endpunktkonfiguration** (erforderlich) – Die kontoübergreifende IAM-Rolle enthält Berechtigungen, die es Cloud NGFW erlauben, 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 **Ja** auswählen, erteilen Sie Cloud NGFW die Berechtigung, die erforderlichen Endpunkte in Ihren VPCs zu erstellen und zu verwalten. Wenn Sie **Nein** auswählen, müssen Sie NGFW-Endpunkte manuell 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.

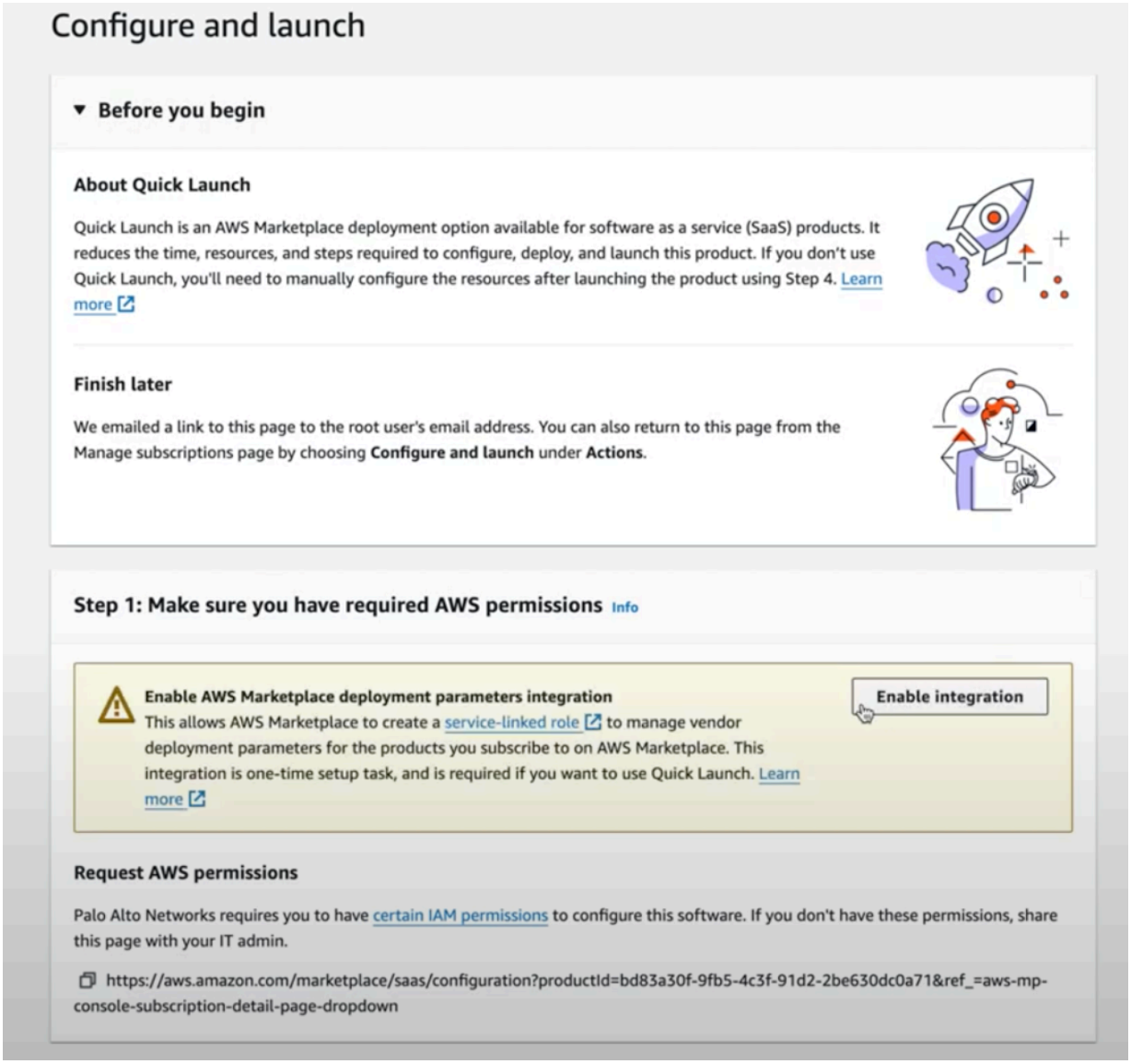
STEP 1 | Melden Sie sich bei der AWS-Konsole an.

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

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

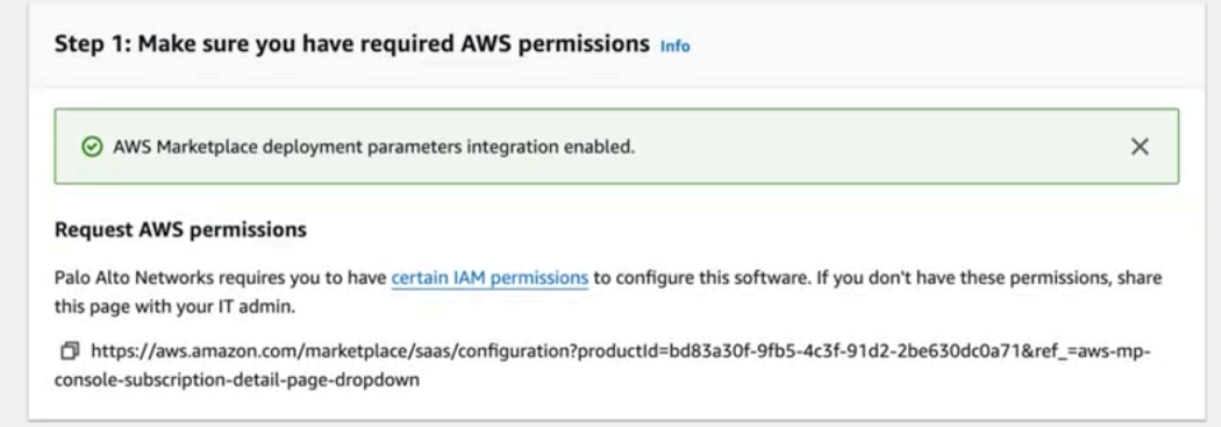
STEP 4 | Klicken Sie auf **Set up product (Produkt einrichten)**. Dadurch wird die Seite „Konfigurieren und Starten“, SaaS-Schnellstart, in AWS Marketplace geöffnet. Palo Alto Networks hat eine Schnellstart-

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



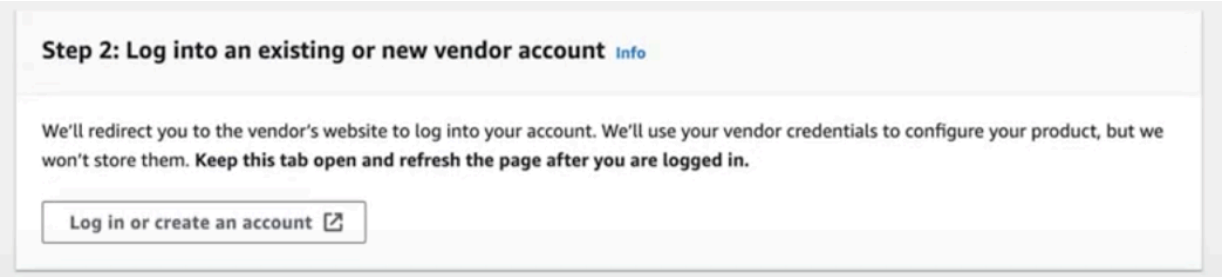
STEP 5 | Klicken Sie auf der Seite „Configure and Launch“ (Konfigurieren und Starten) des Schnellstarts auf **Enable Integration (Integration aktivieren)**, um sicherzustellen, dass Sie über die erforderlichen IAM-Berechtigungen von AWS verfügen.

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

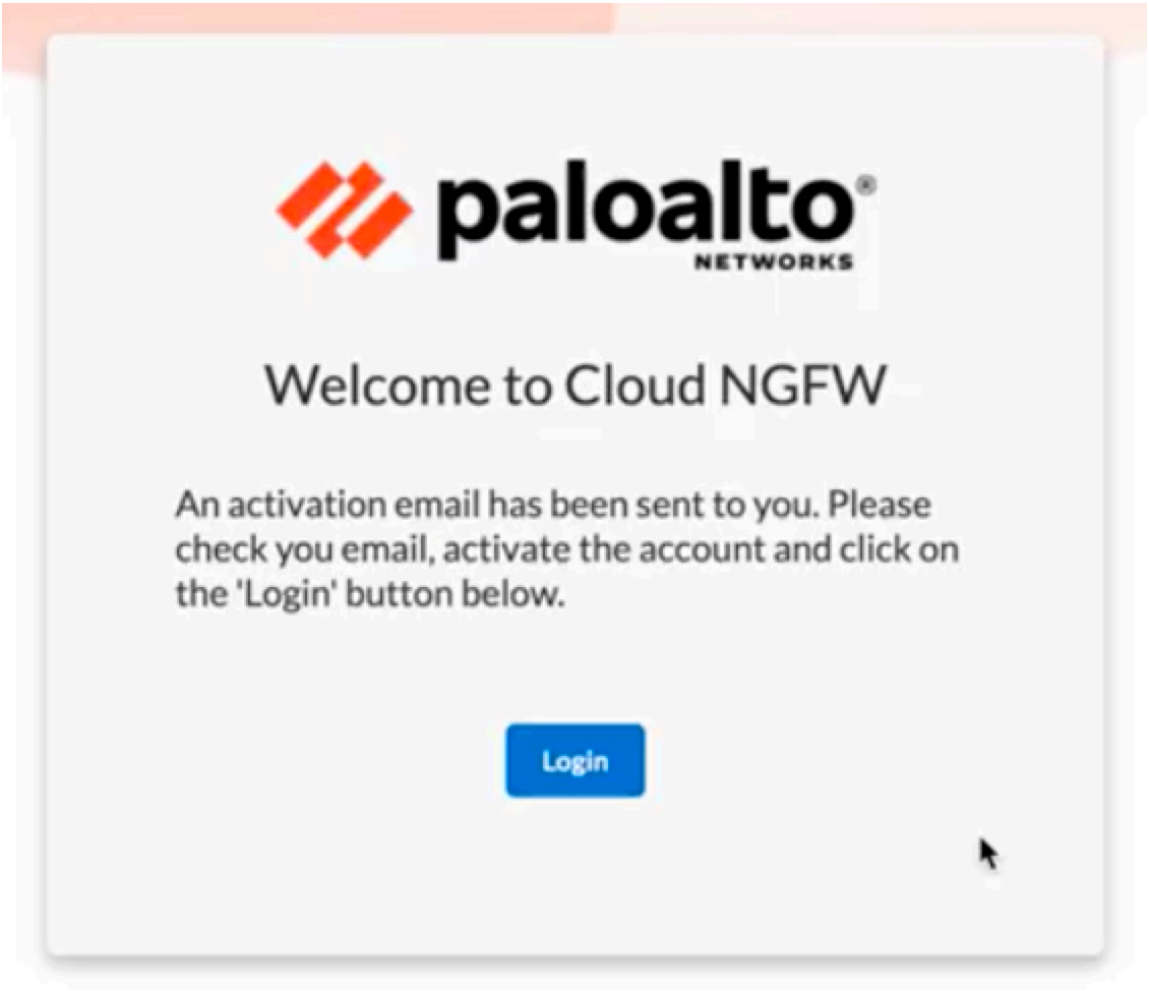
des Anbieters zu erstellen. Dadurch gelangen Sie zu einer Registrierungsseite zum Erstellen eines Mandanten des Cloud NGFW für AWS-Mandanten.



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

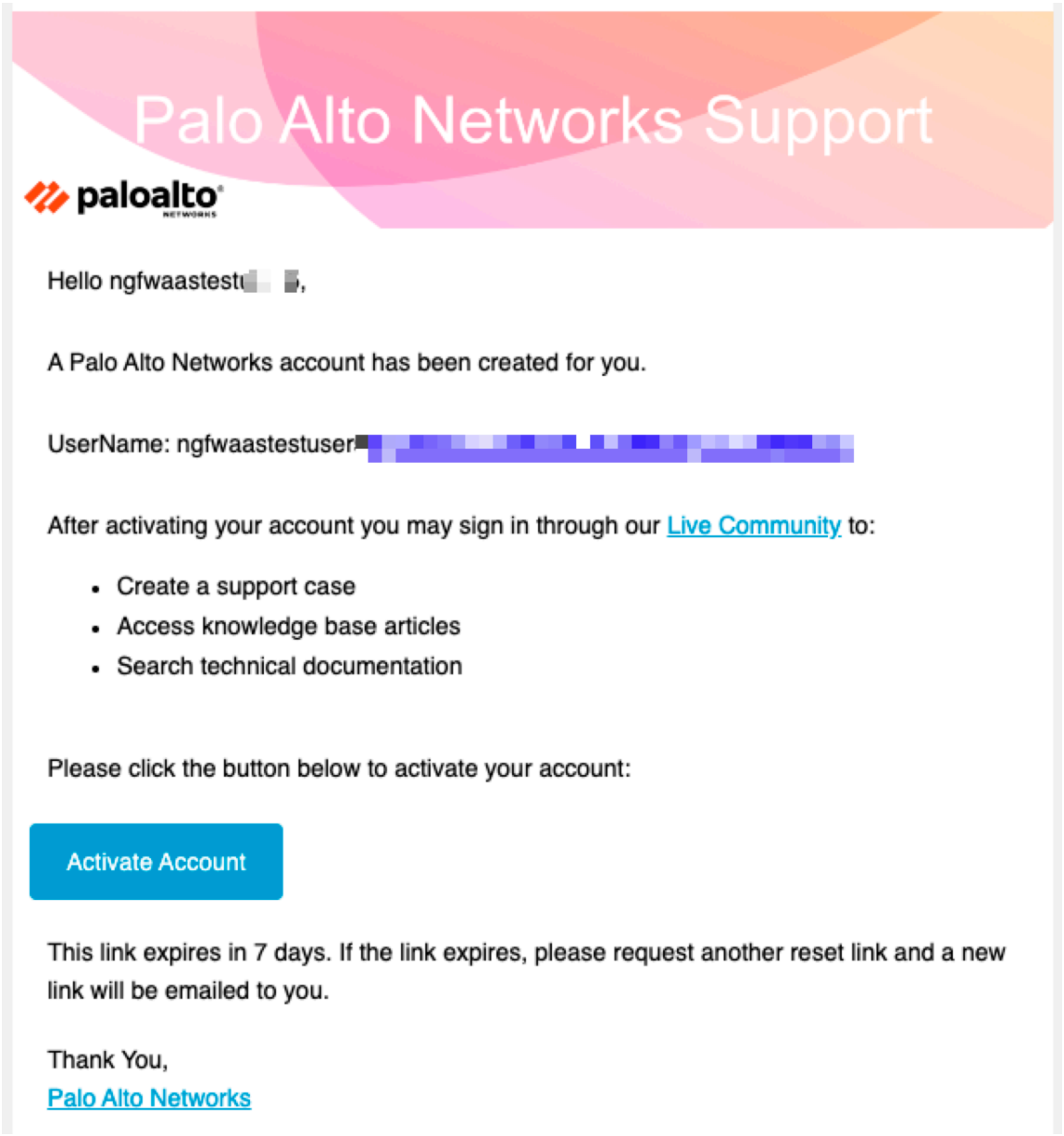
   Die von Ihnen eingegebene E-Mail-Adresse muss identisch mit derjenigen sein, die Sie für die erste Anmeldung beim Cloud NGFW-Dienst verwendet haben. Darüber hinaus wird diese E-Mail-Adresse bei der erstmaligen Anmeldung verwendet, um den ersten Benutzer zu erstellen – den Mandantenadministrator. Außerdem 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.

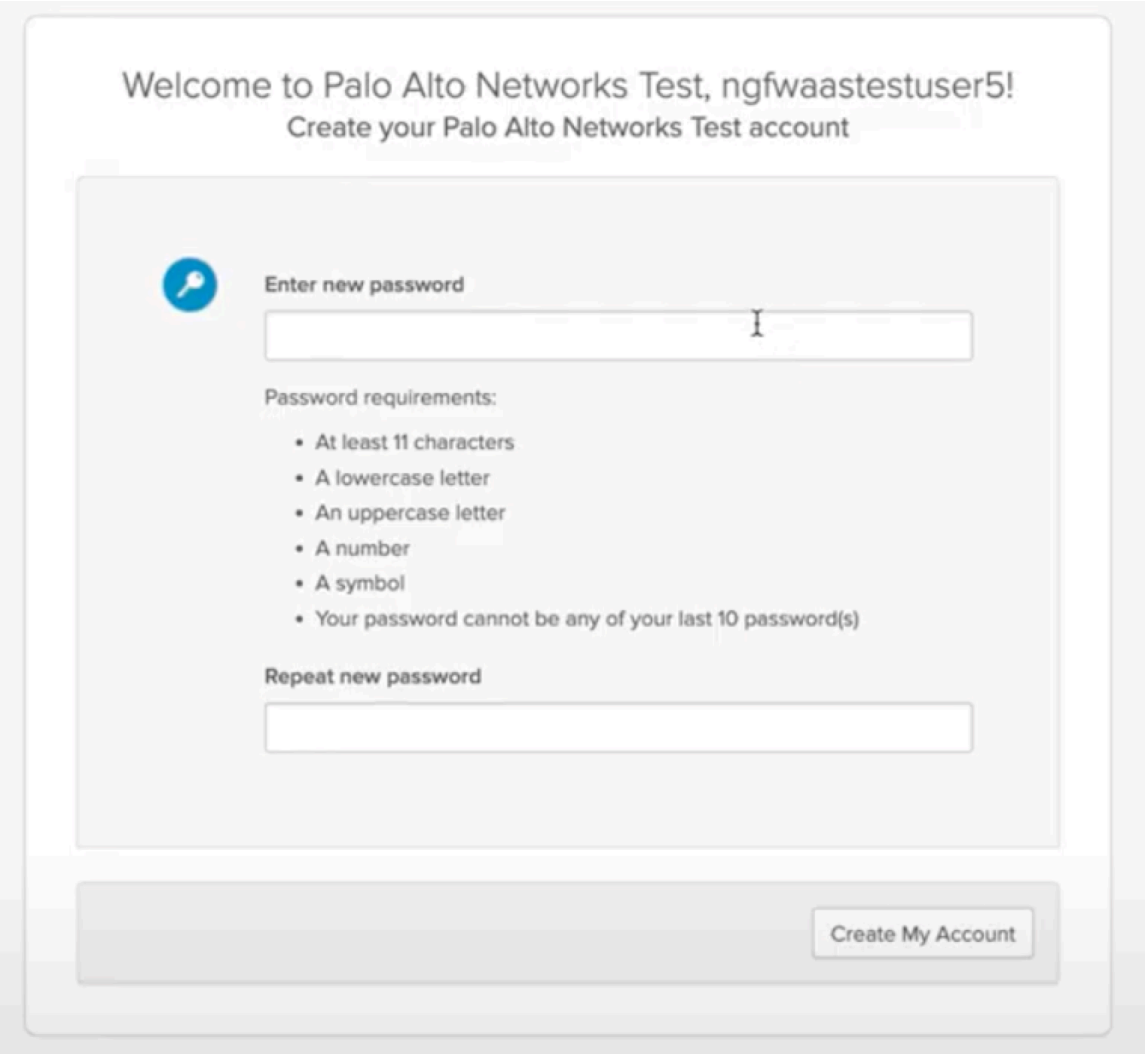


4. Klicken Sie in der E-Mail, die Sie erhalten haben, auf die Schaltfläche **Activate Account (Konto aktivieren)**.

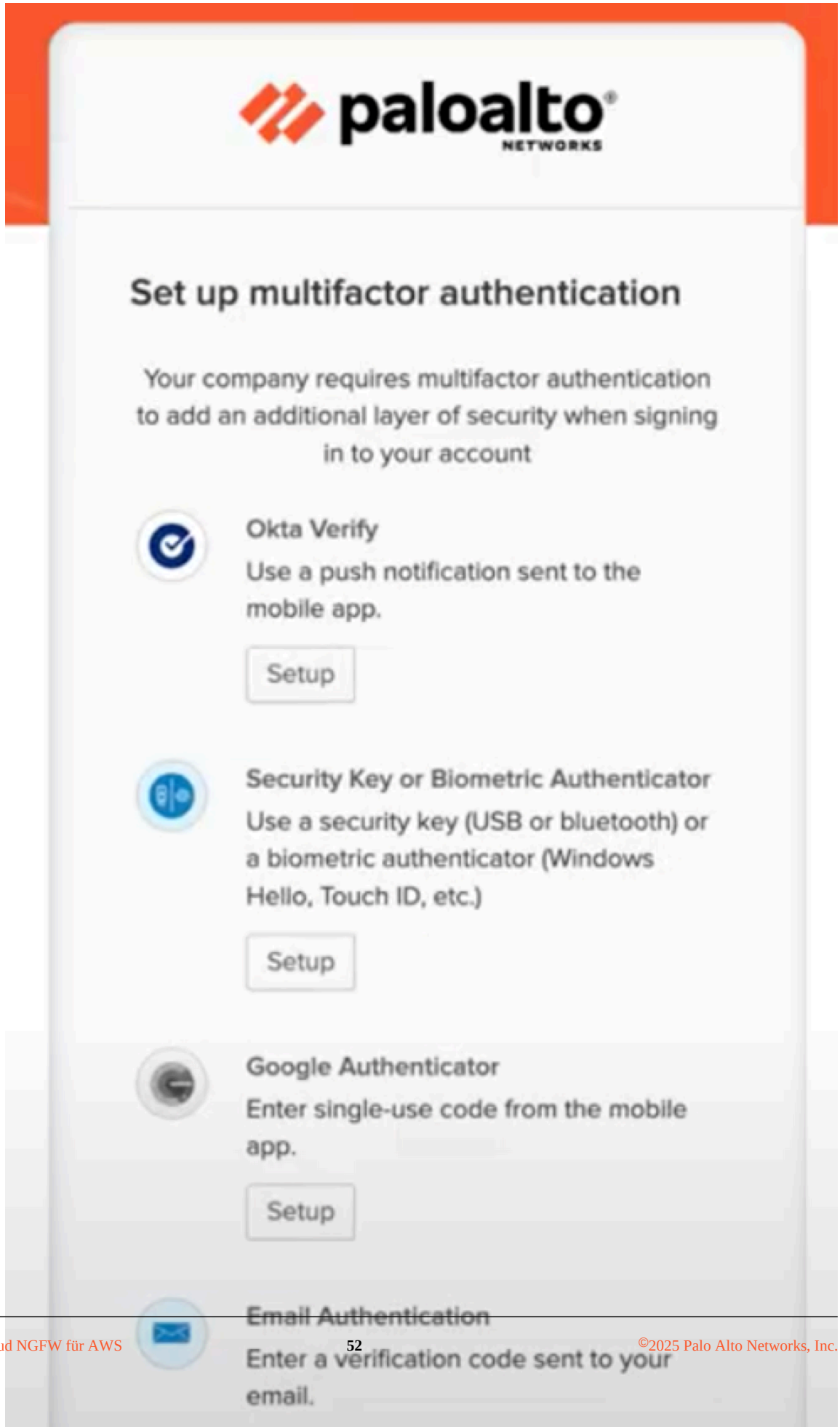
   Der Link ist 7 Tage lang aktiv. Wenn Sie innerhalb von 7 Tagen nicht auf den Link klicken, müssen Sie die Aktivierungs-E-Mail erneut anfordern.



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).

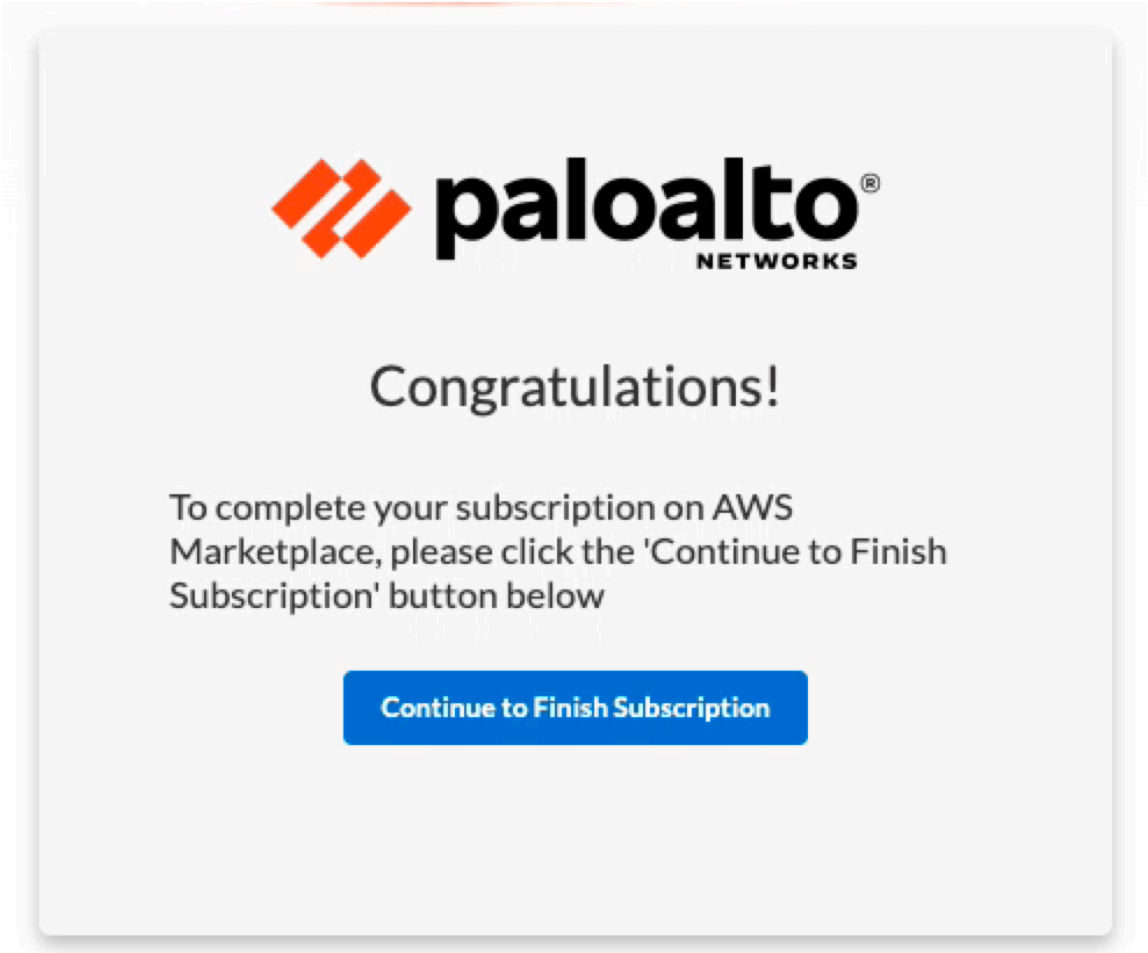


Wenn Sie sich nicht bei MFA registriert haben, aber Ihr SSO-Passwort kennen, werden Sie bei Ihrer ersten Anmeldung bei einer der Anwendungen aufgefordert, sich bei MFA zu registrieren. Um MFA zurückzusetzen, erstellen Sie ein Support-Ticket.

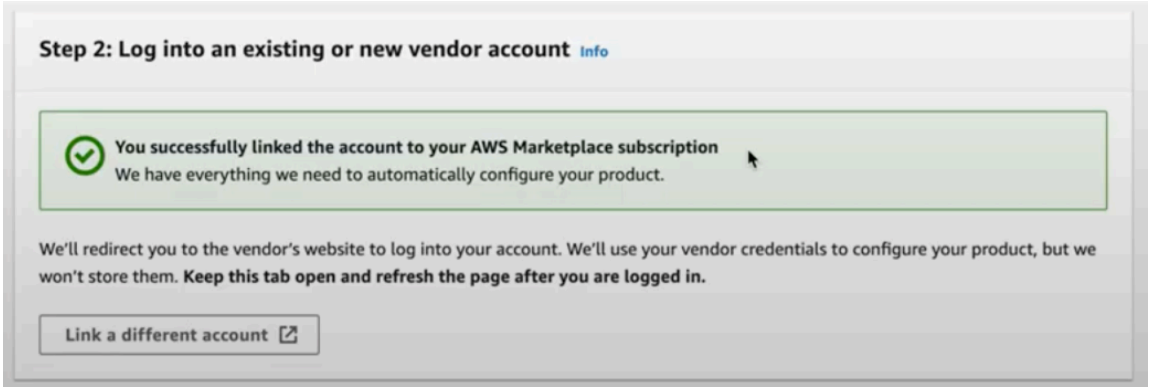
8. Wählen Sie eine der MFA-Methoden aus und klicken Sie auf **Setup (Einrichten)**.
9. Schließen Sie den MFA-Verifizierungsprozess ab. Wenn Sie beispielsweise auf die Schaltfläche „Setup“ (Einrichten) für die E-Mail-Authentifizierung klicken, werden Sie aufgefordert, auf die Schaltfläche **Send me the 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)**.

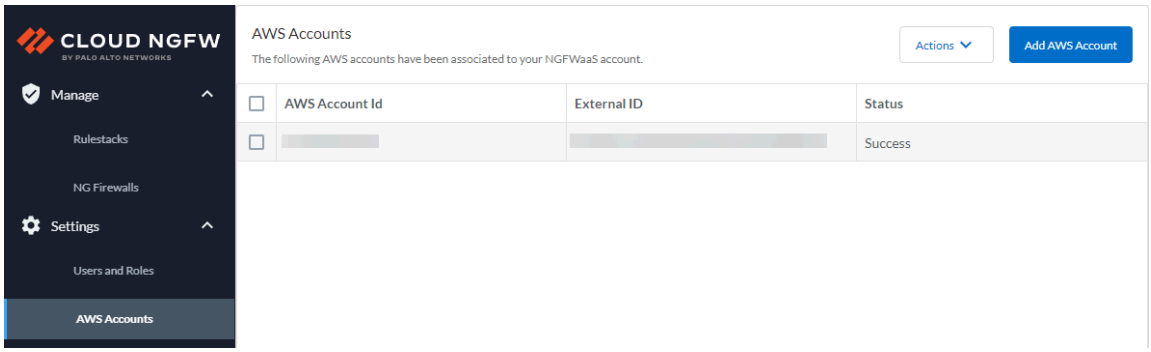
STEP 8 | Aktivieren Sie im Abschnitt „Capabilities“ (Fähigkeiten) unten in der CFT-Konsole das Kontrollkästchen **I acknowledge that AWS CloudFormation might create IAM resources (Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt)**.

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.*

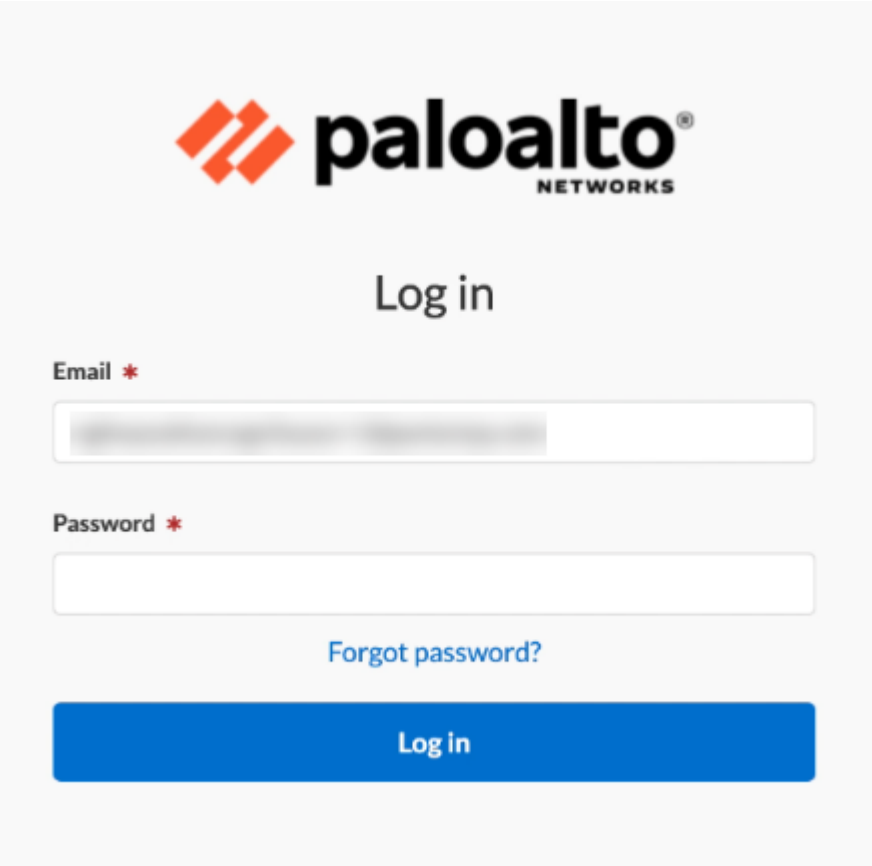


SAML 2.0 kann als Identitätsanbieter für Cloud NGFW für AWS verwendet werden. Weitere Informationen finden Sie unter Integration von Identitätsanbietern von Drittanbietern über allgemeine Dienste verwalten *und* So aktivieren Sie einen Identitätsanbieter (IDP) von Drittanbietern.

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.

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.

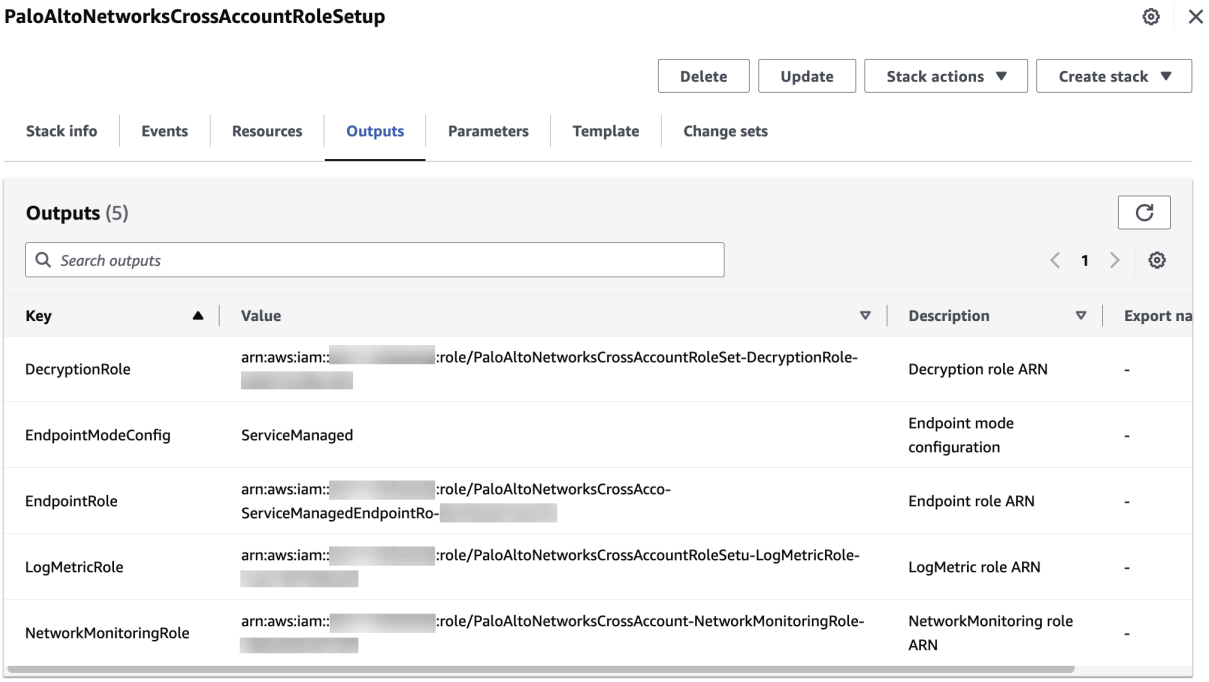
STEP 12 | Melden Sie sich bei Ihrem AWS-Konto an.

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.

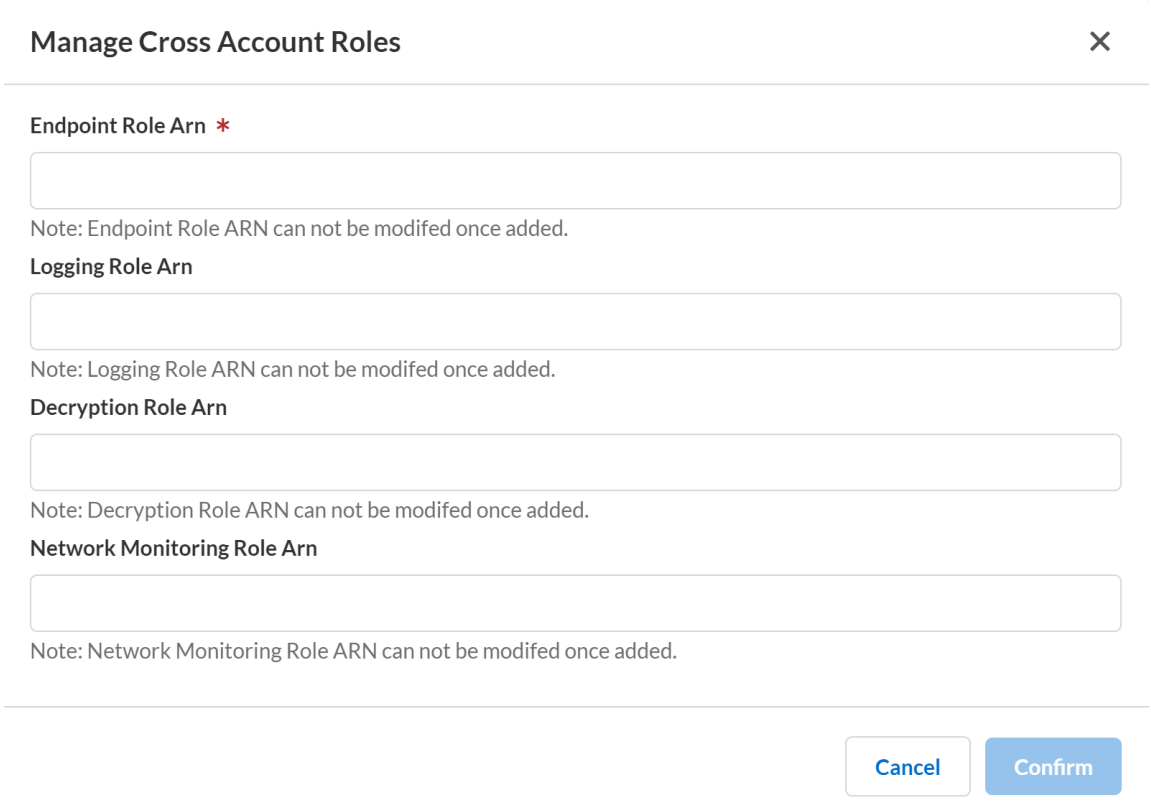
STEP 15 | Klicken Sie auf **Create Stack (Stapel erstellen)**.

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)**.



Erste Schritte mit einem AWS Firewall Manager-Konto

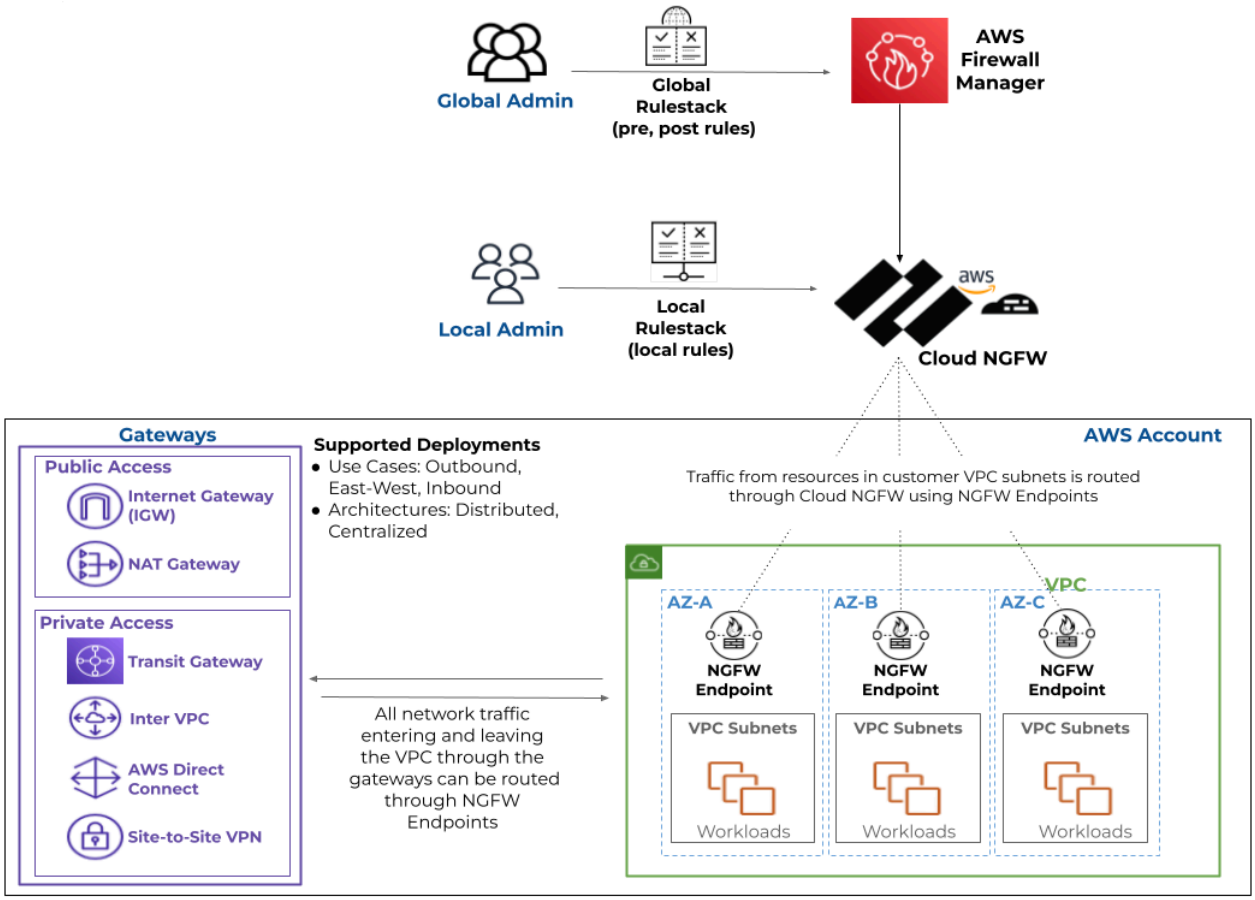
Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

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
- 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 | Abonnieren Sie den Cloud NGFW für AWS-Dienst, 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.

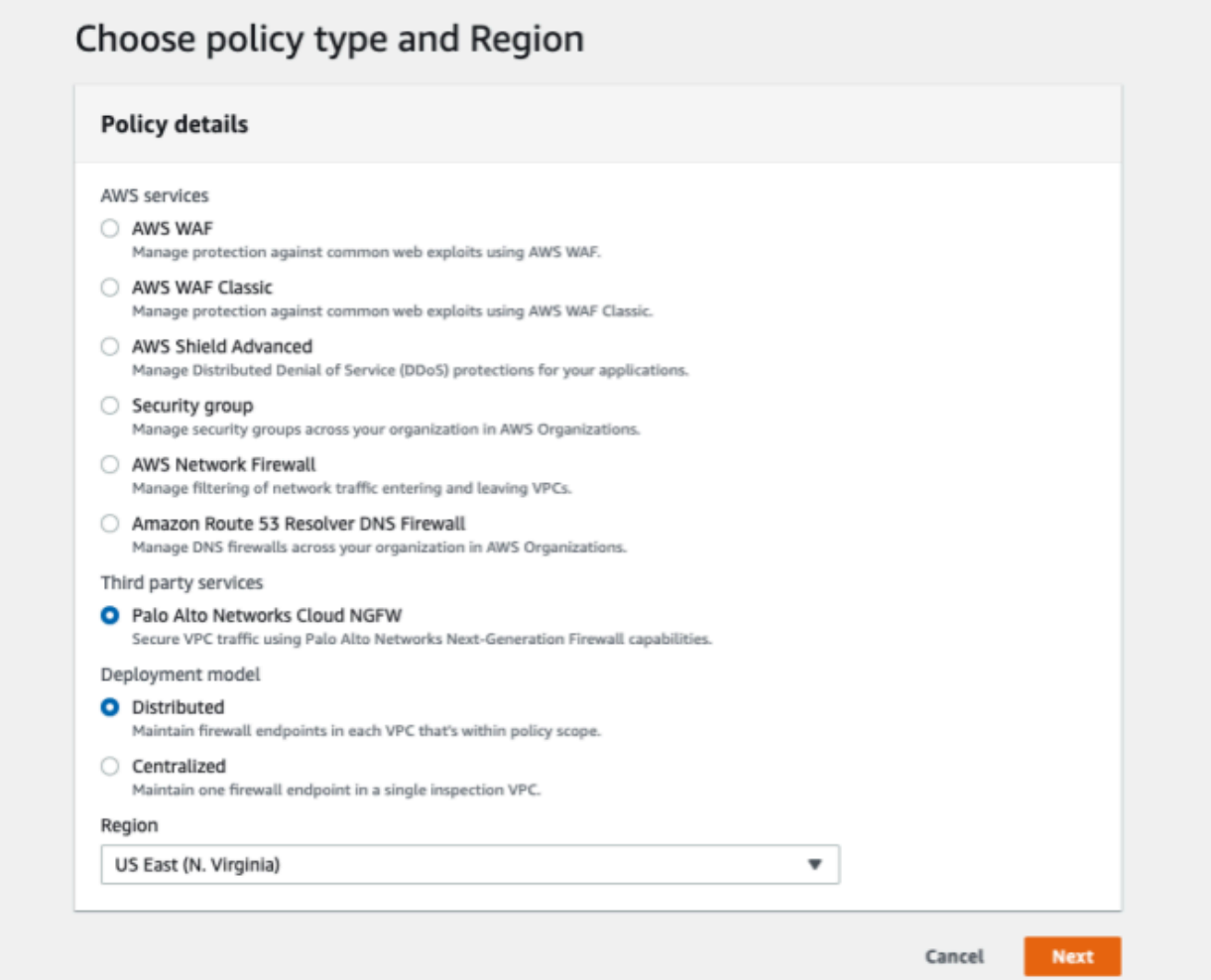
1. Melden Sie sich bei der AWS-Konsole an und wählen Sie **Dienste** > **AWS Firewall Manager** > **Einstellungen** aus.
2. Wählen Sie unter „Verknüpfungsstatus für Firewalls von Drittanbietern“ die Option „Palo Alto Networks Cloud NGFW“ aus.
3. Klicken Sie auf **Associate (Verknüpfen)**.

STEP 3 | Wählen Sie **Sicherheitsrichtlinien** > **Richtlinie erstellen** aus.

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

1. Wählen Sie unter „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 Regeln und Regelstapel.
3. Erstellen Sie einen globalen Regelstapel.

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

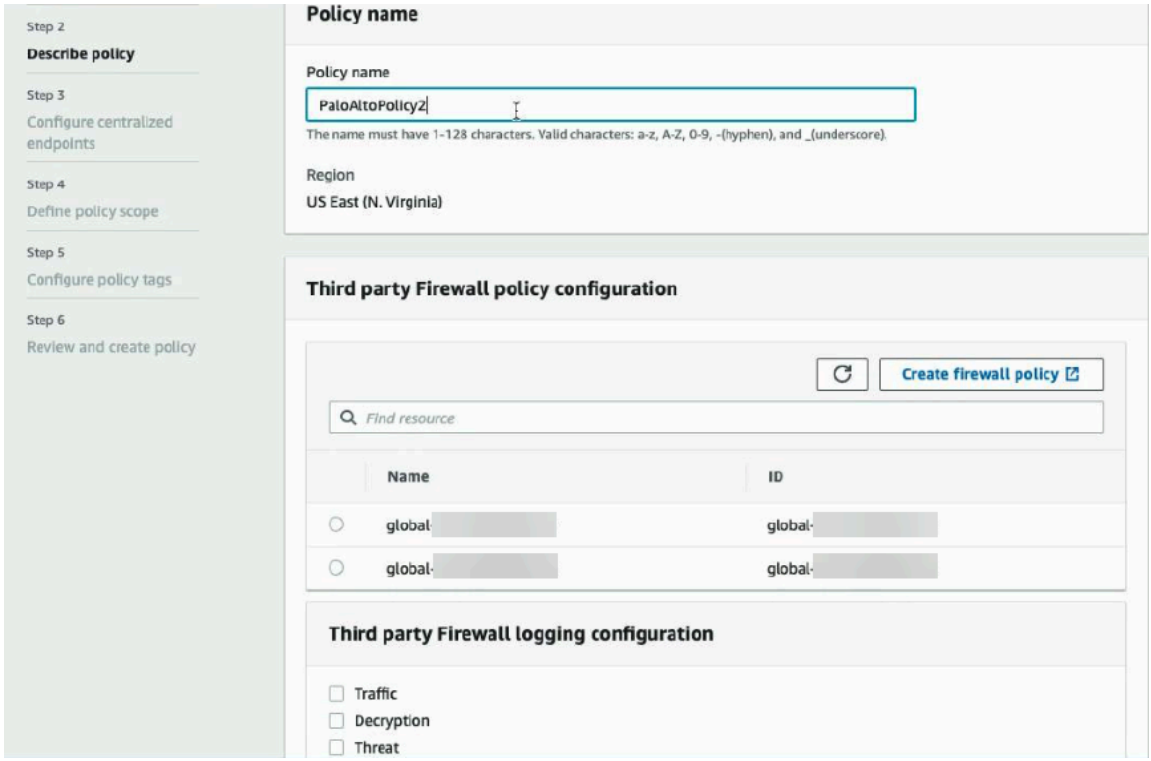
   2. (optional) Geben Sie eine **Beschreibung** für Ihren Regelstapel ein.

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

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

   Sie können **Datenverkehr**, **Entschlüsselung** und/oder **Bedrohungsprotokolle** 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).

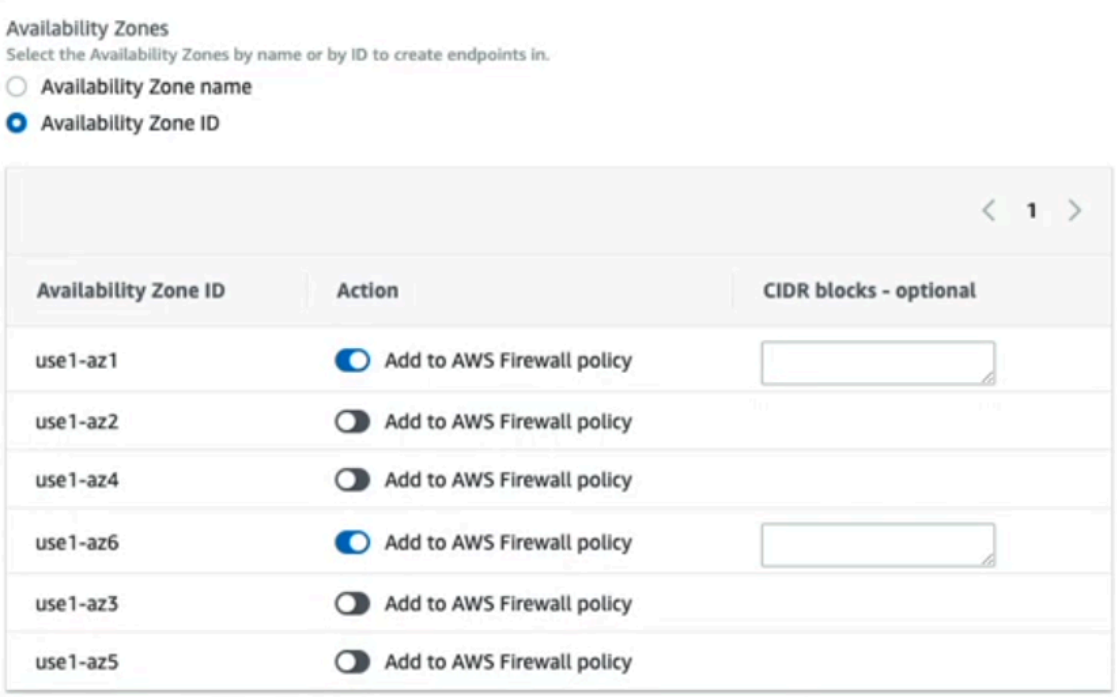
Sie wählen die NGFW-Endpunktstandorte aus, indem Sie Namen oder IDs von Verfügbarkeitszonen festlegen. Beachten Sie, dass die Namen der Verfügbarkeitszonen zwischen AWS-Konten

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-Richtlinienregeln für

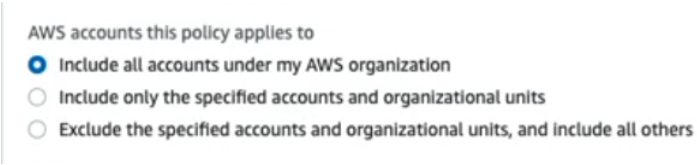
Cloud NGFW auf alle AWS-Konten und VPCs in Ihrer Organisation anwenden oder eine Teilmenge von Konten und/oder VPCs angeben.

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.

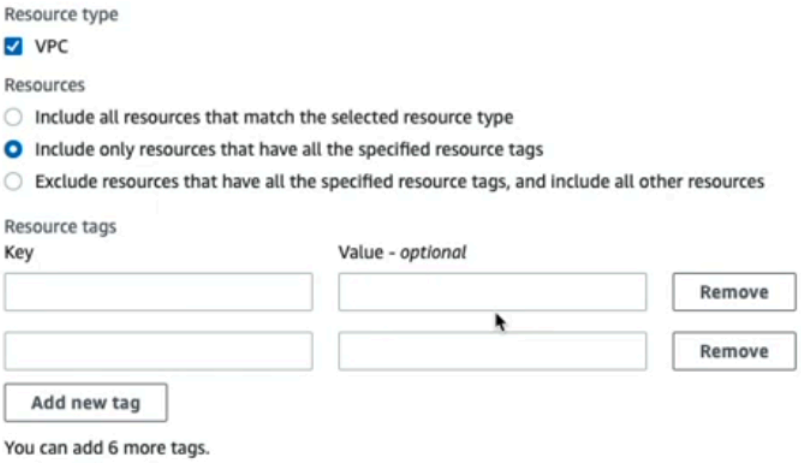
   

2. Geben Sie die VPC an, die in die FMS-Richtlinie für Cloud NGFW eingeschlossen oder ausgeschlossen werden soll.

   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-Ressourcen 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.

Kostenlose Testversion von Cloud NGFW für AWS

Wo kann ich das verwenden?	Was brauche ich?
• Cloud NGFW für AWS	❑ Cloud NGFW-Abonnement ❑ Konto beim Kunden-Support-Portal (CSP) von Palo Alto Networks ❑ AWS Marketplace-Konto ❑ Benutzerrolle (entweder Mandant oder Administrator)

Wenn Sie Cloud NGFW über AWS Marketplace abonnieren, werden Sie automatisch für eine kostenlose Testversion registriert. Navigieren Sie zur Seite **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 Ihre kostenlose Testversion aktiv mit Guthaben 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. Mögliche Aktionen:

- Integrieren Sie Ihre AWS-Konten in Ihre Mandanten.
- Erstellen Sie bis zu zwei NGFW-Ressourcen auf Ihren AWS-VPCs.
- Erstellen Sie Regelstapel.

Sobald 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. Erwägen 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.