paloalto TECHDOCS

Cloud NGFW für Azure

1.0

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

May 31, 2024

Table of Contents

Erste Schritte in Cloud NGFW für Azure

Cloud Next Generation-Firewall von Palo Alto Networks – ein nativer ISV-Dienst von Azure – ist eine ML-gestützte Next Generation-Firewall (NGFW), die von Palo Alto Networks als vollständig verwalteter Cloud-nativer Dienst auf der Microsoft Azure-Plattform bereitgestellt wird. 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.

Cloud NGFW für Azure

Cloud NGFW ist eine Firewall der nächsten Generation für maschinelles Lernen (ML), die als Cloud-nativer Service bereitgestellt wird. Mit Cloud NGFW können Sie mehrere Anwendungen sicher in Cloud-Geschwindigkeit ausführen und skalieren – mit einer echten Cloud-nativen Erfahrung. Cloud NGFW kombiniert erstklassige Netzwerksicherheit mit Benutzerfreundlichkeit, um einen vollständig verwalteten Cloud-nativen Service bereitzustellen. Sie erweitert die Bedrohungspräventionsfunktionen von Palo Alto Networks auf Cloud-Anbieter und ist gleichzeitig nativ in die verschiedenen Serviceangebote der Cloud-Anbieter integriert. Cloud NGFW:

- Minimiert die Verwaltung der Infrastruktur.
- Stoppt webbasierte Zero-Day-Bedrohungen in Echtzeit.
- Sichert Anwendungen, wenn sie sich mit legitimen webbasierten Diensten verbinden.
- Vereinfacht die Erfahrung mit nativen Cloud-Anbietern durch einfache, konsistente Firewall-Richtlinienverwaltung über mehrere Konten hinweg.
- Automatisiert End-to-End-Workflows mit Unterstützung für API, ARM-Vorlagen und Terraform.

Die Cloud NGFW stoppt webbasierte Angriffe, Schwachstellen, Exploits und andere bekannte Umgehungen, einschließlich ausgeklügelter dateibasierter Angriffe, mit einer patentierten Technologie zur Klassifizierung von App-ID-Datenverkehr. Cloud NGFW:

- Sichert den Datenverkehr beim Überschreiten von Vertrauensgrenzen (Trust Boundaries), z. B. Azure VNets und vWANs. Der von Cloud NGFW bereitgestellte verwaltete Service verhindert, dass Angreifer Zugriff auf Ressourcen erhalten, und stoppt Datenexfiltration und Command-and-Control-Datenverkehr (C2). Wurde entwickelt, um nicht autorisierte oder laterale Ost-West-Bewegungen zu stoppen.
- Unter Beachtung der Automatisierung entwickelt. Mit der Konfiguration von Regelstapeln und automatisierten Sicherheitsprofilen ist Cloud NGFW so konzipiert, dass es die Anforderungen an die Netzwerksicherheit mühelos erfüllt. Die Anwendung hat eine intuitive Benutzeroberfläche, die die Erstellung robuster Firewall-Ressourcen vereinfacht, die mit Ihrem Netzwerkverkehr skalieren.
- Enthält ein automatisiertes Cloud-Firewall-Modell, das dynamisch an Ihren Netzwerkverkehr angepasst wird und unvorhersehbare Durchsatzanforderungen mit Gateway Load Balancing (GWLB) für hohe Verfügbarkeit bei Bedarf und elastische Skalierung erfüllt. Sie können auf so viel oder so wenig Kapazität zugreifen, wie Sie benötigen, und nach Bedarf nach oben und unten skalieren.
- Integriert Sicherheit in Workflows, die von Cloud-Anbietern verwaltet werden. Mit Cloud NGFW, der ersten Firewall der nächsten Generation, die bei Cloud-Anbietern integriert werden kann, können Sie langwierige Bereitstellungszyklen vermeiden und schnell starten, selbst wenn Sie die erforderlichen Regelstapel und automatisierten Sicherheitsprofile einrichten. Sie können das Sicherheitsmodell des ausgewählten Cloud-Anbieters nutzen und gleichzeitig eine Integration in dessen Onboarding-, Überwachungs- und Protokollierungsfunktionen vornehmen. Cloud NGFW bietet einen einzigartigen Vorteil bei der Integration mit Cloud-Anbietern. Sie können die Vorteile der automatischen Skalierung und der hohen Verfügbarkeit ohne Wartungsaufwand nutzen. Diese Integration ermöglicht eine konsistente Verwaltung von Firewall-Richtlinien über mehrere Cloud-Anbieterkonten hinweg.

Sie können Cloud NGFW für Azure verwenden. Mit Cloud NGFW können Sie auf die wichtigsten NGFW-Funktionen wie App-ID, URL-Filterung basierend auf URL-Kategorien, Geolokalisierungen und SSL/TLS-Entschlüsselung zugreifen.

Unterstützte Funktionen

Cloud NGFW für Azure bietet die folgenden Funktionen:

- **Cloud-native Bereitstellung und Verwaltung**. Aktivieren Sie Firewallfunktionen der nächsten Generation in Ihrer Azure-Umgebung und verwalten Sie gleichzeitig Tag-0- und Tag-N-Vorgänge für Cloud NGFW-Ressourcen nahtlos, wie Sie es bei jedem anderen Azure-Dienst tun würden. Verwenden Sie für Berechtigungen die Azure role-based access control (RBAC), um Cloud NGFW-Ressourcen zu steuern.
- **Erweiterte Anwendungstransparenz und -kontrolle**. Cloud NGFW bietet erweiterte Anwendungserkennung und Zugriffskontrolle mithilfe von App-ID- und URL-Filtertechniken
- **Bedrohungsabwehr der nächsten Generation**. Die NGFW-Funktionen von Palo Alto Networks mit Cloud-basierten Sicherheitsdiensten und Signaturen zur Bedrohungsprävention werden für die gesamte physische und softwaremäßig installierte Basis bereitgestellt.

Das Modell „Cloud NGFW für Azure“

Die Cloud NGFW ist ein nativer ISV-Dienst von Azure. Dieser Ansatz ermöglicht es Palo Alto Networks, die FWaaS (Firewall-as-a-Service) zu entwickeln und zu verwalten, indem Hooks verwendet werden, die vom Azure-Dienst bereitgestellt werden, um FWaaS nativ über die Benutzeroberfläche und APIs von Azure zu nutzen. Die Cloud NGFW für Azure ist im Azure Marketplace verfügbar. Sie können alle Vorteile von NGFW von Palo Alto Networks für VNets und vWANs von Azure nutzen.

Cloud NGFW-Komponenten

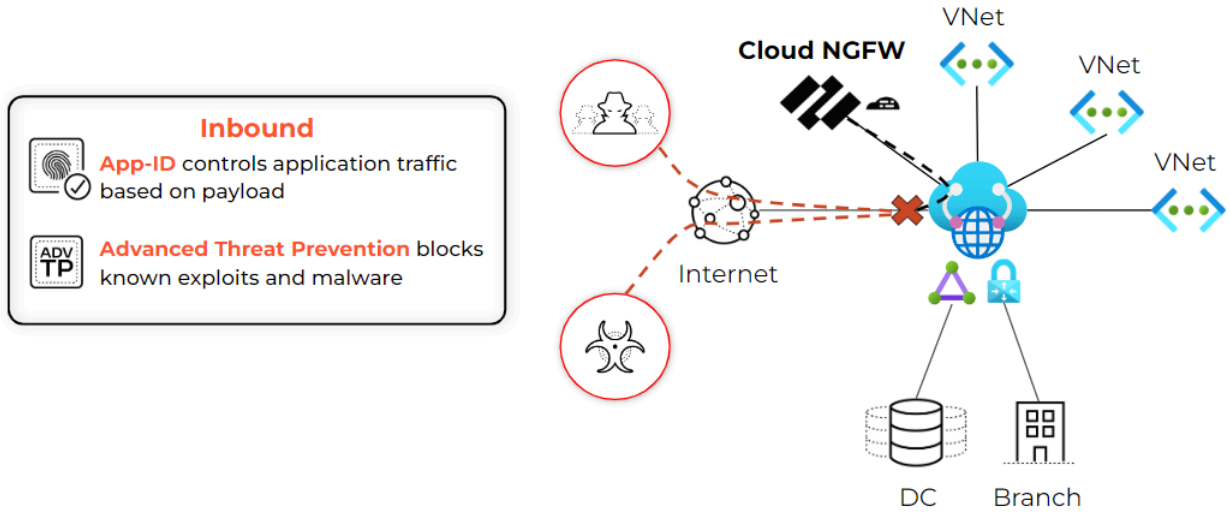
Die Cloud NGFW für Azure umfasst die folgenden Schlüsselkomponenten:

- **Die Cloud NGFW**. Die Cloud NGFW ist ein verwalteter regionaler Azure-Dienst, der in ausgewählten Azure-Regionen verfügbar ist.
- **NGFW**. Palo Alto Networks verwendet die NGFW als Ressource, die dem vNET- oder vWAN-Hub des Kunden zugeordnet ist. Sie bietet Ausfallsicherheit, Skalierbarkeit und Lebenszyklusmanagement. Die NGFW manifestiert sich als private IP-Adressen in dem vom Benutzer angegebenen NGFW-Subnetz. Um die NGFW-Ressource zu verwenden, aktualisieren Sie die benutzerdefinierten Routen (UDRs) des virtuellen Netzwerks (VNet), um Datenverkehr über die privaten IP-Adressen zu senden.
- **NGFW-Regelstapel**. Diese Ressource enthält eine Reihe von Sicherheitsregeln zusammen mit zugeordneten Objekten und Sicherheitsprofilen, um eine erweiterte Zugriffssteuerung mithilfe von App-ID- und URL-Filterung sowie Funktionen zur Bedrohungsprävention zu ermöglichen. Sie können einen lokalen Regelstapel mit einer oder mehreren NGFW verknüpfen.

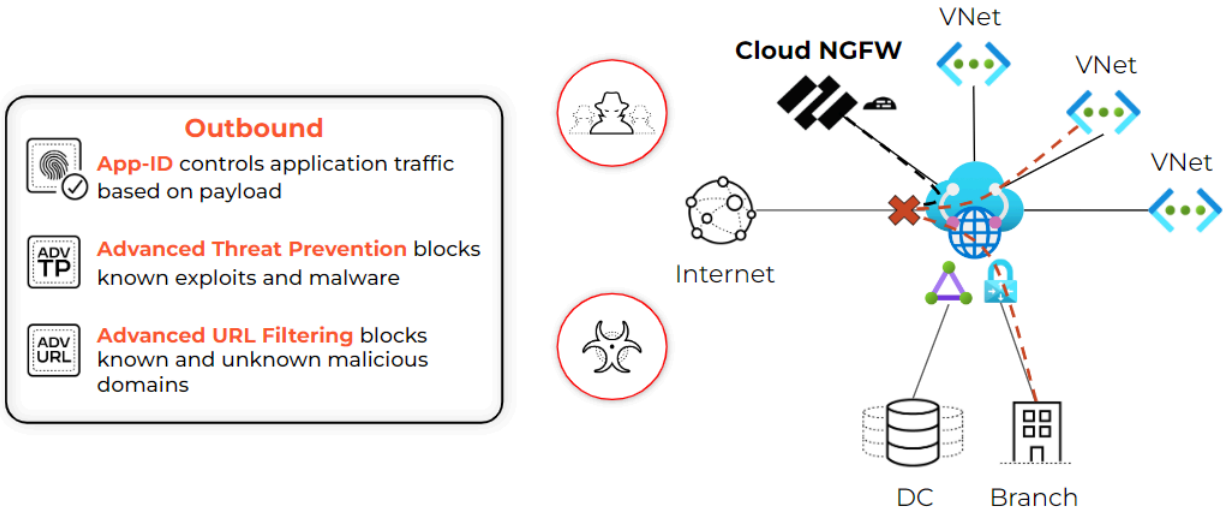
Sichern des Datenverkehrs mit der Cloud NGFW

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

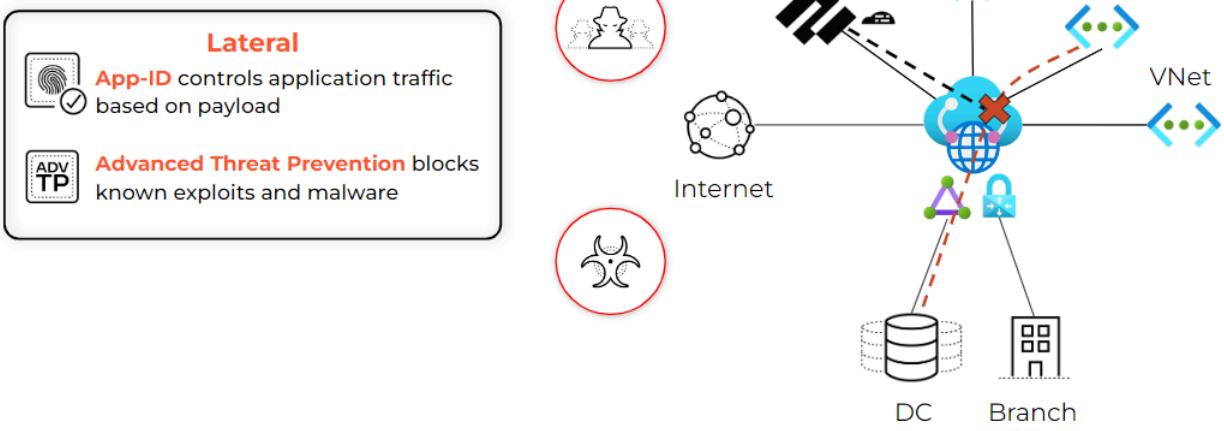
Eingehender Datenverkehr bezieht sich auf jeglichen Datenverkehr, der von außerhalb Ihrer Azure-Region stammt und für Ressourcen innerhalb Ihrer Anwendungs-VNets bestimmt ist, z. B. Server oder Load Balancer. Cloud NGFW kann verhindern, dass Malware und Sicherheitslücken im eingehenden Datenverkehr, der von Azure-Sicherheitsgruppen zugelassen wird, in Ihr VNet gelangen.



Ausgehender Datenverkehr bezieht sich auf Datenverkehr, der von Ihrem Anwendungs-VNet stammt und für Ziele außerhalb der Azure-Region bestimmt ist. Cloud NGFW schützt ausgehende Datenverkehrsflüsse, indem sichergestellt wird, dass Ressourcen in Ihrem Anwendungs-VNet eine Verbindung zu zulässigen Diensten und zulässigen URLs herstellen, und gleichzeitig die Exfiltration sensibler Daten und Informationen verhindert wird.



Ost-West-Datenverkehr wird innerhalb einer Azure-Region verschoben. Insbesondere der Datenverkehr zwischen Quelle und Ziel, der in zwei verschiedenen Anwendungs-VNets oder in zwei verschiedenen Subnetzen im selben VNet bereitgestellt wird. Cloud NGFW kann die Verbreitung von Malware in Ihrer Azure-Umgebung stoppen.



Cloud NGFW-Komponenten

Cloud NGFW für Azure erstellt eine Reihe von Komponenten, die zusammen Ihre Azure-Umgebung sichern:

- Die **Cloud NGFW-Ressource** (oder einfach NGFW) ist Ihrem VNet- oder vWAN-Hub zugeordnet und kann sich über mehrere Verfügbarkeitszonen erstrecken. Diese Ressource verfügt über integrierte Ausfallsicherheit, Skalierbarkeit und Lebenszyklusverwaltung.
- **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.

Unterstützte Regionen in Cloud NGFW für Azure

Eine Azure-Region unterstützt bis zu drei Verfügbarkeitszonen, wobei in jeder Zone nur eine zugewiesene VM erforderlich ist. Der Datenverkehr in jeder Zone nutzt ein VNet, wodurch zonenübergreifende Gebühren entfallen. Die folgende Tabelle zeigt die Verfügbarkeit der Zone für eine bestimmte Region an.

Regionsname	Regionscode
Australien Ost	australiaeast
Australien Südost	australiasoutheast
Brasilien Süd	brazilsouth
Kanada (zentral)	canadacentral
Kanada Ost	canadaeast
Zentralindien	centralindia
Zentral US	centralus
Ostasien	eastasia
Ost US	eastus
Ost US 2	eastus2
Frankreich Zentral	francecentral
Deutschland West Zentral	germanywestcentral
Israel Zentral	israelcentral
Italien Nord (Mailand)	italynorth
Japan Ost	japaneast
Japan West	japanwest
Nord Zentral US	northcentralus
Nordeuropa	northeurope
Norwegen Ost	norwayeast
Südafrika Nord (Johannesburg)	southafricanorth

Regionsname	Regionscode
Süd Zentral US	southcentralus
Südostasien	southeastasia
Schweden Zentral (Gävle)	swedencentral
Schweiz Nord	switzerlandnorth
VAE Nord (Dubai)	uaenorth
UK Süd	uksouth
UK West	ukwest
Westeuropa	westeurope
West Zentral US (Wyoming)	westcentralus
West US	westus
West US 2	westus2
West US 3	westus3

Grenzwerte und Kontingente in Cloud NGFW für Azure

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

Verwenden Sie den Cloud NGFW for Azure pricing estimator, um die Azure-Limits und -Kontingente für Ihr Cloud NGFW-Abonnement zu bestimmen.

Richtlinienverwaltung lokale Regelstapel

Name	Standardgrenzwerte pro Cloud NGFW-Mandant
Anzahl der Cloudkonten (Azure) in einem Mandanten	200

Native Richtlinienverwaltung (Regelstapel)

Attribut	Maximales Limit 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
Intelligente Feeds (einschließlich der fünf vordefinierten Feeds)	30
IP-Adressen in allen Feeds	50.000
Zertifikatobjekte	100

Panorama-Richtlinienverwaltung

Attribut	Maximales Limit pro Cloud NGFW-Ressource*
Richtlinien	
Sicherheitsregeln	10.000
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
URL Filtering	
Gesamtzahl der Entitäten für Zulassungsliste, Sperrliste und benutzerdefinierte Kategorien	25.000
Maximale Anzahl benutzerdefinierter Kategorien	500

*Die angegebenen Limits 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 Azure-Leistung

Die folgende Tabelle enthält Leistungsinformationen für Ihre Cloud NGFW für Azure-Mandanten.

Die in der folgenden Tabelle bereitgestellten Informationen gehen von maximal 40 Instanzen aus.

Attribut	Leistungsmetrik
Firewall-Durchsatz (App-ID aktiviert)	Maximaler Durchsatz: 100 Gbit/s; pro Instanz 2,92 Gbit/s Kaltstart: 8,55 Gbit/s *Bei Kaltstart-Datenverkehr ist die Erkennung von Inhaltsbedrohungen aktiviert. Ohne Inhaltsbedrohungsschutz ist jede Firewall-Instanz aufgrund des Instanztyps auf 3,00 Gbit/s begrenzt. Dies ist eine Beschränkung von Azure.*
Durchsatz Bedrohungsschutz	Maximaler Durchsatz: 92 Gbit/s; pro Instanz 2,31 Gbit/s
Durchsatz verschlüsselter Datenverkehr	44 Gbit/s (mit Inhaltsbedrohungsschutz); pro Instanz 1,11 Gbit/s 60 Gbit/s (ohne Inhaltsbedrohungsschutz); pro Instanz 1,52 Gbit/s

Preise für Cloud NGFW für Azure

Cloud NGFW ist als Pay-as-you-go (PAYG)-Abonnement im Azure Marketplace verfügbar. Bei diesem Modell zahlen Sie nur für die Dienste, die Sie jeden Monat nutzen. Sie profitieren außerdem von Azure Marketplace-Vorteilen, z. B. konsolidierter Abrechnung und Gutschrift für das Microsoft Azure Consumption Commitment (MACC) einer Organisation.

Cloud NGFW für Azure rechnet den Verbrauch über den Azure Marketplace-Messdienst ab. Das Modell bietet Preisflexibilität basierend auf den Bereitstellungsstunden aller Cloud NGFWs, dem Gesamtvolumen des verarbeiteten Datenverkehrs und den verwendeten Sicherheitsfunktionen. Die Abrechnung für die **NGFW-Basisressource** erfolgt anhand folgender Dimensionen und Einheiten:

Dimension	Preis	Äquivalente Cloud NGFW-Credits
Grundlegende NGFW-Ressourcennutzung	1,50 USD pro Bereitstellungsstunde	125
Gesicherter Datenverkehr (erste 15 TB/Monat) pro Mandant	0,065 USD pro verarbeitetem 1 GB	5,416666667
Gesicherter Datenverkehr (folgende 15 TB/Monat) pro Mandant	0,045 USD pro verarbeitetem 1 GB	3,75
Gesicherter Datenverkehr (über 30 TB/Monat) pro Mandant	0,030 USD pro verarbeitetem 1 GB	2,5
Add-ons	0,12 USD pro 10 Einheiten	Weiter unten finden Sie spezifische Abrechnungsinformationen für jedes Add-on.
Gebühren für Azure-Netzwerk	0,01 USD pro verarbeitetem 1 GB	

Cloud NGFW für Azure berechnet die ausgehende Nutzung (eingehender, ausgehender und Ost-West-Datenverkehr) mittels Gebührendimension des Azure-Netzwerks. Dann werden die Verbrauchsdetails für den Azure Marketplace freigegeben. Die Preise für virtuelle Azure-Netzwerke bestimmen diese Gebühren. Weitere Informationen finden Sie unter Preise für virtuelle Netzwerke.

Erweiterter Bedrohungsschutz, erweiterte URL-Filterung, erweiterte Add-ons für Wildfire

Die Abrechnung der Nutzung dieser Sicherheitsdienste erfolgt über die **Add-ons-Dimension**. Die Nutzung wird in $/Stunde und $/GB gemessen, wie in der folgenden Tabelle beschrieben.

Gesicherter Datenverkehr	Preis pro Stunde	Preis pro GB	Äquivalente Cloud NGFW-Credits
Nutzungsstunde	0,450 USD	-	37,5
Erste 15 TB/Monat		0,020 USD	1,6
Folgende 15 TB/Monat		0,014 USD	1,125
Über 30 TB/Monat		0,009 USD	0,75

WildFire- und DNS-Sicherheits-Add-ons

Die Abrechnung der Nutzung dieser Sicherheitsdienste erfolgt über die **Add-ons-Dimension**. Die Nutzung wird in $/Stunde und $/GB gemessen, wie in der folgenden Tabelle beschrieben.

Gesicherter Datenverkehr	Preis pro Stunde	Preis pro GB	Äquivalente Cloud NGFW-Credits
Nutzungsstunde	0,300 USD	-	25
Erste 15 TB/Monat		0,013 USD	1,083333333
Folgende 15 TB/Monat		0,009 USD	0,75
Über 30 TB/Monat		0,006 USD	0,5

Panorama Add-on für zentralisierte Verwaltung

Die Abrechnung der Nutzung dieses Sicherheitsdienstes erfolgt über die **Add-ons-Dimension**. Die Nutzung wird in $/Stunde und $/GB gemessen, wie in der folgenden Tabelle beschrieben.

Gesicherter Datenverkehr	Preis pro Stunde	Preis pro GB	Äquivalente Cloud NGFW-Credits
Nutzungsstunde	0,300 USD	-	25
Erste 15 TB/Monat		0,003 USD	0,2166666667
Folgende 15 TB/Monat		0,002 USD	0,15
Über 30 TB/Monat		0,001 USD	0,1

Gebühren für Azure-Netzwerk

Für Palo Alto Networks fallen die VNet-Peering-Kosten an, die mit den Netzwerkschnittstellen verbunden sind, die zum Bereitstellen der Cloud NGFW-Ressource im Abonnement des Kunden verwendet

werden. Diese Kosten werden auf der Grundlage der Preise für das Peering virtueller Azure-Netzwerke weitergegeben.

Sichtbarkeit von Verbrauch und Nutzung von Credits

Sie können jetzt NGFW-Credits für die Nutzung von Cloud NGFW für langfristige Verträge verwenden, die Sie für Ihre Firewallressourcen in Azure-Cloudumgebungen auf Mandantenebene zuweisen können. Sie können Cloud NGFW-Credits über die standardmäßigen Vertriebskanäle und -prozesse von Palo Alto Networks erwerben.

Sie benötigen ein PAYG-Abonnement, um Credits zu abonnieren. Wenden Sie sich an Ihr Vertriebsteam, um weitere Informationen zu erhalten.

Beachten Sie Folgendes:

- Der Credit-Pool hat eine Start- und eine Endzeit. Die Einheit des Werts ist Credit/Stunde (auch als „Kapazität“ bezeichnet).
- Die Kapazität wird auf der Grundlage der Kombination von Diensten und der Menge des im Laufe der Zeit verarbeiteten Datenverkehrs (z. B. pro Stunde) berechnet.
- Um das erforderliche Guthaben für die Cloud NGFW-Firewall in Azure zu schätzen, verwenden Sie den Preisschätzer für Cloud NGFW für Azure. Der Schätzer gibt die Anzahl der Credits an, die für die Menge der eingegebenen Ressourcen, Dienste und des eingegebenen Datenverkehrs erforderlich sind. Der Credit-zu-Dollar-Betrag wird ebenfalls angezeigt.
- Nachdem die Credits erworben und beansprucht wurden, werden sie dem Azure-Konto auf Mandantenebene hinzugefügt:
  - Alle Ressourcen, die im Mandanten bereitgestellt werden, nutzen/verbrauchen Credits aus demselben Pool.
  - Wenn die Nutzung den zugewiesenen Creditbetrag übersteigt, wird die Überschreitung als PAYG (Standardzahlungsmethode) berechnet.
  - Diese Gebühren werden als Gebühr für Marketplace-Partner auf der monatlichen Azure-Rechnung ausgewiesen.

Wenn Sie sich für *x* Kapazität, dann *x * 24 (Stunden) * 30 (Anzahl der Tage in einem Monat)* angemeldet haben, wird die Anzahl der Credits Ihrem Konto jeden Monat in Ihrem Credit-Topf hinzugefügt. Die Credits werden entsprechend Ihrer Nutzung für den Monat bis zum Enddatum des Vertrags vom Credit-Topf abgezogen. Sie können die Kapazität von Credits über Ihren Vertriebskanal erhöhen. Nach Ablauf der Credits können Sie die Credits für eine andere Kapazität und ein anderes Enddatum erneuern.

So beanspruchen Sie Credits

Sie benötigen die Seriennummer des Cloud NGFW-Produkts und die Supportkonto-ID des CSP (Customer Support Portal von Palo Alto Networks), um die Credits zu beanspruchen. Die Seriennummer des Cloud NGFW-Produkts kann auf zwei Arten generiert werden:

- Erstellen Sie eine Firewall.
- Erstellen Sie einen Regelstapel.

Sie können dann ein neues serielles CSP-Konto mit der Produktseriennummer (CSP-Seriennummer des Mandanten) erstellen oder ein vorhandenes CSP-Konto mit dem Link *Register your Azure tenant to a new or existing Palo Alto Networks support account* im Abschnitt „New Support Request“ verknüpfen.

Nachdem Sie einen Mandanten registriert haben, können Sie ihn 30 Tage lang als kostenlose Testversion verwenden. Wenn Sie die kostenlosen Credits vor Ablauf der 30-tägigen Testversion verbraucht haben, wird die zusätzliche Nutzung zu PAYG-Tarifen berechnet.

Wenn Sie Cloud NGFW-Credits während eines kostenlosen Testzeitraums hinzufügen, beginnt Ihr Vertrag sofort und setzt die kostenlose Testversion außer Kraft.

Sie können Ihre Informationen zur Creditnutzung im Abschnitt **New Support request** im Azure Marketplace überprüfen.

Wenn Ihr durchschnittlicher Verbrauch pro Monat die gekauften Credits übersteigt, werden Überschreitungen zu den PAYG-Tarifen berechnet.

Die Credits werden am ersten Tag jedes Monats zurückgesetzt. Wenn Ihre Credits ablaufen, wird Ihr Konto auf die PAYG-Tarife zurückgesetzt. Ungenutzte Credits werden nicht auf den nächsten Monat übertragen. Verwenden Sie die Schaltfläche Cloud NGFW for Azure pricing estimator*, um bei der Ermittlung der Azure-Preise für Ihren Cloud NGFW-Mandanten unterstützt zu werden.*

Kostenlose Testversion von Cloud NGFW für Azure

Wenn Sie die erste Cloud NGFW oder den ersten Regelstapel in Ihrem Azure AD-Mandanten erstellen, werden Sie automatisch für eine kostenlose 30-Tage-Testversion registriert. Die kostenlose Testphase beginnt mit der Erstellung Ihrer ersten Cloud NGFW für die Azure-Ressource.

Die kostenlose Testversion gilt für alle Abonnements im Azure AD-Mandanten.

Während der kostenlosen Testphase können Sie Folgendes kostenlos nutzen:

- Zwei Cloud NGFW-Ressourcen
- Insgesamt 1 TB an geprüftem Datenverkehr (durchschnittlich 500 GB pro Cloud NGFW-Ressource)
- Panorama-Integration
- Die Bedrohungsabwehr (Threat Prevention) und die URL-Filterung durch in der Cloud bereitgestellte Sicherheitsdienste (CDSS, Cloud-Delivered Security Services) sind aktiviert

Wenn der kostenlose Testzeitraum endet oder Ihre Nutzung die Grenzen der kostenlosen Testversion überschreitet, fallen Gebühren an, die auf den Bedingungen basieren, die in der Abonnementliste für **Palo Alto Networks Cloud NGFW Pay-As-You-Go** im Azure Marketplace beschrieben sind. Beachten Sie bei der Nutzung der kostenlosen Testversion Folgendes:

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

Mit Cloud NGFW für Azure starten

Sie registrieren zunächst Palo Alto Networks als **Resource Provider**. Wählen Sie in der Azure-Konsole im Abschnitt **Settings** die Option **Resource providers** aus. Suchen Sie nach „Palo Alto Networks Cloud NGFW“ und wählen Sie **PaloAltoNetworksCloudngfw** aus. Klicken Sie dann auf **Register**.

Anschließend melden Sie sich beim Azure-Portal an, um Cloud NGFWs und die zugehörigen Richtlinienregeln zu erstellen. Wenn Sie eine NGFW erstellen, geben Sie die Azure VNets oder vWANs und die Subnetze an, die Sie sichern müssen. Nach dem Erstellen der NGFW müssen Sie die Routing-Tabellen für Ihre Gateways und Subnetze aktualisieren, um den gesamten Datenverkehr zur Prüfung an die NGFW weiterzuleiten.

Cloud NGFW-Rollen für Azure-Benutzer 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. Die hier bereitgestellten Informationen sind hilfreich für die Erstellung benutzerdefinierter Rollen, beispielsweise für die Erstellung eines Firewall-Benutzers mit Lesezugriff. Standardmäßig erfordert Cloud NGFW Eigentümer- oder Mitwirkendenrollen für das Abonnement, um den Ressourcenanbieter zu abonnieren und die Cloud NGFW-Ressource zu verwenden.

Informationen zum Verwalten von Cloud NGFW-Rollen finden Sie unter Zuweisen von Azure-Rollen über das Azure-Portal.

Single Sign-on integrieren

Sie können den SSO-Anmeldefluss Ihres Unternehmens mit Ihrem Palo Alto Networks Customer Support Portal-Konto in Ihr Azure Cloud NGFW-Abonnement integrieren.

Identitätsanbieter (IDP, Identity Provider) von Drittanbietern aktivieren

Durch die Aktivierung eines Identitätsanbieters (IDP) von Drittanbietern im Customer Support Portal (CSP) können Sie sich mit Ihren eigenen Unternehmensanmeldedaten im Palo Alto Networks Customer Support Portal (CSP) anmelden. Da IDP auf Domänenebene eingerichtet werden, können sich Mitglieder innerhalb der Domäne mit SSO-Anmeldeinformationen für Unternehmen bei mehreren CSP-Konten anmelden. Bei *Domänenadministratorkonten* müssen jedoch weiterhin die Anmeldeinformationen von Palo Alto Networks verwendet werden.

So aktivieren Sie IDP von Drittanbietern für Ihre Domäne:

- Sie müssen im CSP über die Domänenadministratorrolle verfügen, um den IDP-Zugriff von Drittanbietern für Ihr Konto zu konfigurieren.
- Sie müssen Administratorzugriff auf den Identitätsanbieter haben, um die von Palo Alto Networks bereitgestellten SSO-Konfigurationsdetails aktualisieren zu können.
- Zur Verifizierung benötigen Sie ein Nicht-Domänen-Administratorkonto.

STEP 1 | Melden Sie sich im Azure Portal an und suchen Sie nach **Active Directory**.

STEP 2 | Wählen Sie in Active Directory **Enterprise Application** und **New Application** aus.

STEP 3 | Geben Sie den Namen für Ihre SSO-Anwendung ein (z. B. „panorama-sso“) und klicken Sie auf **Create**.

STEP 4 | Wählen Sie im Fenster **Create your own application** die Option **Integrate any other application you don't find in the gallery (Non-gallery)** aus.

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

STEP 6 | Klicken Sie im Abschnitt **Manage** auf **Single sign-on**.

STEP 7 | Wählen Sie die Single Sign-On-Methode **SAML** aus. Die SAML-basierte Anmeldeseite enthält Informationen, die Sie benötigen, um Ihre neue SSO-Unternehmensanwendung mit Ihrem Palo Alto Networks CSP-Konto zu verknüpfen.

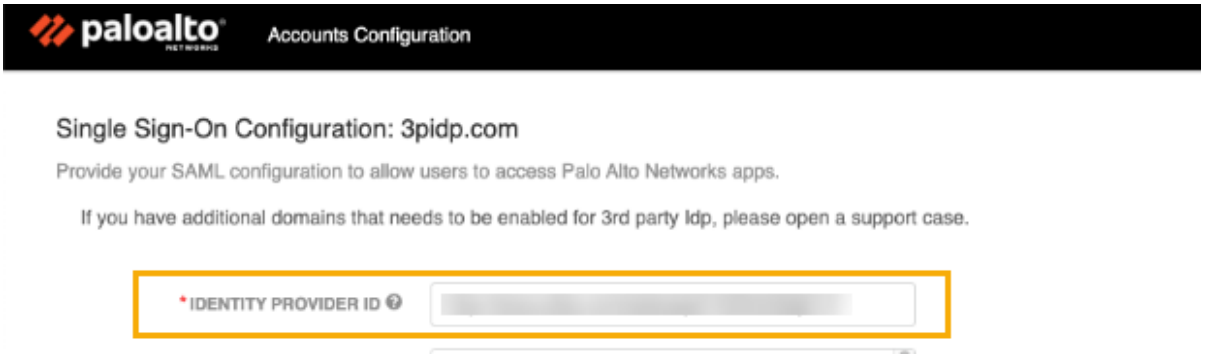
STEP 8 | Scrollen Sie auf der SAML-basierten Anmeldeseite nach unten, um URLs im Abschnitt **Set up [your SSO application name]** zu finden. Kopieren Sie die **Azure AD Identifier**.

STEP 9 | Melden Sie sich beim CSP an.

STEP 10 | Wählen Sie im CSP **Account Management > Account Details** aus.

STEP 11 | Klicken Sie im Abschnitt **SSO** auf **View Single Sign-On settings for your domain**.

STEP 12 | Fügen Sie unter **Accounts Configuration** die kopierte **Azure AD identifier** aus Schritt 8 in das Feld **Identifier Provider ID** ein.



STEP 13 | Kehren Sie zum **SAML-basierten Anmeldebildschirm** im Azure-Portal zurück. Scrollen Sie nach unten, um URLs im Abschnitt **Set up [your SSO application name]** zu finden. Kopieren Sie die **Login URL**.

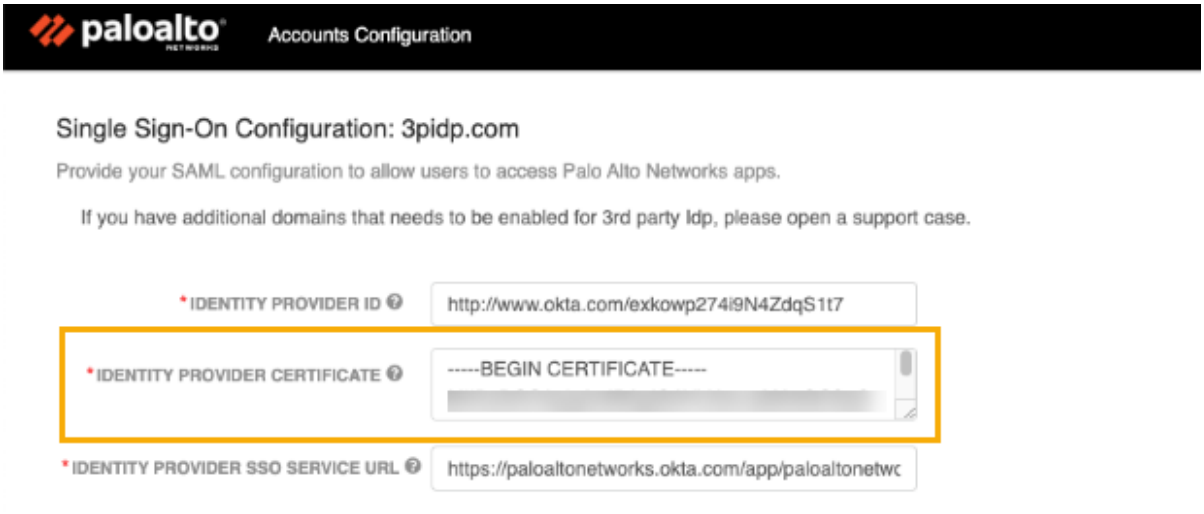
STEP 14 | Kehren Sie zur Seite **Accounts Configuration** im CSP zurück. Fügen Sie die kopierte **Login URL** (aus dem vorherigen Schritt) in das Feld **Identity Provider SSO Service URL** ein.

STEP 15 | Verwenden Sie dieselbe **Identity Provider SSO Service URL**-Adresse für das Feld **Identity Provider Destination URL**.

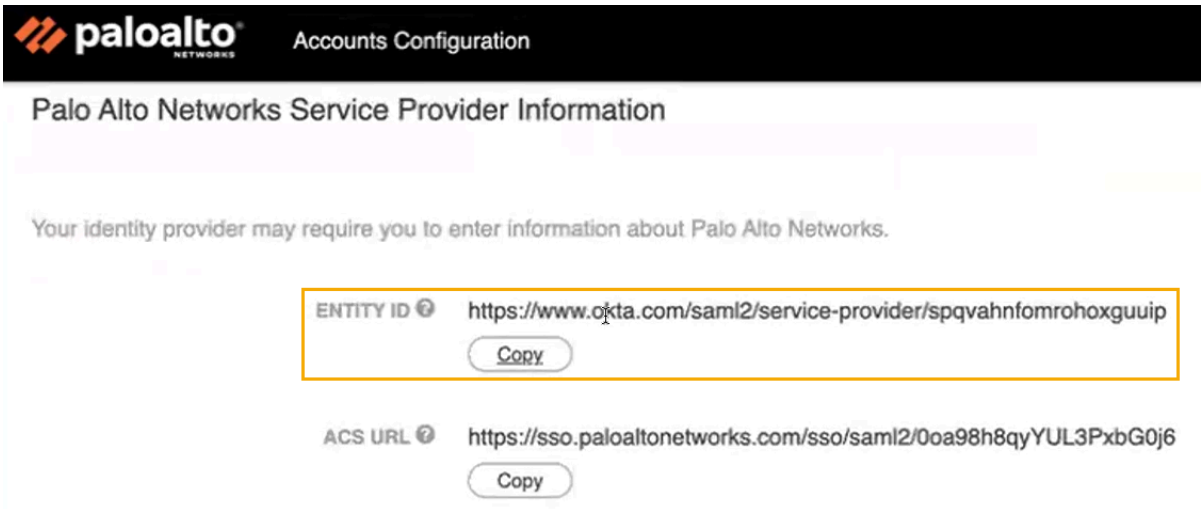
STEP 16 | Kehren Sie zum **SAML-basierten Anmeldebildschirm** im Azure-Portal zurück. Scrollen Sie nach unten, um den Abschnitt **SAML Certificates** zu finden.

STEP 17 | Laden Sie im Abschnitt „SAML Certificates“ das **Certificate (Base64)** herunter.

STEP 18 | Kehren Sie im CSP zur Seite **Account Management > Account Details** zurück. Fügen Sie das heruntergeladene Zertifikat (aus dem vorherigen Schritt) in das Feld **Identity Provider Certificate** ein.



STEP 19 | Die Seite **Accounts Configuration** ändert sich, um **Palo Alto-Dienstanbieterinformationen** anzuzeigen. Kopieren Sie die URL der **Entity ID**.



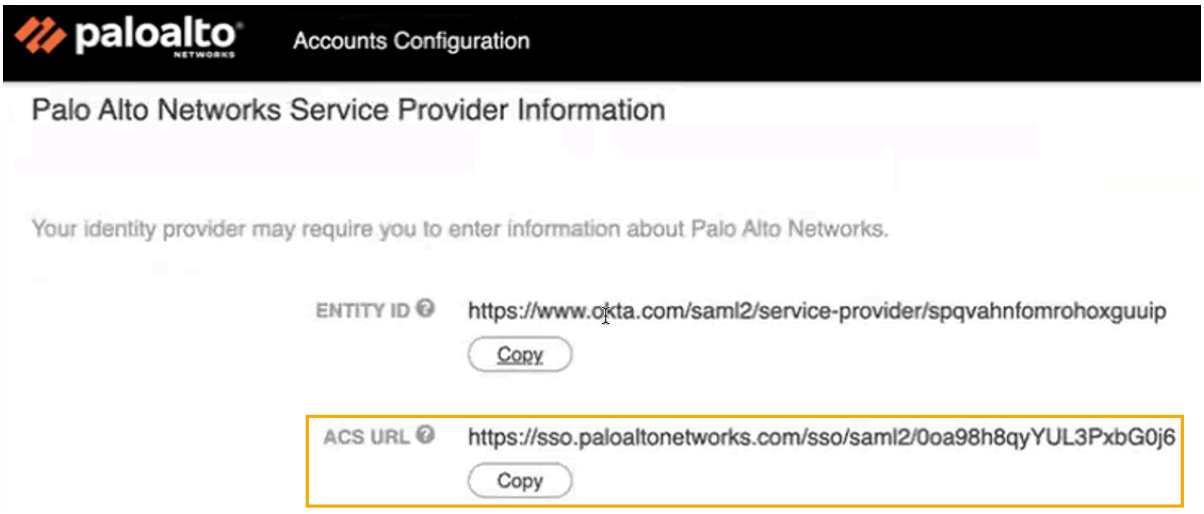
STEP 20 | Kehren Sie zum **SAML-basierten Anmeldebildschirm** im Azure-Portal zurück.

STEP 21 | Klicken Sie im Bildschirm **Basic SAML Configuration** auf **Edit**.

STEP 22 | Klicken Sie im Feld **Identifier (Entity ID)** auf **Add Identifier**.

STEP 23 | Fügen Sie die Palo Alto Networks **Entitäts-ID** (ab Schritt 21) in das Feld **Identifier** ein.

STEP 24 | Kehren Sie im CSP zur Seite **Account Management > Account Details** zurück. Kopieren Sie die **ACS-URL**.



STEP 25 | Kehren Sie zum **SAML-basierten Anmeldebildschirm** im Azure-Portal zurück.

STEP 26 | Klicken Sie im Bildschirm **Basic SAML Configuration** auf **Edit**.

STEP 27 | Geben Sie die ACS-URL (kopiert aus Schritt 24) in die **Reply URL (Assertion Consumer Service URL)** ein.

STEP 28 | Kehren Sie zur Seite **Accounts Configuration** im CSP zurück. Verwenden Sie die Umschalttaste, um **Identitätsanbieter zu aktivieren**.

STEP 29 | Klicken Sie auf **Save (Speichern)**.

STEP 30 | Kehren Sie zum Azure-Portal zurück. Klicken Sie im Abschnitt **Manage** Ihrer SSO-Anwendung auf **Users and groups**.

STEP 31 | Verwenden Sie die Option **Add user/group**, um die Verwendung des SSO-Logins für jeden angegebenen Benutzer zu aktivieren.

SSO-Login verifizieren

Nach Aktivierung des Identitätsanbieters müssen sich alle Benutzer (außer Domänenadministratoren) mit SSO anmelden. So überprüfen Sie, ob die SSO-Anmeldung ordnungsgemäß eingerichtet ist:

- Geben Sie auf der Anmeldeseite eine E-Mail-Adresse an. Verwenden Sie keine Anmeldeinformationen für Domänenadministratoren.
- Überprüfen Sie, ob Sie zur Authentifizierung an die IDP-Anmeldeseite weitergeleitet werden.
- Nach der Authentifizierung erscheint die Palo Alto Networks Customer Support Portal-Seite.

Integration von SSO mit CSP für Nicht-Domänenbenutzer mit Azure Marketplace

So integrieren Sie einen Benutzer mit einem CSP-Konto mithilfe von Azure Marketplace:

STEP 1 | Melden Sie sich bei Ihrem Azure-Konto an.

STEP 2 | Wählen Sie in **Azure Services Cloud NGFWs by Palo Alto Networks** aus.

STEP 3 | Wählen Sie die Firewall aus, die Sie in Ihr CSP-Konto integrieren möchten.

STEP 4 | Klicken Sie im Abschnitt **Support + Troubleshooting** auf **New Support Request**. Der Support-Bildschirm von Palo Alto Networks wird mit der **Mandanten-ID** und der **Seriennummer des Produkts** angezeigt.

STEP 5 | Klicken Sie auf **Register User account and create a case at Customer Support Portal**.

STEP 6 | Geben Sie auf der Seite **Create New Account / Use Existing Account** Ihre E-Mail-Adresse ein und schließen Sie die Authentifizierungsschritte ab. Klicken Sie dann auf **Next**.

STEP 7 | Wählen Sie im Abschnitt **Device Registration** das **Cloud Marketplace**-Abonnement aus dem Drop-down-Menü aus. Zum Beispiel *Azure Cloud NGFW*.

STEP 8 | Geben Sie die **Mandanten-ID** und **Seriennummer** für Ihr Azure Marketplace-Abonnement ein. Sie können diese Informationen von der Palo Alto Support-Seite aus Schritt 4 kopieren. Klicken Sie auf **Next (Weiter)**.

STEP 9 | Geben Sie den **Authentifizierungscode** ein, der an Ihre E-Mail-Adresse gesendet wurde. Klicken Sie auf **Next (Weiter)**.

STEP 10 | Nach der Authentifizierung mit SSO erscheint die CSP-Anmeldeseite. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Next**.

Integration von SSO mit CSP für Domänenbenutzer mit Azure Marketplace

Um einen *Domänenbenutzer* mit einem CSP-Konto über Azure Marketplace zu integrieren, benötigen Sie Ihre Palo Alto Networks-Anmeldeinformationen:

STEP 1 | Melden Sie sich mit den *Domänenbenutzer-Anmeldeinformationen* bei Ihrem Azure-Konto an.

STEP 2 | Wählen Sie in **Azure Services Cloud NGFWs by Palo Alto Networks** aus.

STEP 3 | Wählen Sie die Firewall aus, die Sie in Ihr CSP-Konto integrieren möchten.

STEP 4 | Klicken Sie im Abschnitt **Support + Troubleshooting** auf **New Support Request**. Der Support-Bildschirm von Palo Alto Networks wird mit der **Mandanten-ID** und der **Seriennummer des Produkts** angezeigt.

STEP 5 | Klicken Sie auf **Register User account and create a case at Customer Support Portal**.

STEP 6 | Geben Sie auf der Seite **Create New Account / Use Existing Account** Ihre E-Mail-Adresse ein und schließen Sie die Authentifizierungsschritte ab. Klicken Sie dann auf **Next**.

STEP 7 | Wählen Sie im Abschnitt **Device Registration** das **Cloud Marketplace**-Abonnement aus dem Drop-down-Menü aus. Zum Beispiel *Azure Cloud NGFW*.

STEP 8 | Geben Sie die **Mandanten-ID** und **Seriennummer** für Ihr Azure Marketplace-Abonnement ein. Sie können diese Informationen von der Palo Alto Support-Seite aus Schritt 4 kopieren. Klicken Sie auf **Next (Weiter)**.

STEP 9 | Geben Sie den **Authentifizierungscode** ein, der an Ihre E-Mail-Adresse gesendet wurde. Klicken Sie auf **Next (Weiter)**.

STEP 10 | Nach der Authentifizierung mit SSO erscheint die CSP-Anmeldeseite. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Next**.

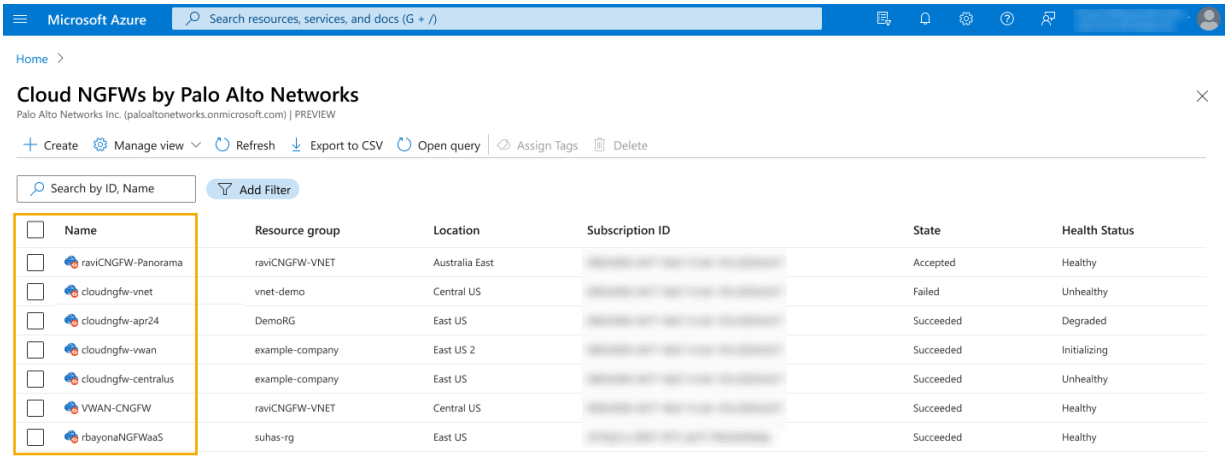
Überwachen des Cloud NGFW-Zustands

Cloud NGFW unterstützt die Zustandsüberwachung über das Azure-Portal. Zeigen Sie den allgemeinen Zustand der Firewall, den Verbindungsstatus und Diagnoseinformationen an, mit denen Sie die Ursache eines fehlerhaften Firewall-Zustands ermitteln können.

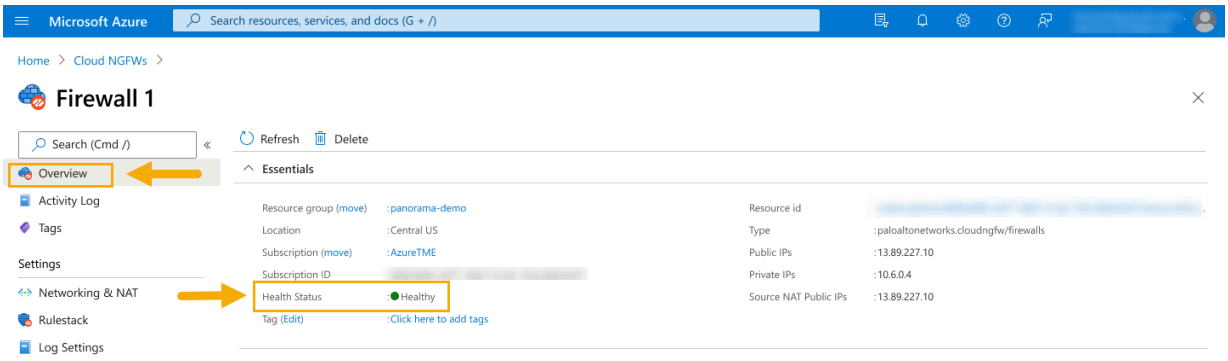
So überwachen Sie den Zustand Ihrer Cloud NGFW:

STEP 1 | Melden Sie sich beim Azure-Portal an und suchen Sie nach **Cloud NGFW by Palo Alto Networks**. Hier werden die Cloud NGFWs angezeigt, die Sie bei Azure registriert haben.

STEP 2 | Wählen Sie die Cloud NGFW aus, die Sie überwachen möchten.



STEP 3 | Erweitern Sie auf der Seite **Overview** die Option **Essentials**. Der Abschnitt „Essentials“ zeigt den Zustand der ausgewählten Cloud NGFW an.



Zustandsmonitor-Status

Der Zustand wird als farbcodiertes Symbol angezeigt und wird sowohl für die *Netzwerksicherheit* als auch für die *Cloud-Sicherheit* dargestellt.

Zustand für *die Netzwerksicherheit*:

- **Healthy** (grünes Symbol). Zeigt an, dass das primäre und sekundäre Panorama mit der Cloud NGFW-Ressource für Netzwerksicherheitsanwendungen verbunden ist.
- **Degraded** (gelbes Symbol). Die Netzwerksicherheit der Cloud NGFW-Ressource ist beeinträchtigt.
- **Unhealthy** (rotes Symbol). Zeigt an, dass die Cloud NGFW keine Verbindung zur virtuellen Panorama-Appliance herstellen kann. Stellen Sie sicher, dass Ihre Cloud NGFW bei Panorama registriert ist.

Der Zustand für die *Cloud-Sicherheit* gilt für die Erstellung und Aktualisierung einer Firewall:

- **Healthy** (grünes Symbol). Zeigt den individuellen Status des mit der Cloud NGFW-Ressource verknüpften Regelstapels und den Status der primären und sekundären virtuellen Panorama-Appliance an, die mit der Cloud NGFW-Ressource verbunden ist. Diese Informationen erscheinen im Abschnitt **Associated rulestack** und werden als **Connected** oder **Not Connected** angezeigt.
- **Degraded** (gelbes Symbol). Die Cloud-Sicherheit ist beeinträchtigt.
- **Unhealthy** (rotes Symbol). Zeigt an, dass der Cloud NGFW-Regelstapel auf keiner Instanz erfolgreich festgeschrieben wurde. Nachdem das Problem behoben wurde, ändert sich der Zustandsmonitor und zeigt einen fehlerfreien Status an (grünes Symbol).

- **Initializing** (blaues Symbol). Zeigt an, dass die Cloud NGFW-Ressource initialisiert wird.

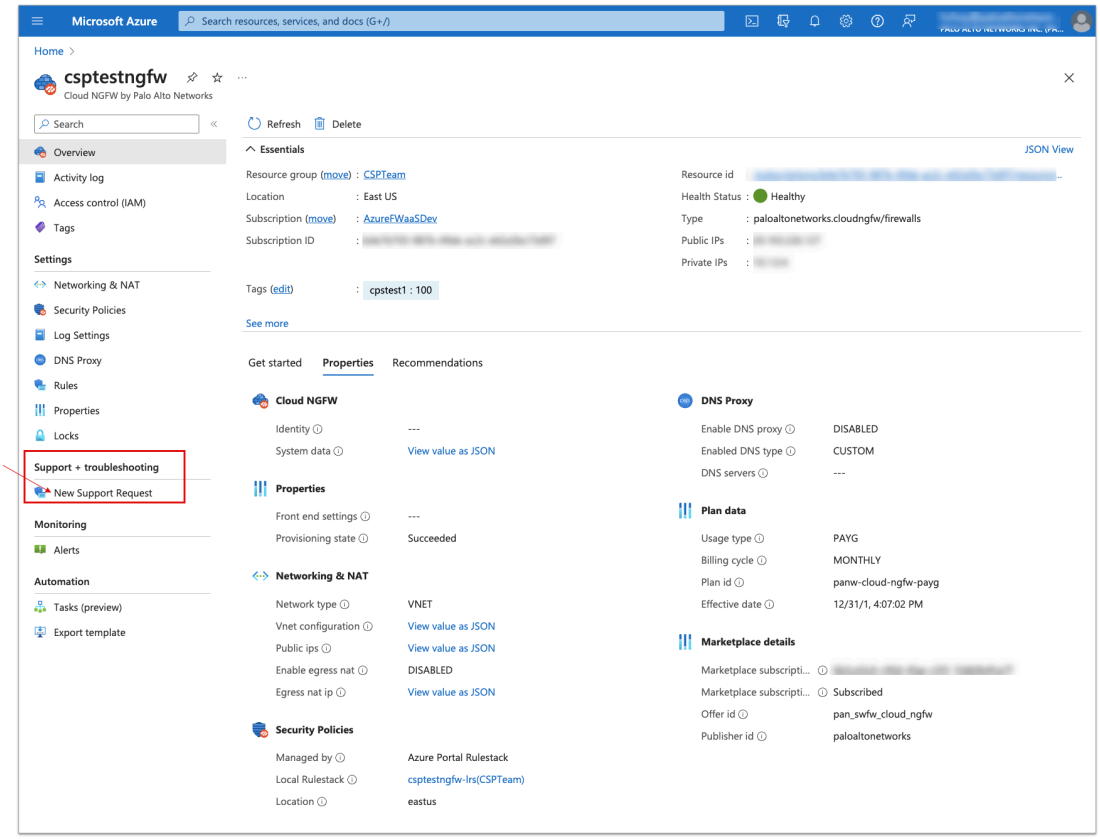
Supportfall erstellen

So erstellen Sie einen Supportfall über das Azure-Portal:

STEP 1 | Melden Sie sich beim Azure-Portal an.

STEP 2 | Klicken Sie im Abschnitt **Support + Troubleshooting** auf **New Support Request**.

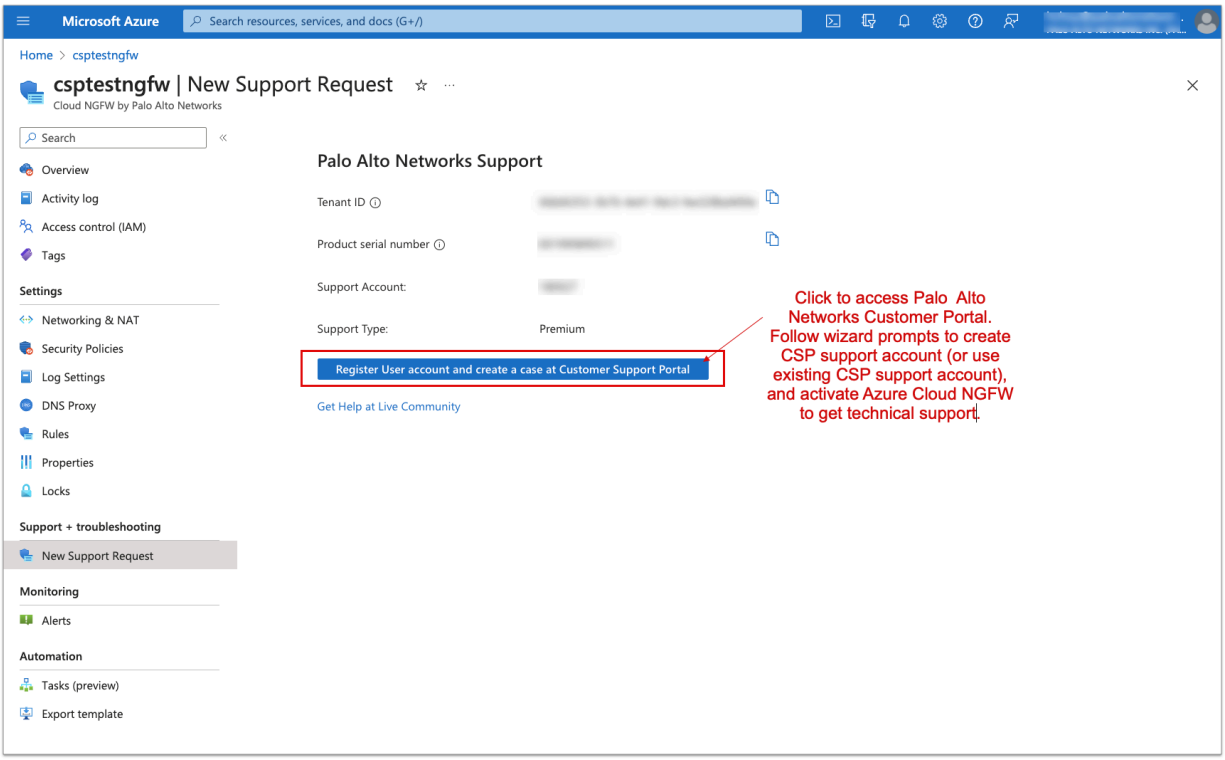
1.



Click for technical support from Palo Alto Networks

STEP 3 | Klicken Sie auf der Seite **New Support Request** auf **Register User account and create a case at Customer Support Portal**.

2.



STEP 4 | Befolgen Sie die Anweisungen, um ein Konto für das Palo Alto Networks Customer Support Portal (CSP) zu erstellen. Wenn Sie bereits über ein CSP-Konto verfügen, verwenden Sie Ihre vorhandenen Anmeldedaten.

Cloud NGFW für Azure bereitstellen

Die Informationen in diesem Abschnitt dienen als Referenz für die Bereitstellung von Cloud NGFW über das Azure-Portal. Sie können das Azure-Portal verwenden, um die Cloud NGFW über mehrere Azure-Konten hinweg bereitzustellen. Das Azure-Portal verwendet die Cloud NGFW-Konsole zum Erstellen lokaler Regelstapel.

Es werden zwei Bereitstellungsmethoden unterstützt:Azure VNets und Azure vWANs. Ein Azure vNET ermöglicht die sichere Kommunikation mit anderen Azure-Ressourcen, dem Internet und lokalen Netzwerken. Ein Azure vWAN stellt einen Netzwerkdienst dar, der Netzwerk-, Sicherheits- und Routingfunktionen kombiniert, um eine einzige, betriebsbereite Schnittstelle bereitzustellen. Für die Bereitstellung in Ihrer Azure-Umgebung sind die Cloud NGFW-Konsole und das Azure-Portal erforderlich.

Der Durchsatz für ein vNET oder vWAN ist auf 100 Gbit/s begrenzt.

- Bereitstellen der Cloud NGFW in einem vNET
- Bereitstellen der Cloud NGFW in einem vWAN

Bereitstellen der Cloud NGFW in einem vNET

Die Cloud NGFW manifestiert sich als zwei private IP-Adressen (öffentlich und privat) in Ihrem vNET. Mithilfe benutzerdefinierter Routen (mit der privaten IP-Adresse der Cloud NGFW als nächsten Hop) können Sie den Datenverkehr zur Paketprüfung und Bedrohungsprävention an die Cloud NGFW umleiten.

Die Azure Cloud NGFW kommuniziert mit der Cloud NGFW, um Regelstapel hinzuzufügen. Die Cloud NGFW misst kontinuierlich die Nutzung der Cloud NGFW-Ressource und sendet Nutzungsaufzeichnungen für jedes Azure-Abonnement an den Azure-Messdienst. Dieser Dienst ist für die Abrechnung zuständig.

Weitere Informationen finden Sie auf der Beispielkonfigurationsseite, nachdem Sie die Cloud NGFW in einem vNET bereitgestellt haben.

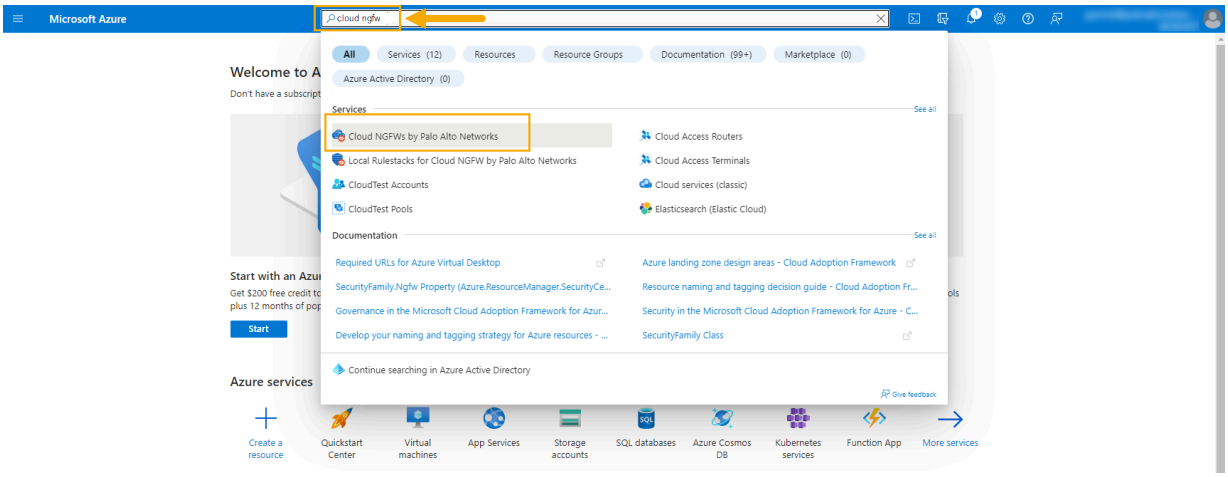
Voraussetzungen

Um Cloud NGFW in einem vNET bereitzustellen, benötigen Sie ein Azure-Abonnement. Dieses Abonnement sollte über eine Eigentümer- oder Mitwirkenden-Rolle verfügen.

Beim Bereitstellen der Cloud NGFW in einem vNET unter Verwendung eines vorhandenen vNET-Hubs sollte die Mindestgröße /25 betragen. Sie müssen über 2 Subnetze mit der Mindestgröße /26 verfügen; diese Subnetze müssen an den Dienst ***PaloAltoNetworks.Cloudngfw/firewalls*** *delegiert werden.*

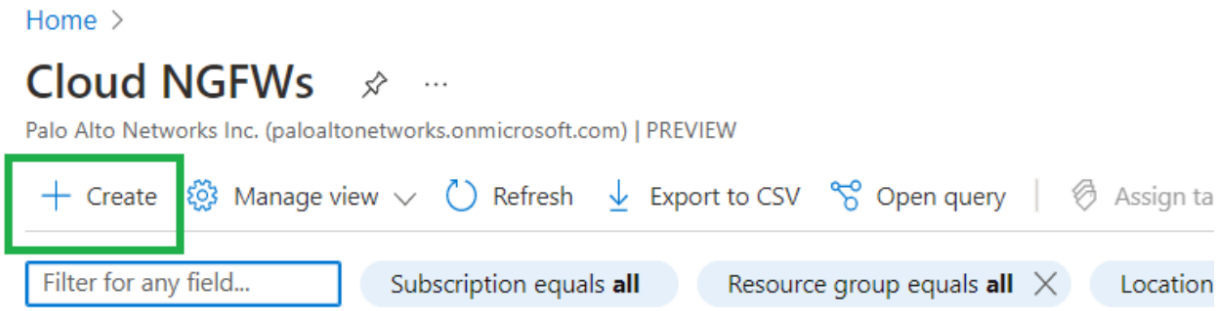
Für Bereitstellungen, die 100 Gbit/s unterstützen, benötigen Sie insgesamt 80 freie IP-Adressen; 40 IP-Adressen werden für öffentlich und 40 IP-Adressen für privat verwendet.

STEP 1 | Melden Sie sich beim Azure-Portal an und suchen Sie nach **Cloud NGFW**. Diese Suche zeigt den Cloud NGFW-Dienst an: **Cloud NGFW von Palo Alto Networks**.



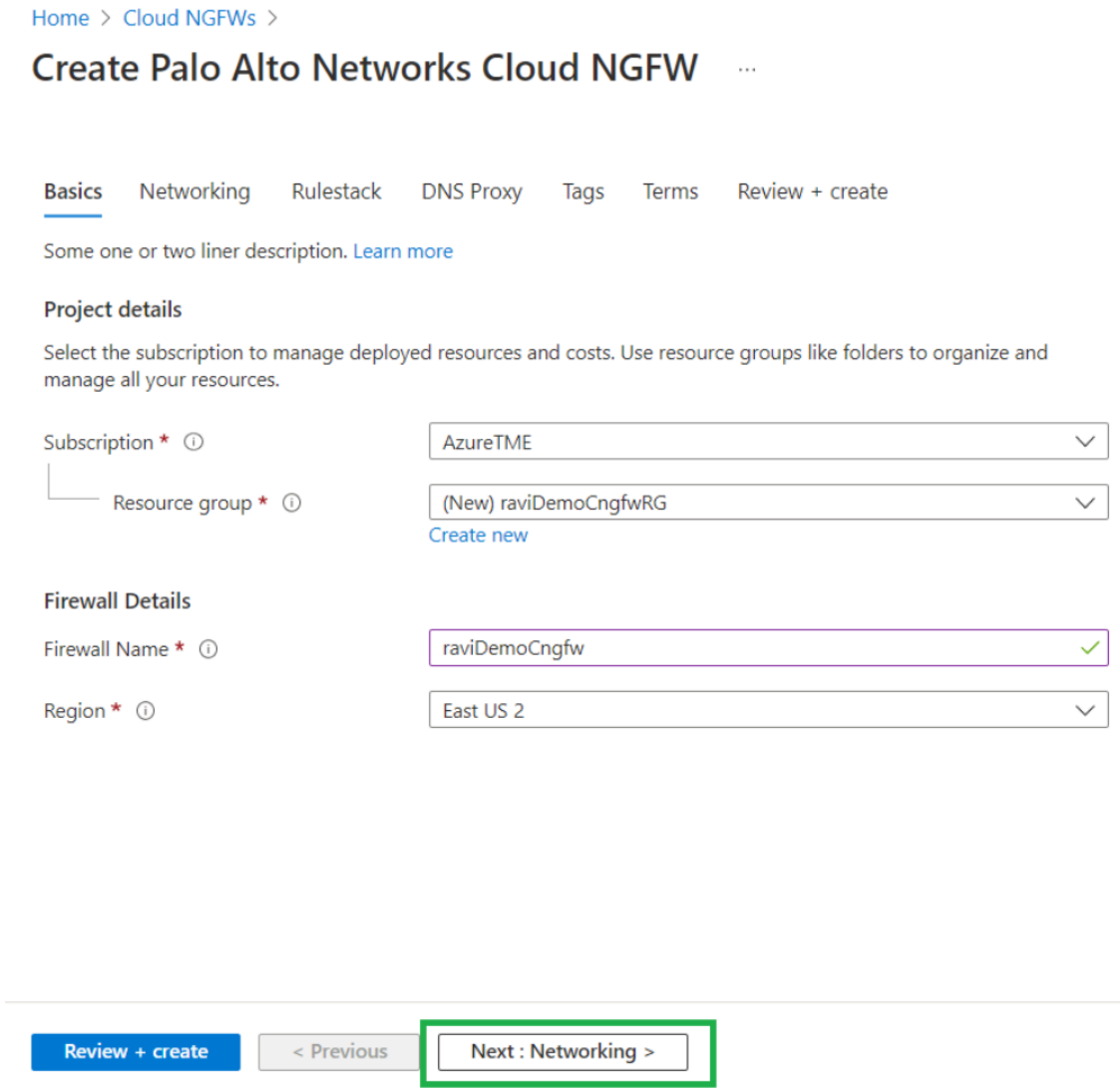
STEP 2 | Klicken Sie auf **Cloud NGFWs**, um mit der Erstellung des Cloud NGFW-Dienstes für Azure von Palo Alto Networks zu beginnen.

STEP 3 | Klicken Sie auf der Zielbildschirmseite der Cloud NGFW-Ressource auf **Create**, um mit der Erstellung der Cloud NGFW-Ressource zu beginnen.



Wenn Ihr Abonnement zuvor erstellt wurde, enthält die Zielseite Informationen zu Cloud NGFW-Ressourcen.

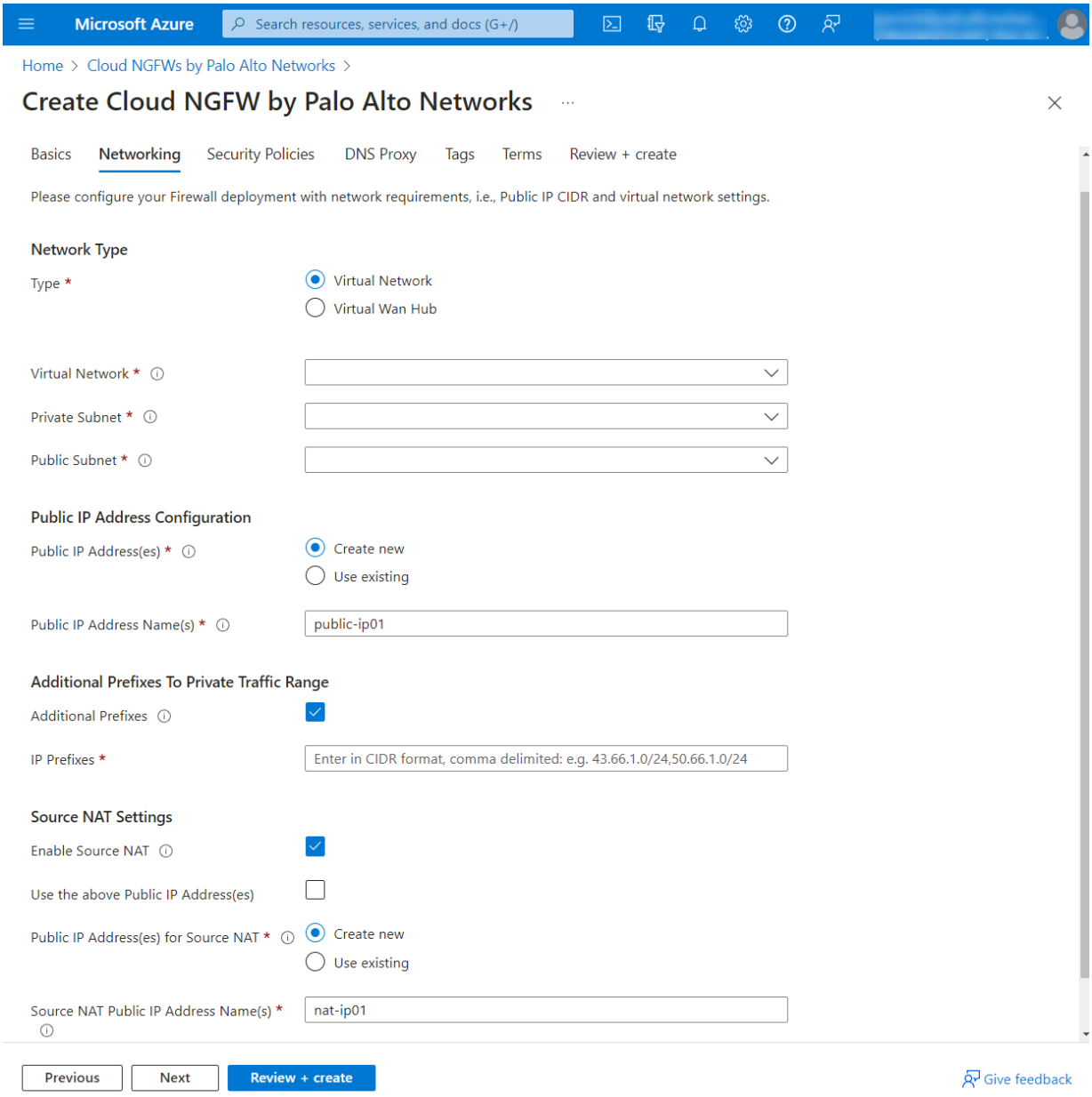
STEP 4 | Nachdem Sie auf **Create** geklickt haben, wird der Bildschirm **Create Palo Alto Networks Cloud NGFW** angezeigt.



Geben Sie mit den Angaben in der folgenden Tabelle **grundlegende** Informationen ein und klicken Sie dann auf **Next: Networking**:

Feld	Beschreibung
Abonnement	Wird automatisch basierend auf dem während der Anmeldung verwendeten Abonnement ausgewählt.
Ressourcengruppe	Verwenden Sie eine der vorhandenen Ressourcengruppen oder erstellen Sie eine neue (mit der Option **Create New**), in der die Cloud NGFW-Ressource erstellt wird.
Firewallname	Name der Cloud NGFW Firewall-Ressource. *Verwenden Sie für von Panorama verwaltete Firewalls nicht ausschließlich Großbuchstaben für den Firewall-Namen.*
Region	Region, in der Cloud NGFW bereitgestellt wird.

STEP 5 | Geben Sie im Bildschirm **Networking** Informationen zur Firewall-Bereitstellung ein:



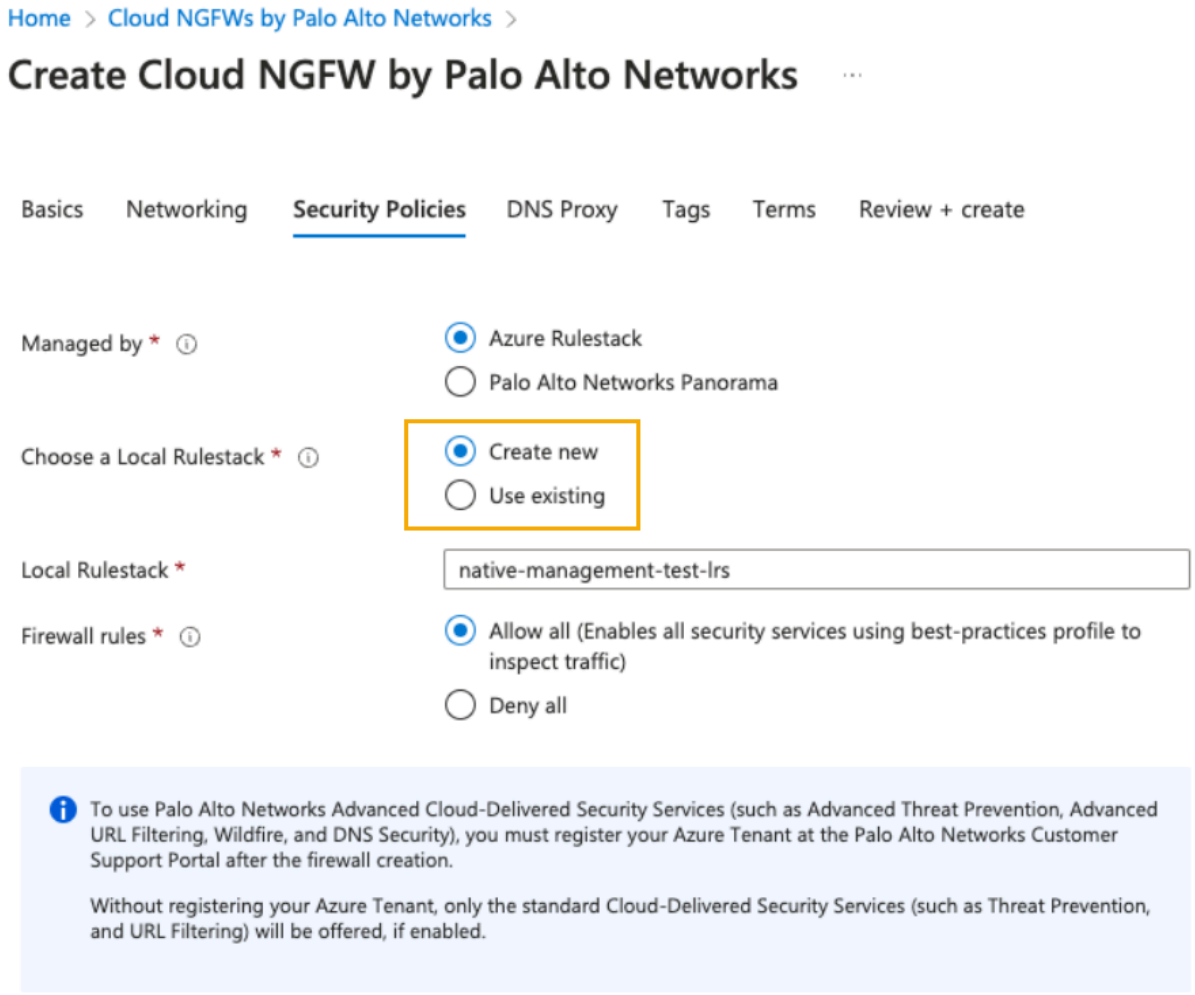
Der Bildschirm **Networking** enthält Felder in der folgenden Tabelle:

Feld	Beschreibung
Typ	Wird automatisch basierend auf dem während der Anmeldung verwendeten Abonnement ausgewählt.
Virtuelles Netzwerk	Wählen Sie **Virtual network** aus. Erstellen Sie ein neues virtuelles Netzwerk oder wählen Sie ein vorhandenes virtuelles Netzwerk aus.
Privates Subnetz	Wählen Sie ein privates Subnetz aus.
Öffentliches Subnetz	Wählen Sie ein öffentliches Subnetz aus.
Konfiguration der öffentlichen IP-Adresse	Geben Sie **Public IP addresses** an. Klicken Sie auf **Create new**, um eine neue Adresse einzurichten, oder klicken Sie auf **Use existing**, um eine vorhandene Adresse anzugeben.
Zusätzliche Präfixe für privaten Datenverkehrsbereich	Wenn Sie neben den in RFC 1918 angegebenen Bereichen weitere private IP-Adressbereiche unterstützen möchten, verwenden Sie die Option **Additional Prefixes to Private Traffic Range**. Mit dieser Unterstützung können Sie öffentliche IP-Adressblöcke in Ihrem privaten Netzwerk verwenden, ohne den Datenverkehr ins Internet umzuleiten. Aktivieren Sie das Kontrollkästchen **Additional Prefixes**. Geben Sie Adressen im CIDR-Format ein (z. B. 40.0.0.0/24). Verwenden Sie eine durch Kommas getrennte Liste, um mehrere Adressen einzuschließen. *Standardmäßig werden RFC 1918-Präfixe automatisch in den privaten Verkehrsbereich aufgenommen. Wenn Ihre Organisation öffentliche IP-Bereiche verwendet, geben Sie diese IP-Präfixe explizit an. Sie können diese öffentlichen IP-Präfixe einzeln oder als Aggregate angeben.* *Informationen zum Hinzufügen zusätzlicher Präfixe nach der Bereitstellung der Firewall finden Sie im Abschnitt* Bearbeiten einer vorhandenen Firewall, um zusätzliche private Adressen für Nicht-RFC 1918-Unterstützung hinzuzufügen.
Quell-NAT-Einstellungen	Schließen Sie die Option **Source NAT** ein, wenn für den ins Internet ausgehenden Datenverkehr Network Address Translation (NAT) verwendet wird.

STEP 6 | Klicken Sie auf **Next: Security Policies**.

STEP 7 | Erstellen Sie auf der Seite **Security Policies** einen lokalen Regelstapel oder wählen Sie einen vorhandenen Regelstapel aus. Ein neuer Regelstapel enthält keine Regeln. Sie können Sicherheitsregeln definieren, nachdem Sie die Cloud NGFW-Ressource bereitgestellt haben.

Als Administrator können Sie eine Sicherheitsrichtlinie entweder mithilfe eines nativen Azure-Regelstapels verwalten oder Palo Alto Networks Panorama zur Richtlinienverwaltung verwenden. Weitere Informationen finden Sie unter Verknüpfen von Cloud NGFW mit Palo Alto Networks Management.

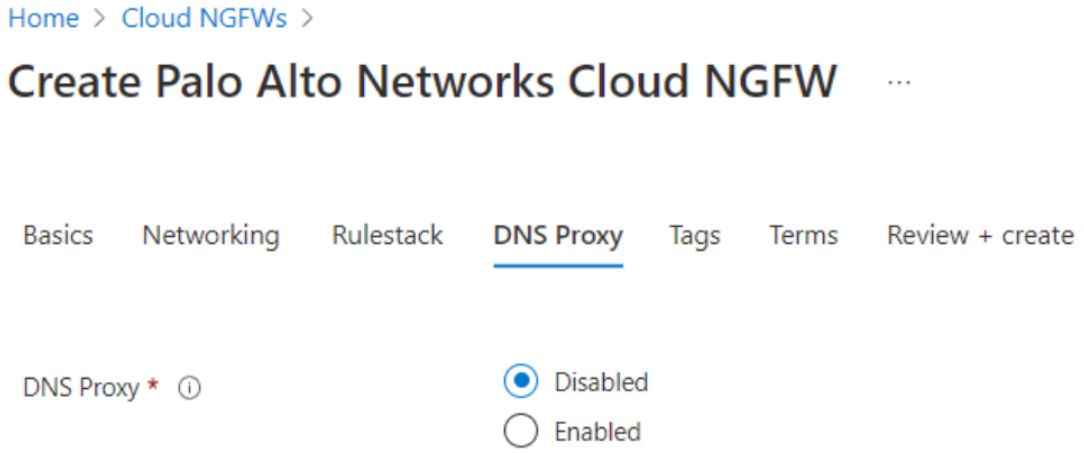


Wenn Sie die erweiterten Sicherheitsdienste von Palo Alto Networks (wie etwa „Advanced Threat Prevention“ und „Advanced URL Filtering“) nutzen möchten, müssen Sie Ihren Azure-Mandanten nach der Erstellung Ihrer Firewall im Palo Alto Networks Customer Support Portal *registrieren. Weitere Informationen zum Registrieren eines Mandanten finden Sie unter* Mit Cloud NGFW für Azure starten.

1.

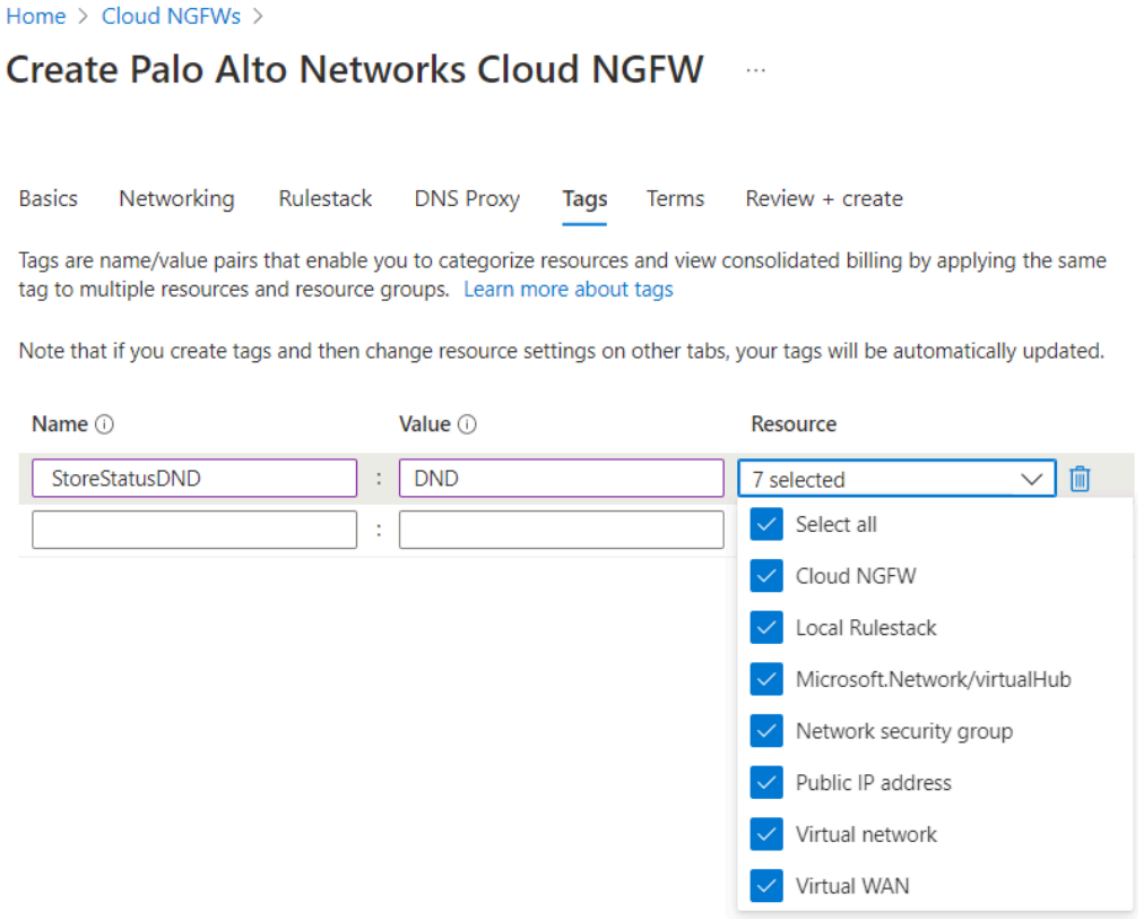
STEP 8 | Klicken Sie auf **Next: DNS Proxy**, um die Cloud NGFW-Ressource als DNS-Proxy zu konfigurieren. Sie können die Cloud NGFW so konfigurieren, dass sie den gesamten DNS-Verkehr überprüft, indem sie als Proxy für vNET-Ressourcen fungiert. Wenn der DNS-Proxy konfiguriert ist,

leitet er die DNS-Anforderung an den standardmäßigen Azure-DNS-Server oder an einen von Ihnen angegebenen DNS-Server weiter. Standardmäßig ist der DNS-Proxy deaktiviert.



STEP 9 | Klicken Sie auf **Next: Tags**, um Tags für Ihre Azure-Anforderungen anzugeben. Tags sind vordefinierte Bezeichnungen, die Ihnen dabei helfen können, die Sicherheitslücken in Ihrer Umgebung zu verwalten und die konsolidierte Abrechnung im Zusammenhang mit Ihrem

Azure-Konto anzuzeigen. Sie werden zentral definiert und können auf Sicherheitslücken und als Richtlinienausnahmen festgelegt werden.



Tags werden wie folgt verwendet:

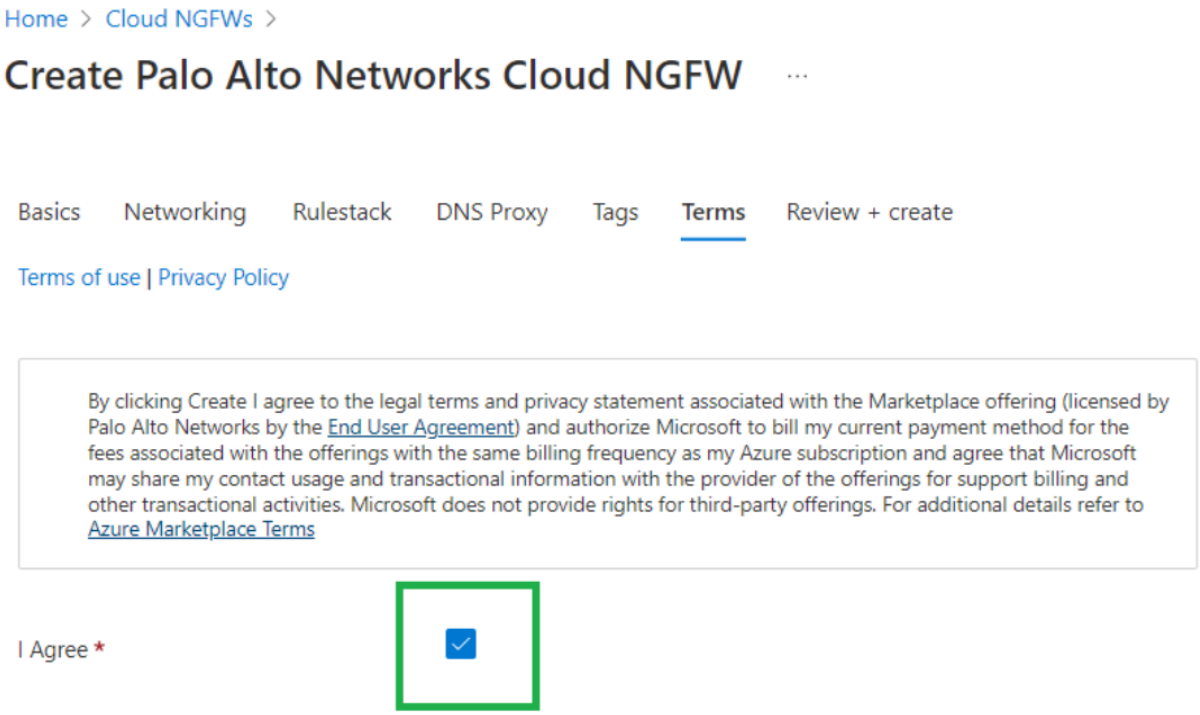
- Kennzeichnung der Sicherheitslücken. Sie sind eine praktische Möglichkeit, die Sicherheitslücken in Ihrer Umgebung zu kategorisieren.
- Richtlinienausnahmen. Sie können Teil Ihrer Regeln sein, um gezielt auf markierte Sicherheitslücken einzuwirken.
- Die konsolidierte Abrechnung für Ihr Azure-Konto anzeigen.

  Tags sind nützlich, wenn Sie große Containerbereitstellungen mit mehreren Teams haben, die in derselben Umgebung arbeiten. Beispielsweise könnten sich verschiedene Teams mit unterschiedlichen Arten von Sicherheitslücken befassen. Anschließend können Sie Tags festlegen, um Verantwortlichkeiten für Sicherheitslücken zu definieren. Andere Verwendungsmöglichkeiten wären, den Status der Behebung der Sicherheitslücke festzulegen oder Sicherheitslücken zu markieren, die ignoriert werden sollen, wenn es sich um ein bekanntes Problem handelt, das in naher Zukunft nicht behoben werden kann.

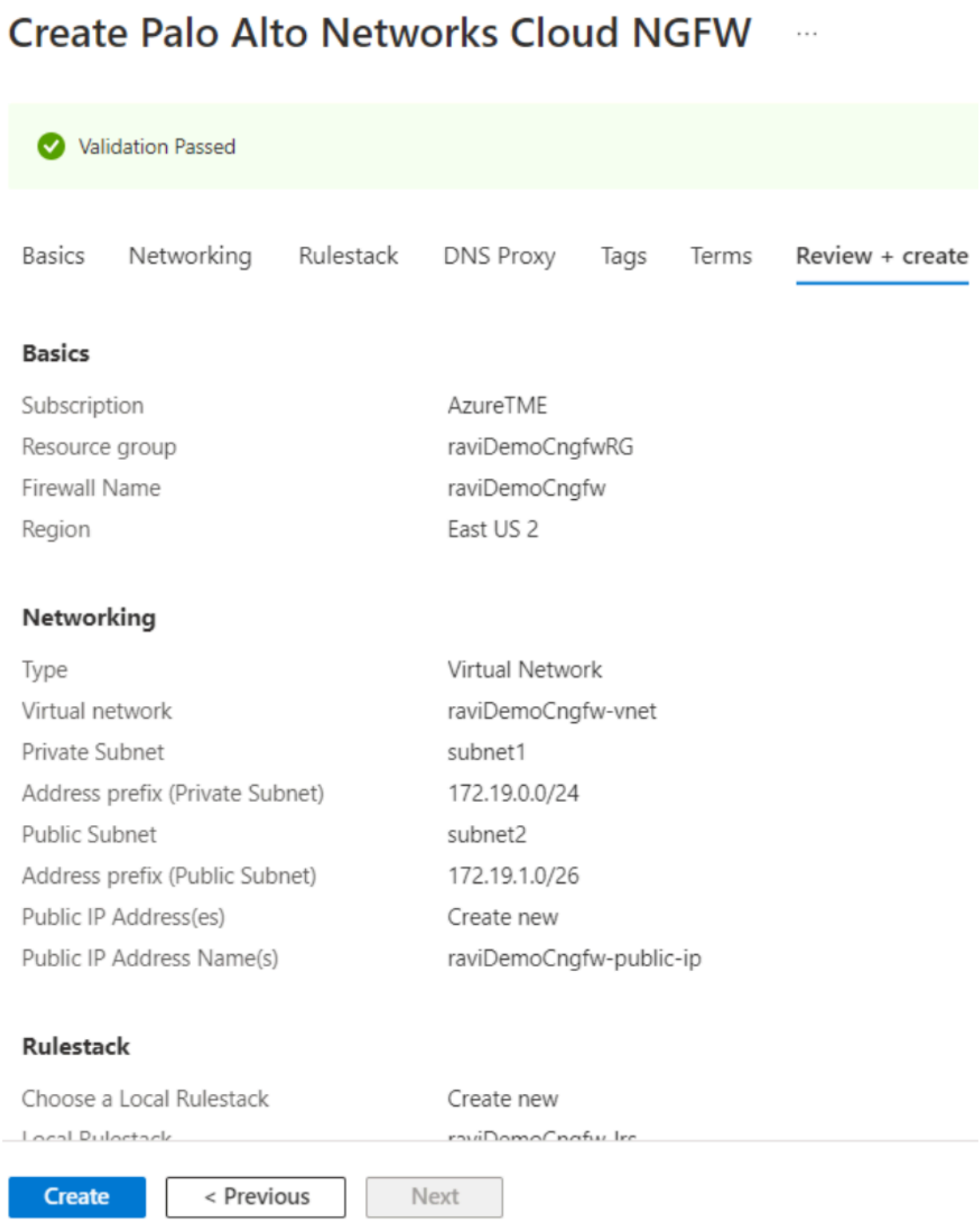
  Sie können beliebig viele Tags definieren. Informationen zum Erstellen von Tags für Ihr Azure-Konto finden Sie unter Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen und -Verwaltungshierarchie.

STEP 10 | Klicken Sie auf **Next: Terms** und akzeptieren Sie die Bedingungen für die Bereitstellung.



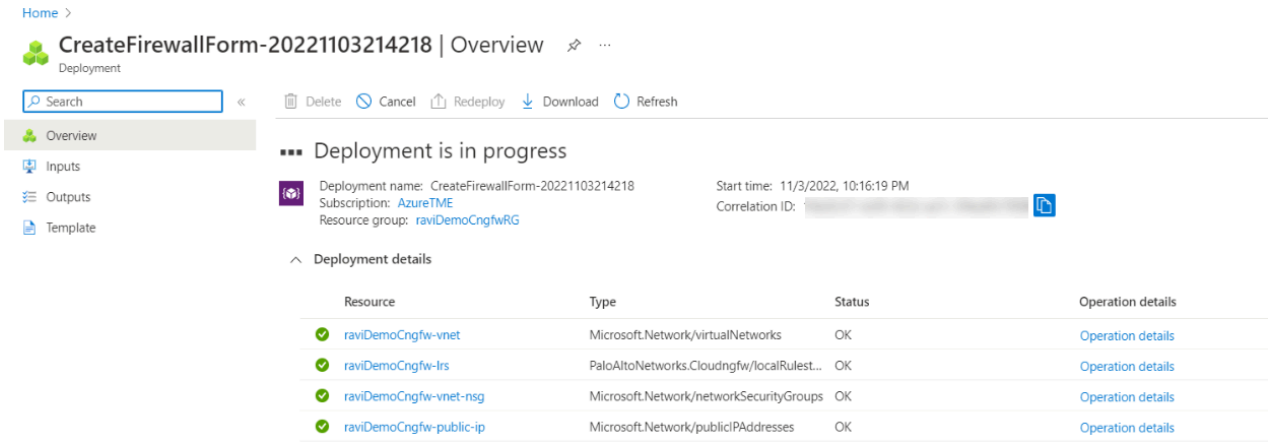
STEP 11 | Klicken Sie auf **Next: Review + create**, um Ihr Azure-Abonnement für die Cloud NGFW-Ressource zu überprüfen und zu validieren. Die Ressource wird zuerst validiert und dann erstellt. Auf dem

Bildschirm wird **Validation Passed** angezeigt. Klicken Sie auf **Create**, um den Cloud NGFW-Dienst bereitzustellen:



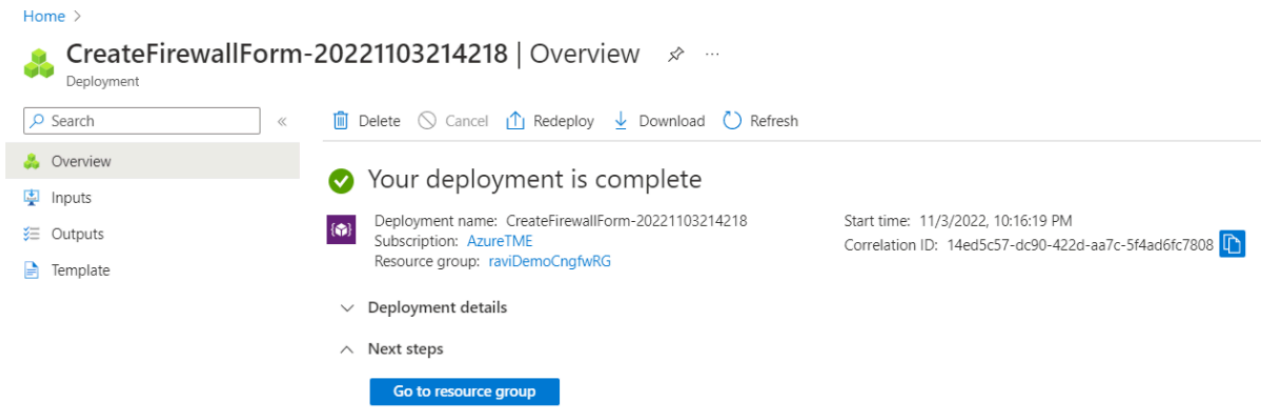
Überprüfen Sie die Bereitstellung der Cloud NGFW im vNET

Nach dem Erstellen des Cloud NGFW-Dienstes wird der Bereitstellungsfortschritt angezeigt.

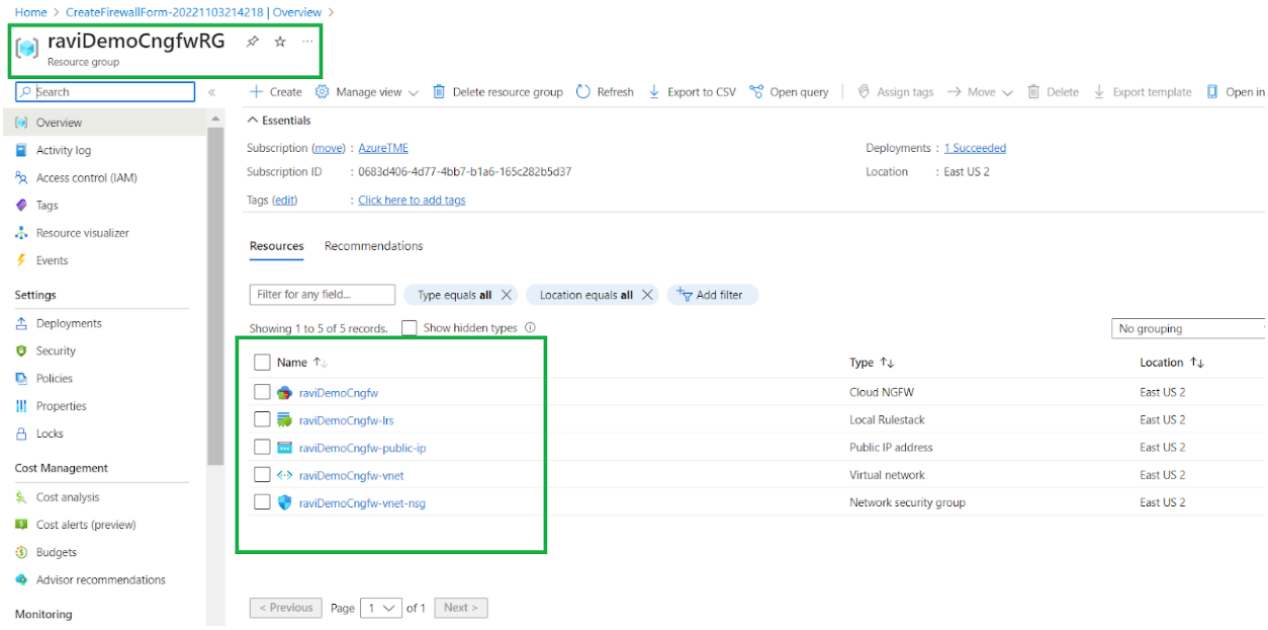


Die Bereitstellung einer Cloud NGFW-Ressource dauert ungefähr 30 Minuten.

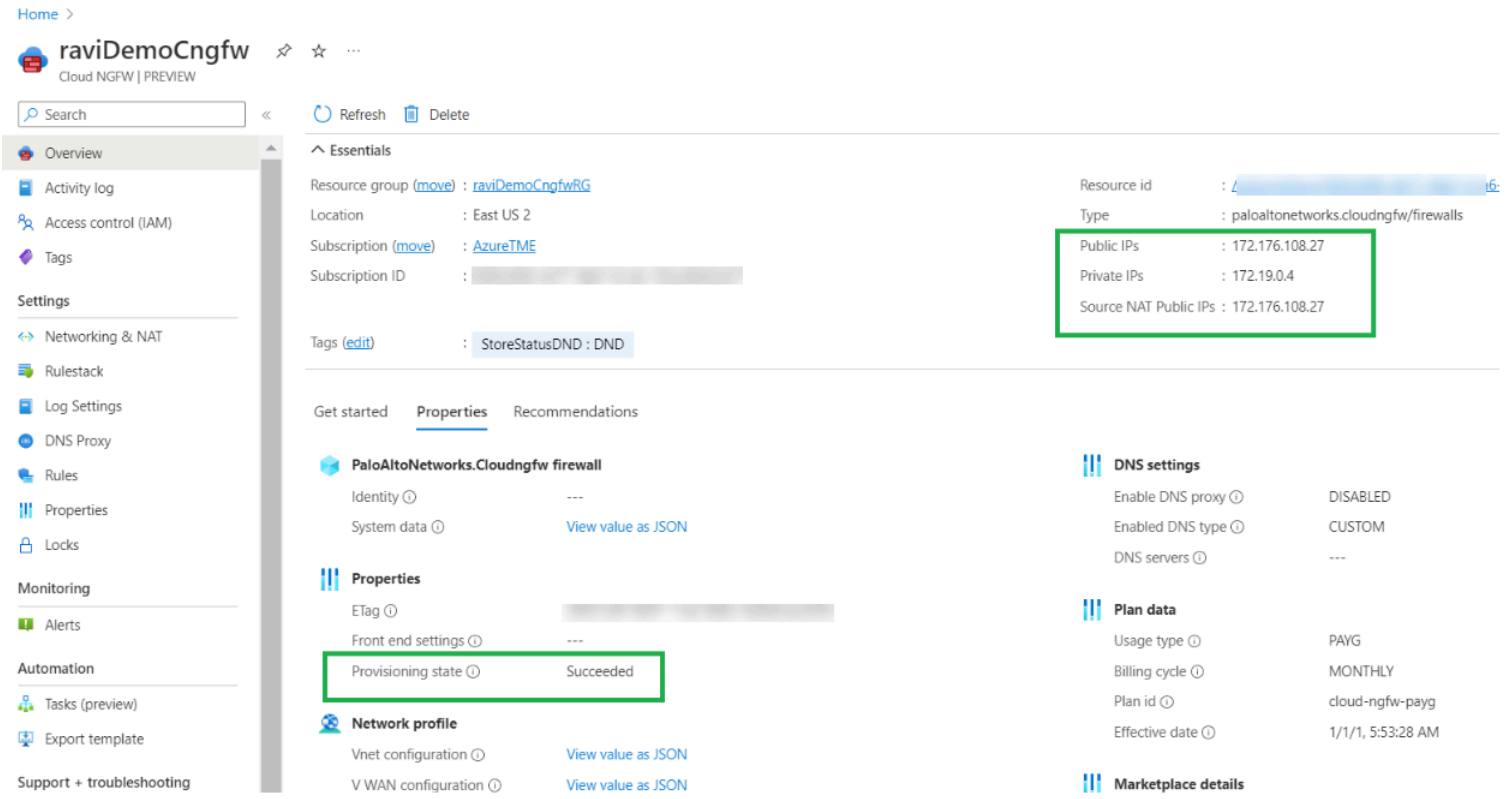
Bei einer erfolgreichen Bereitstellung wird der folgende Bildschirm angezeigt. Klicken Sie auf **Go to resource group**, um die für diese Bereitstellung erstellten Ressourcen zu überprüfen:



Es werden fünf Ressourcen erstellt. Dazu gehören Cloud NGFW, lokaler Regelstapel, öffentliche IP-Adresse, virtuelles Netzwerk und Sicherheitsgruppe:



Sobald die Cloud NGFW-Ressource erstellt ist, wählen Sie sie aus, um zu überprüfen, ob der Bereitstellungsstatus **Succeeded** anzeigt. Auf diesem Bildschirm werden auch die öffentlichen und privaten IP-Adressen angezeigt, die mit dem Cloud NGFW-Dienst verknüpft sind.



Weitere Informationen nach der Bereitstellung der Cloud NGFW in einem vNET finden Sie in der Beispielkonfiguration.

Bearbeiten einer vorhandenen Firewall, um zusätzliche private Adressen für Nicht-RFC 1918-Unterstützung hinzuzufügen

So bearbeiten Sie eine vorhandene Firewall, um zusätzliche private Adressen hinzuzufügen:

STEP 1 | Suchen Sie die Cloud NGFW im Azure-Portal.

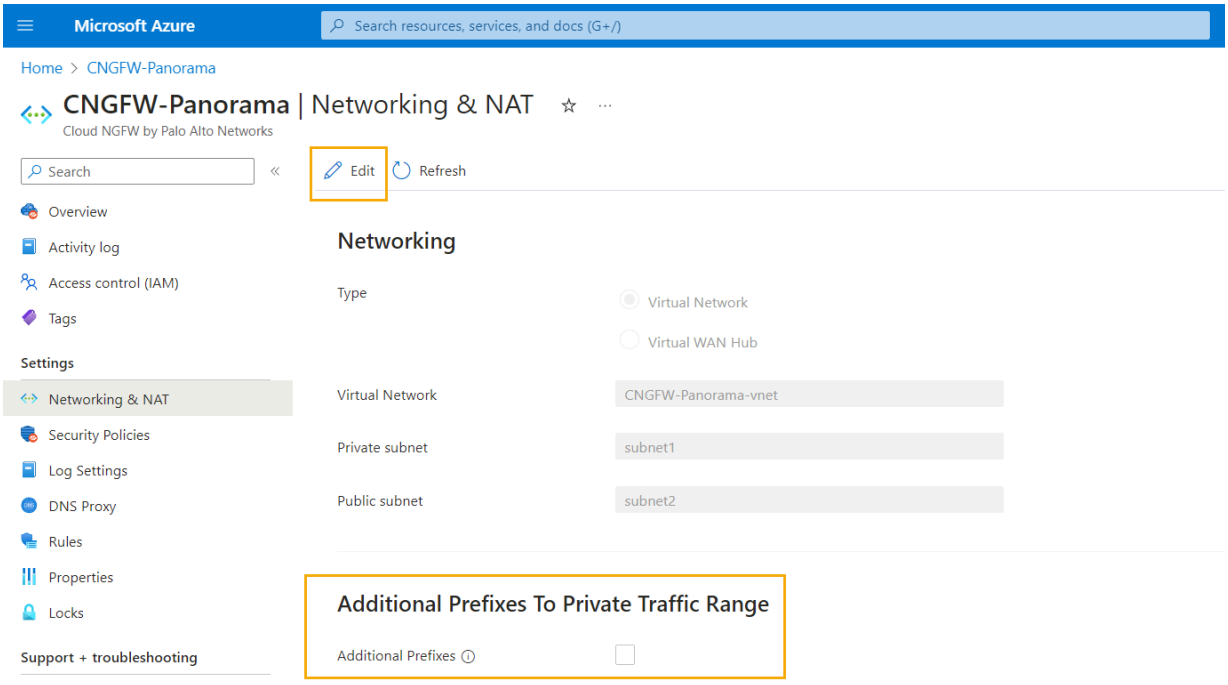
STEP 2 | Wählen Sie im Abschnitt **Settings** die Option **Networking & NAT** aus.

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

STEP 4 | Aktivieren Sie im Abschnitt **Additional Prefixes to Private Traffic Range** das Kontrollkästchen für **Additional Prefixes** aus.

STEP 5 | Geben Sie Adressen im CIDR-Format ein (z. B. 40.0.0.0/24). Verwenden Sie eine durch Kommas getrennte Liste, um mehrere Adressen einzuschließen.

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



Bearbeiten einer vorhandenen Firewall, um private Quell-NAT zu aktivieren

Verwenden Sie die Option **Private Source NAT**, wenn Sie eine Quellnetzwerkadressübersetzung für Anforderungen von einer Instanz in einem nicht weiterleitbaren Subnetz durchführen möchten. Mit dieser Option können Sie Datenverkehr an eine weiterleitbare IP-Adresse senden, die dem Application Load Balancer (ALB) zugewiesen ist. Geben Sie nach der Aktivierung der privaten Quell-NAT die Ziel-IP-Adresse an.

*Der Ost-West-Datenverkehr der Cloud NGFW basiert auf benutzerdefinierten Routen (UDR), um den Datenverkehr an die Firewall weiterzuleiten. Diese Abhängigkeit wird durch typischen Ost-West-Datenverkehr unterstützt, wenn beide Enden des Netzwerks Teil des privaten Netzwerks sind. Dies bringt jedoch Herausforderungen für einen neuen Datenverkehrstyp mit sich: Eine Seite der Bereitstellung ist das private Netzwerk, während die andere Seite der Bereitstellung einen Partner oder PaaS-Dienst unterstützt, auf den über einen privaten Endpunkt im virtuellen Netzwerk zugegriffen werden kann. In solchen Umgebungen verfügen Sie möglicherweise nicht über Verwaltungszugriff auf das gesamte (andere) Netzwerk, um benutzerdefinierte Routen (UDR) zu konfigurieren. Der Datenverkehr wird durch UDR an die Cloud NGFW geleitet, der Rückverkehr wird jedoch an die Quell-IP des Clients gesendet, ohne die Cloud NGFW zu durchlaufen. Dies führt zu einem asymmetrischen Routenproblem und der resultierende TCP-Handshake kann von der Firewall nicht abgeschlossen werden. Cloud NGFW verwendet die **Private Source NAT**, um die Quell-IP-Adresse in die private Schnittstellen-IP der Firewall-Instanz zu übersetzen. Dadurch wird sichergestellt, dass der Rückverkehr von Cloud NGFW an die entsprechende Schnittstelle weitergeleitet wird.*

STEP 1 | Suchen Sie die Cloud NGFW im Azure-Portal.

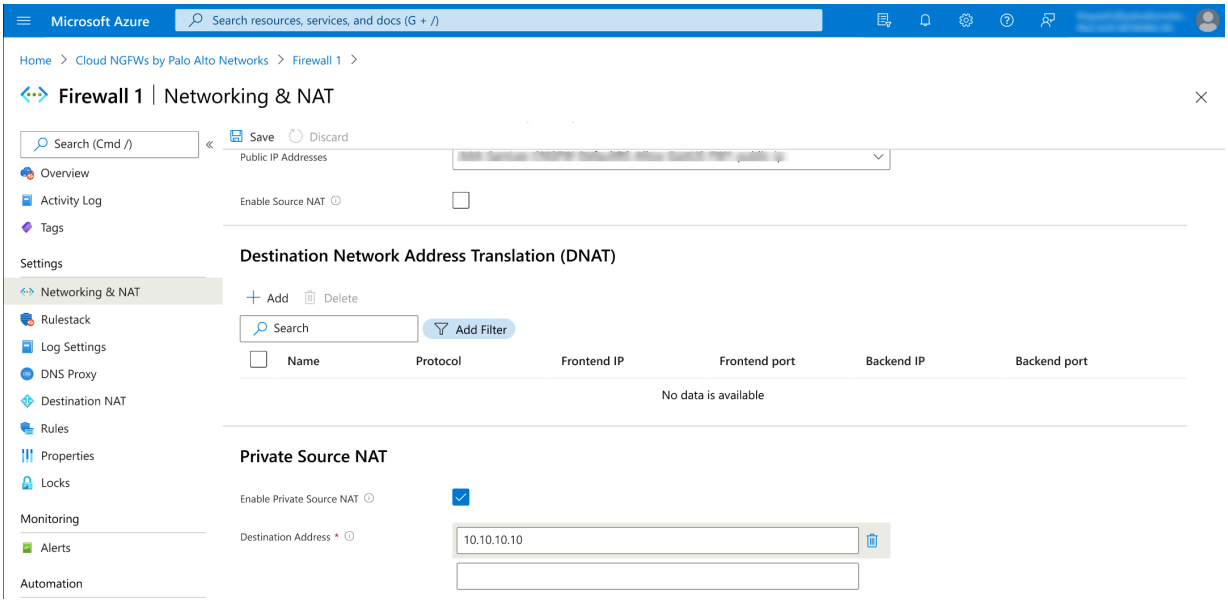
STEP 2 | Wählen Sie im Abschnitt **Settings** die Option **Networking & NAT** aus.

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

STEP 4 | Aktivieren Sie im Abschnitt **Private Source NAT** das Kontrollkästchen **Enable Private Source NAT**.

STEP 5 | Geben Sie die Zieladresse ein.

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



Beispielkonfiguration nach vNET-Bereitstellung

Nachdem Sie Cloud NGFW erfolgreich in einem Azure vNET bereitgestellt haben, können Sie mit der Konfiguration des Cloud NGFW-Dienstes beginnen. Die in diesem Abschnitt bereitgestellten Informationen veranschaulichen allgemeine Aufgaben zum Ausführen von Cloud NGFW in Ihrer Azure-Umgebung:

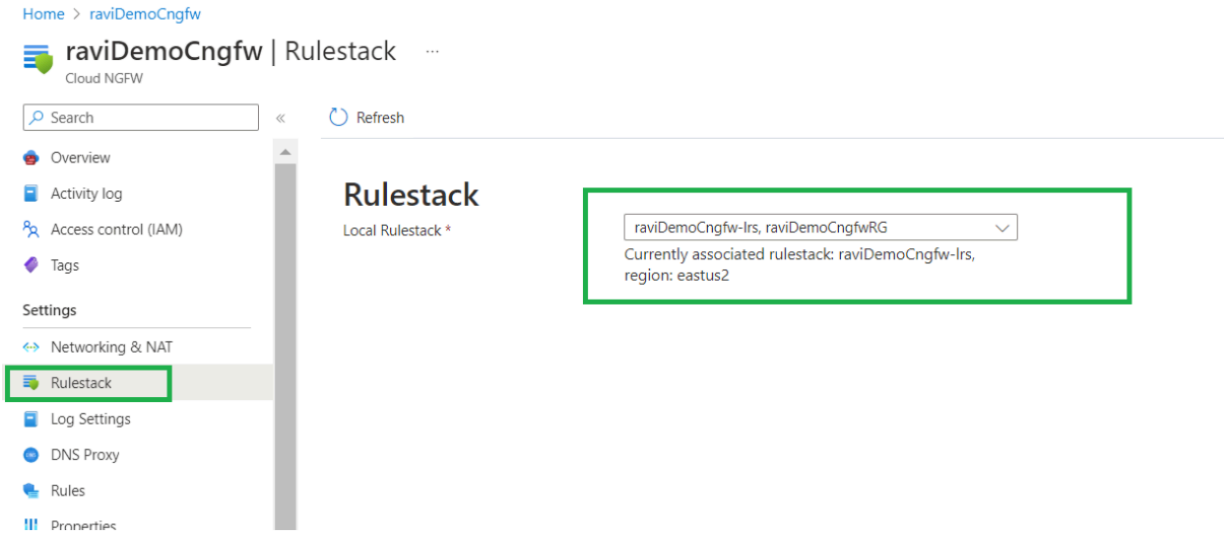
- Erstellen oder Aktualisieren eines Regelstapels
- Hinzufügen einer FQDN-Liste
- Hinzufügen einer Regel
- Konfigurieren einer Quell- und Ziel-NAT-Regel
- Konfigurieren der Protokollierung
- Aktualisieren der Netzwerksicherheitsgruppe
- Konfigurieren des vNET-Peerings
- Hinzufügen einer Routentabelle

Erstellen oder Aktualisieren eines Regelstapels

In diesem Abschnitt aktualisieren Sie einen lokalen Regelstapel, indem Sie eine Regel hinzufügen und die Protokollierung aktivieren.

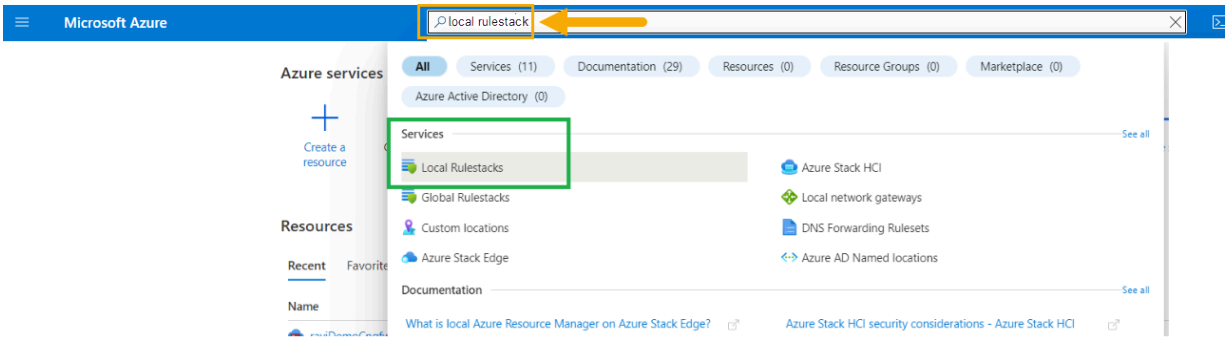
So aktualisieren Sie einen vorhandenen Regelstapel:

STEP 1 | Klicken Sie in der ARM-Konsole (Azure Resource Manager) für die Cloud NGFW-Ressource, die Sie konfigurieren möchten, auf **Rulestacks**. Der mit dem Cloud NGFW-Dienst verknüpfte Regelstapel wird zusammen mit der Ressourcengruppe angezeigt.

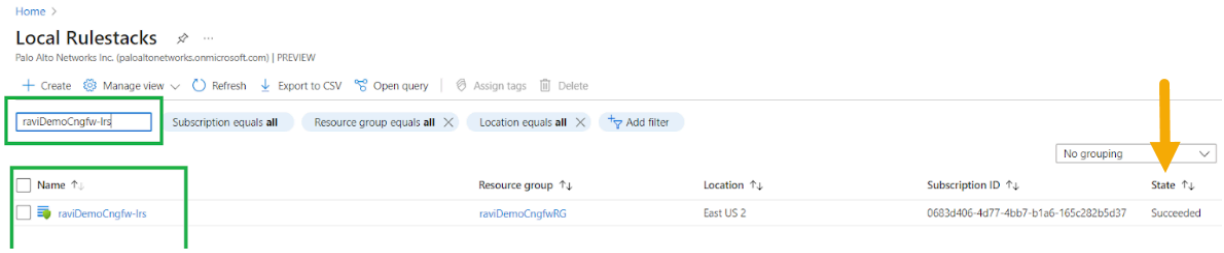


STEP 2 | Ändern Sie den Regelstapel, um Firewall-Regeln hinzuzufügen. Diese Regeln lassen einen gewissen Datenverkehr zu, während bestimmter Datenverkehr blockiert wird. Standardmäßig blockiert Cloud

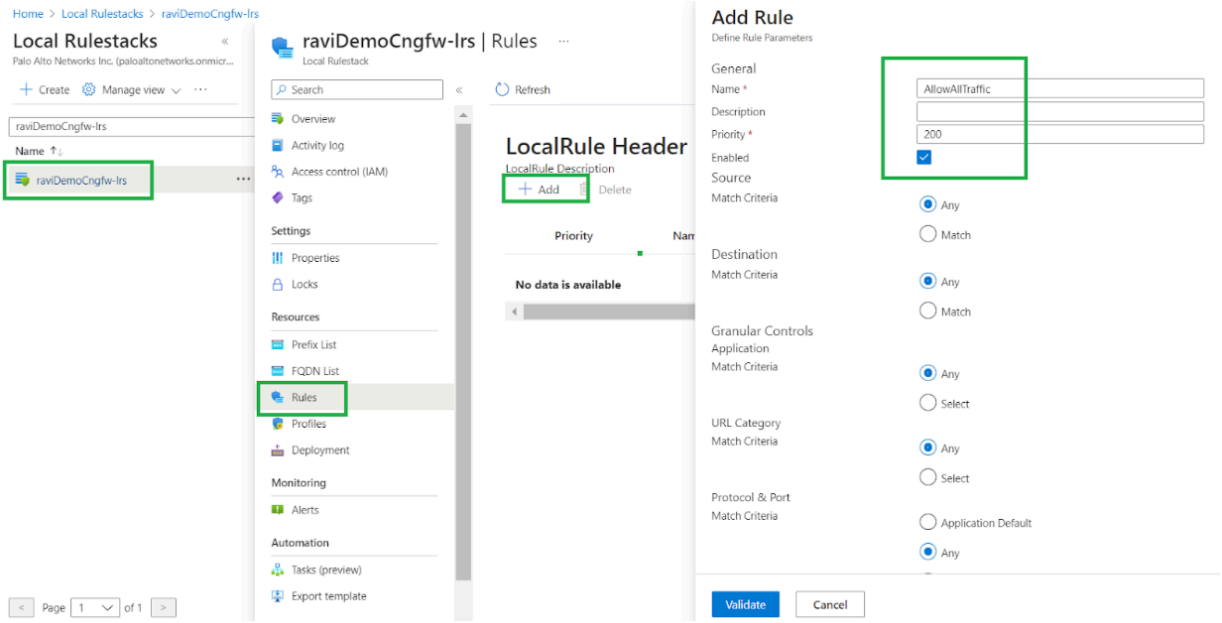
NGFW den gesamten Datenverkehr. Suchen Sie mithilfe der globalen Suchoption im Azure-Portal nach dem lokalen Regelstapel.



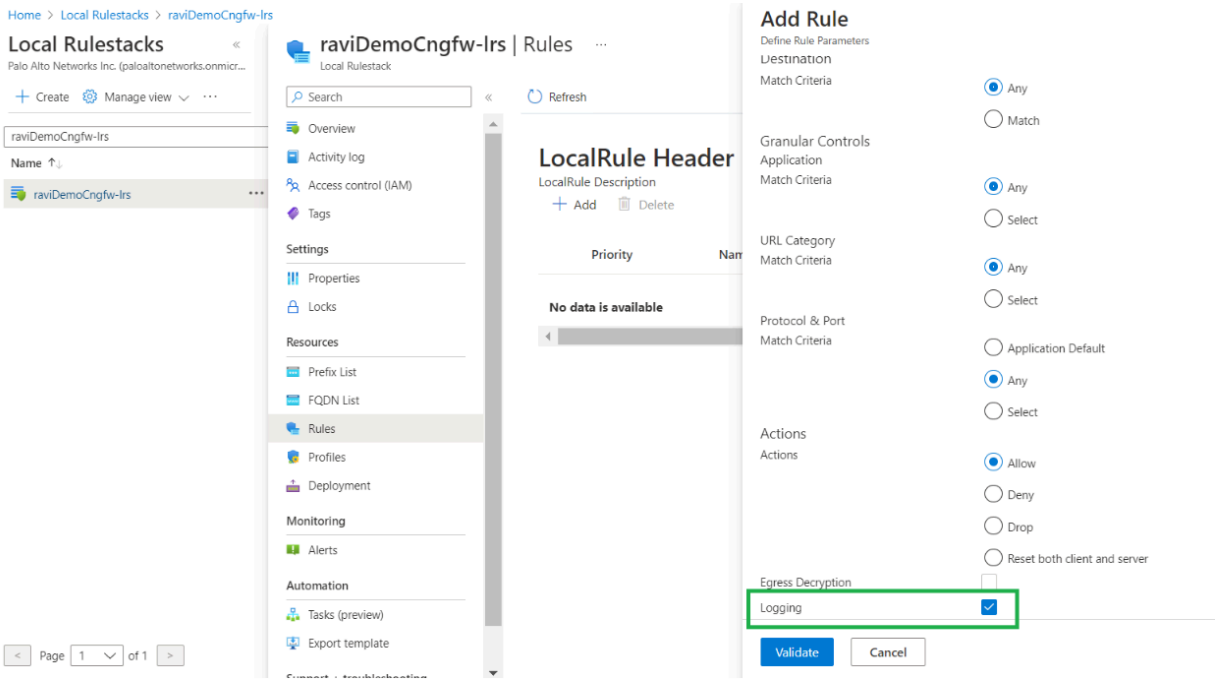
STEP 3 | Wählen Sie den lokalen Regelstapeldienst aus, um zur Liste der lokalen Regelstapel zu navigieren, die Ihrem Cloud NGFW-Abonnement zugeordnet sind. Suchen Sie nach einem lokalen Regelstapel und überprüfen Sie, dass der Status **Succeeded** lautet.



STEP 4 | Klicken Sie auf den Regelstapel, um Regeln hinzuzufügen. Ändern Sie im Fenster **Add Rule** die Regeln. Fügen Sie z. B. eine Regel hinzu, die Datenverkehr zulässt. Füllen Sie die Pflichtfelder aus und verwenden Sie die Standardeinstellungen für die restlichen Felder.



STEP 5 | Aktivieren Sie die Protokollierung für die Regel. Wählen Sie im Fenster „Add Rule“ die Option **Logging** aus.



STEP 6 | Klicken Sie auf **Validate**, dann auf **Add**, um die Regel zum Regelstapel hinzuzufügen.

Hinzufügen einer FQDN-Liste

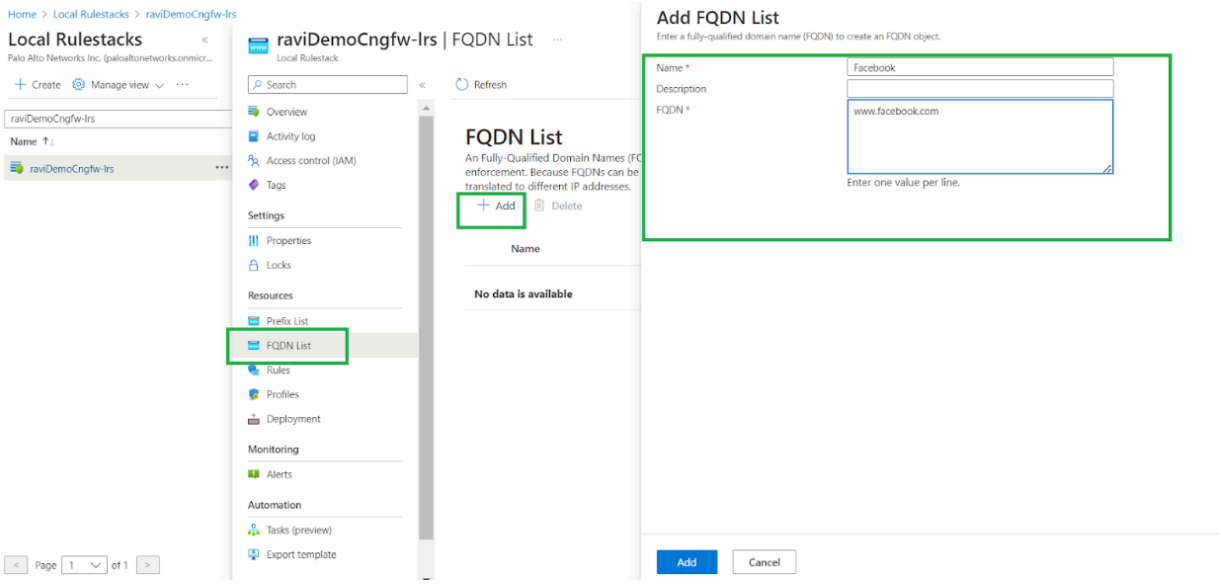
Fügen Sie dem lokalen Regelstapel eine FQDN-Liste hinzu, die Facebook enthält. Verwenden Sie diese Liste, um eine Regel hinzuzufügen, die den Datenverkehr zu facebook.com blockiert.

STEP 1 | Klicken Sie auf der lokalen Regelstapelseite für die Cloud NGFW-Ressource auf **FQDN List**.

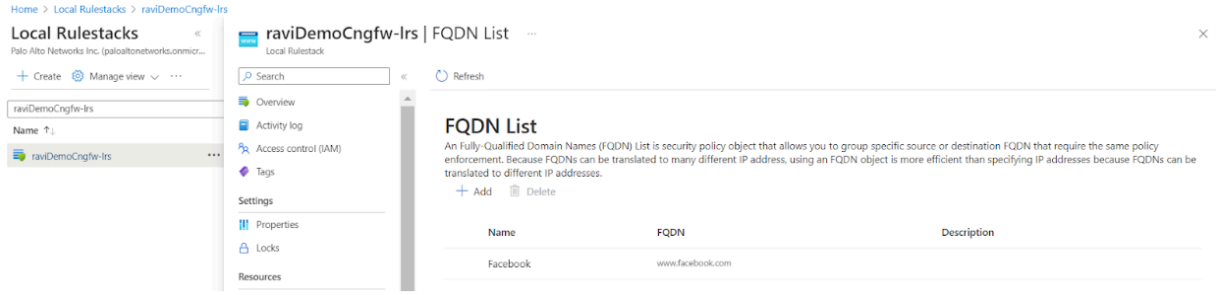
STEP 2 | Klicken Sie auf **Add (Hinzufügen)**.

STEP 3 | Geben Sie im Bildschirm **Add FQDN List** einen Namen und eine Beschreibung ein. Geben Sie im FQDN-Feld eine oder mehrere URLs ein, beispielsweise www.facebook.com. Pro Zeile des FQDN-Felds kann nur eine FQDN-URL vorhanden sein.

STEP 4 | Klicken Sie auf **Add (Hinzufügen)**.



STEP 5 | Überprüfen Sie, ob die angegebenen URLs in der FQDN-Liste angezeigt werden.



Hinzufügen einer Regel

Fügen Sie dem lokalen Regelstapel eine Regel hinzu, die der zuvor erstellten FQDN-Liste entspricht. Mit der Regel können Sie eine Aktion festlegen, z. B. die Unterbrechung des Datenverkehrs. Sie können z. B. eine Aktion auf die FQDN-Regel anwenden, um Datenverkehr zu unterbinden, der auf die URL „www.facebook.com“ zugreifen möchte.

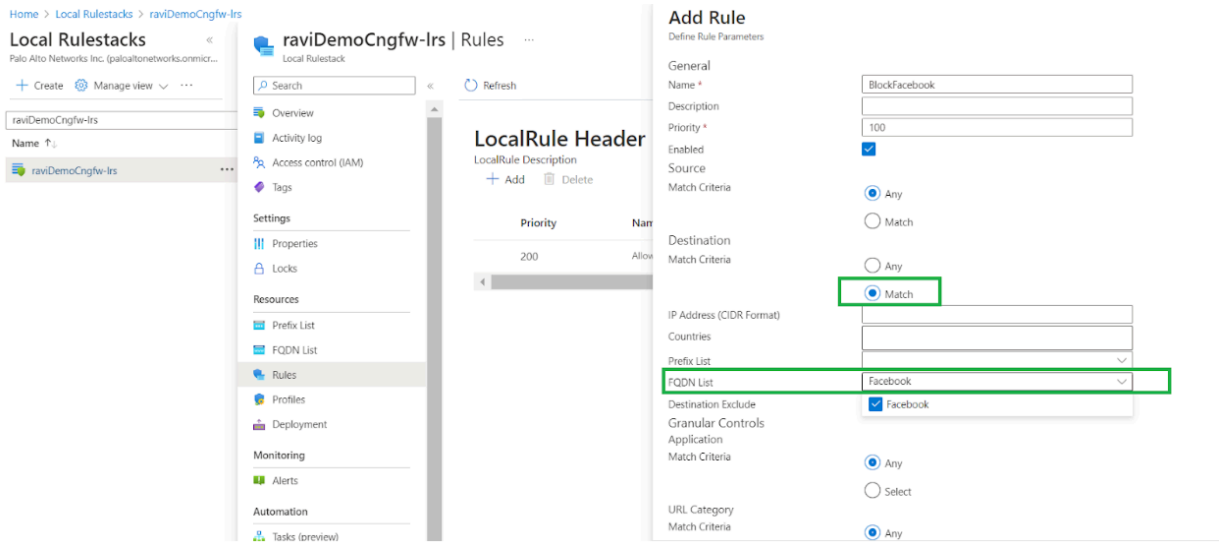
STEP 1 | Klicken Sie auf der lokalen Regelstapelseite für die Cloud NGFW-Ressource auf **Rules**.

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

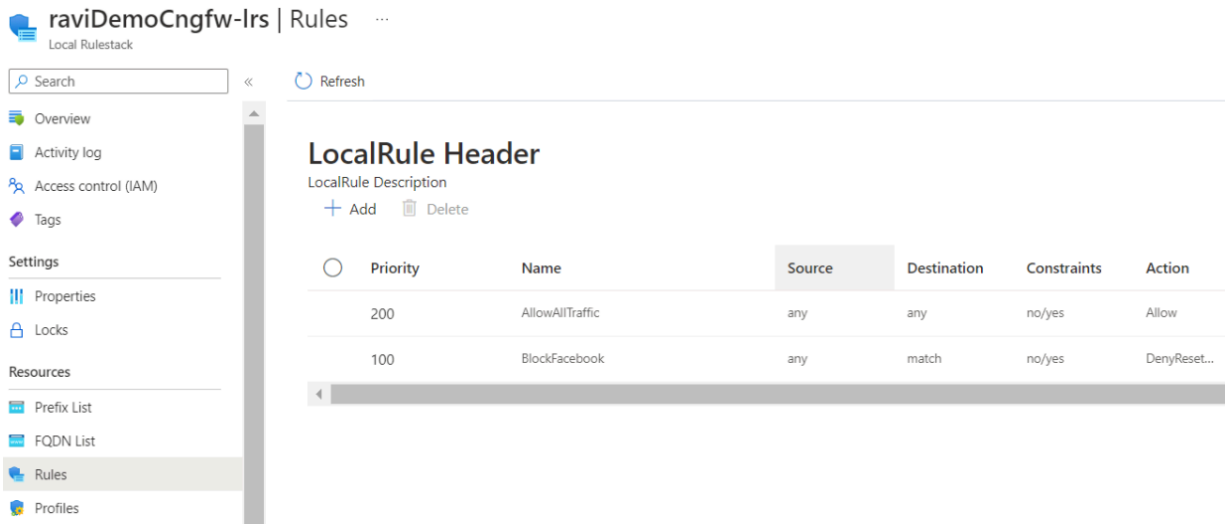
STEP 3 | Legen Sie im Bildschirm **Add Rule** die Kriterien zur Übereinstimmung fest. Wählen Sie im Feld **FQDN List** im Drop-down-Menü die Option „Facebook“ aus.

STEP 4 | Wählen Sie im Feld **Actions** die Option **Drop** aus.

STEP 5 | Klicken Sie auf **Add (Hinzufügen)**.

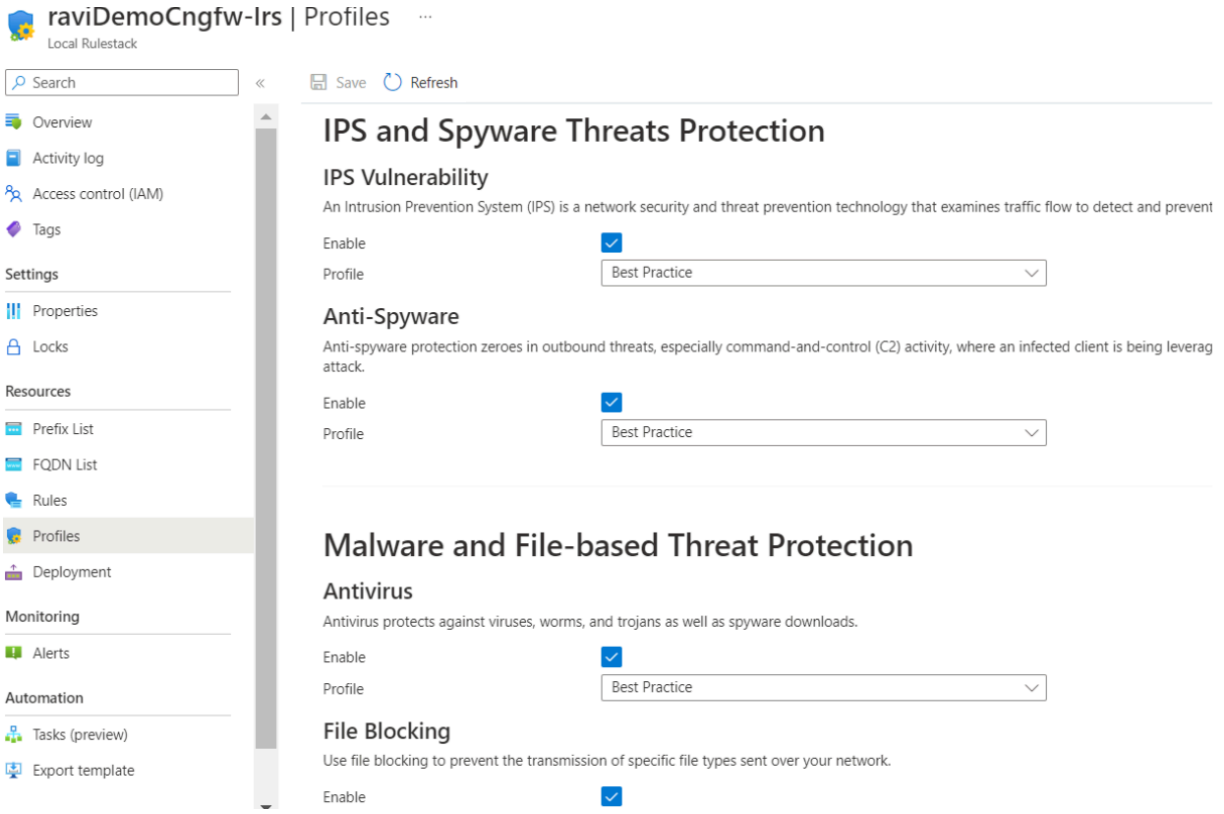


Beide Regeln erscheinen auf der Kopfseite des lokalen Regelstapels.



Als Teil des Cloud NGFW-Dienstes sind Sicherheitsprofile standardmäßig mit Best-Practice-Konfigurationen aktiviert. Sobald die Cloud NGFW im Netzwerk bereitgestellt ist, wird der

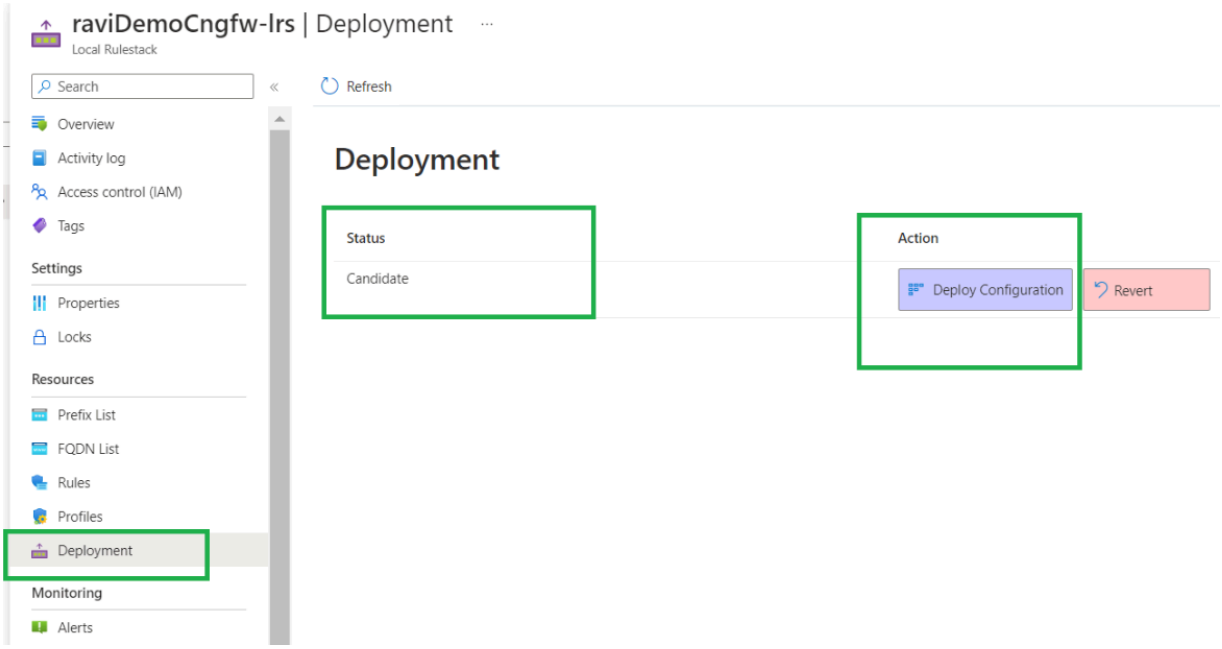
Datenverkehr mit den besten Sicherheitsprofilen gesichert. Dieser kann auf der Seite **Profiles** für den lokalen Regelstapel angezeigt werden.



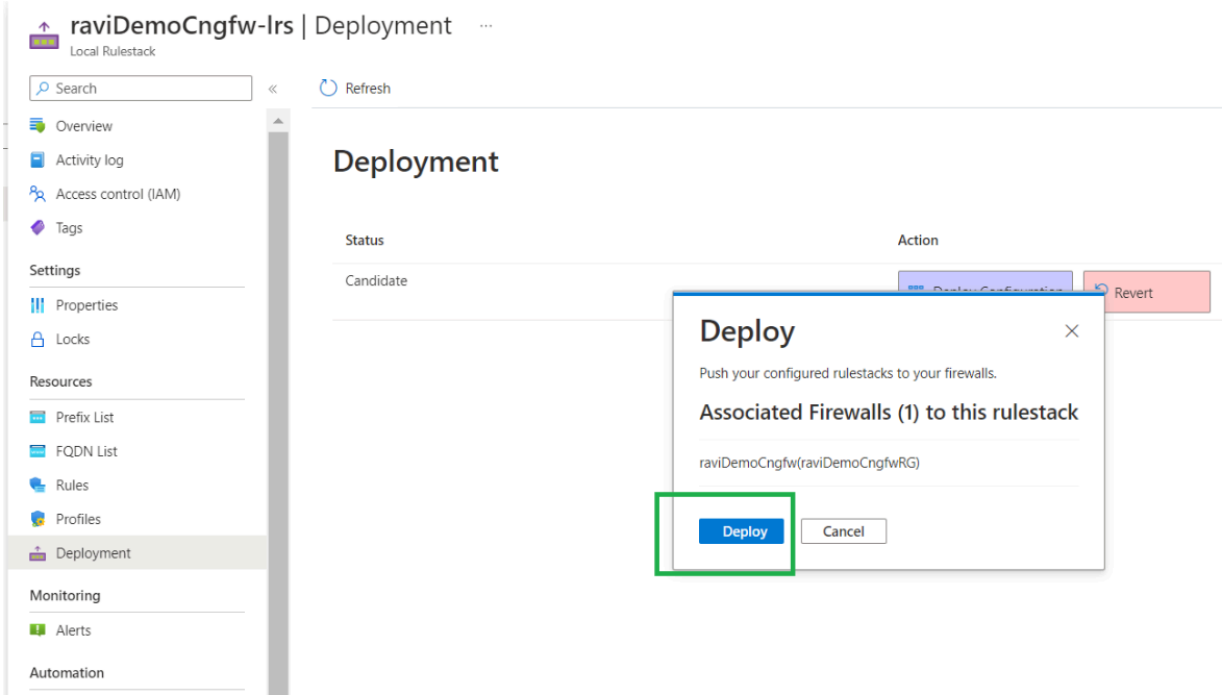
Nachdem Sie die Regeln geändert haben, stellen Sie sie auf dem lokalen Regelstapel bereit, der mit dem Cloud NGFW-Dienst verknüpft ist.

STEP 6 | Klicken Sie im lokalen Regelstapel auf **Deployment**. Auf der Bereitstellungsstatusseite wird „Candidate“ angezeigt. Dies bedeutet, dass die Konfiguration erstellt, aber nicht bereitgestellt wurde.

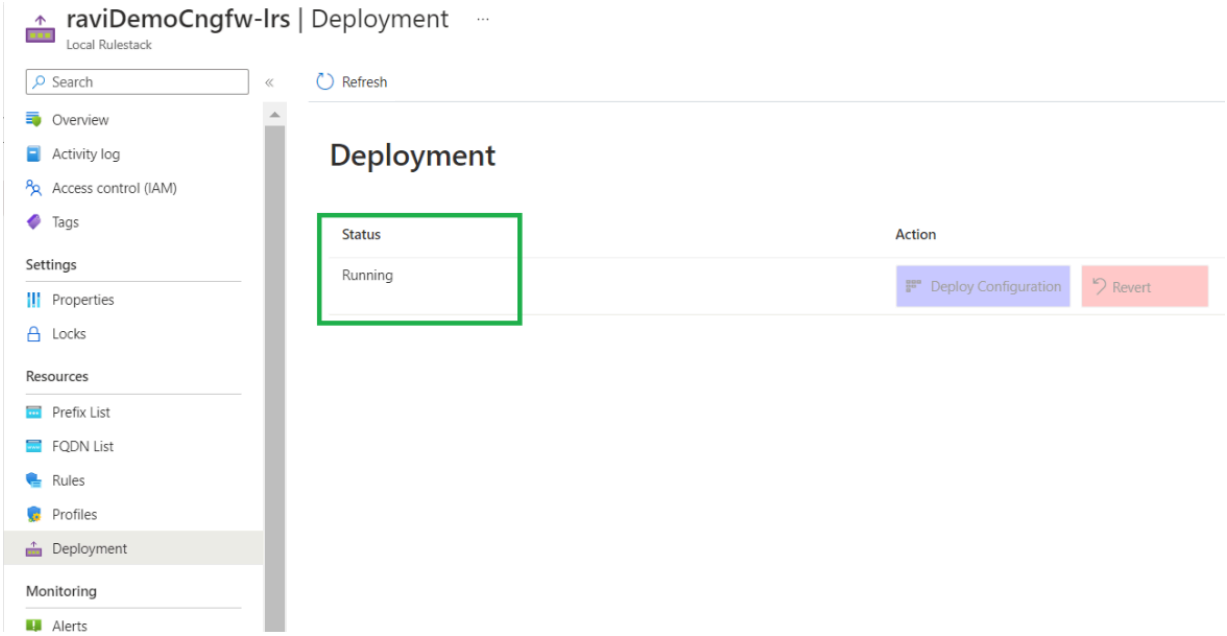
STEP 7 | Klicken Sie auf **Deploy Configuration**, um die Konfiguration auf dem Cloud NGFW-Dienst bereitzustellen. Sie müssen diesen Schritt ausführen, um die Regeln im Regelstapel bereitzustellen.



STEP 8 | Nachdem Sie auf **Deploy Configuration** geklickt haben, werden in einer Popup-Meldung die Firewalls angezeigt, die dem Regelstapel zugeordnet sind. Klicken Sie auf **Deploy**, um diesen Regelstapel auf allen zugehörigen Firewalls zu konfigurieren.



STEP 9 | Nach der erfolgreichen Bereitstellung der Konfiguration lautet der **Bereitstellungsstatus Running**.

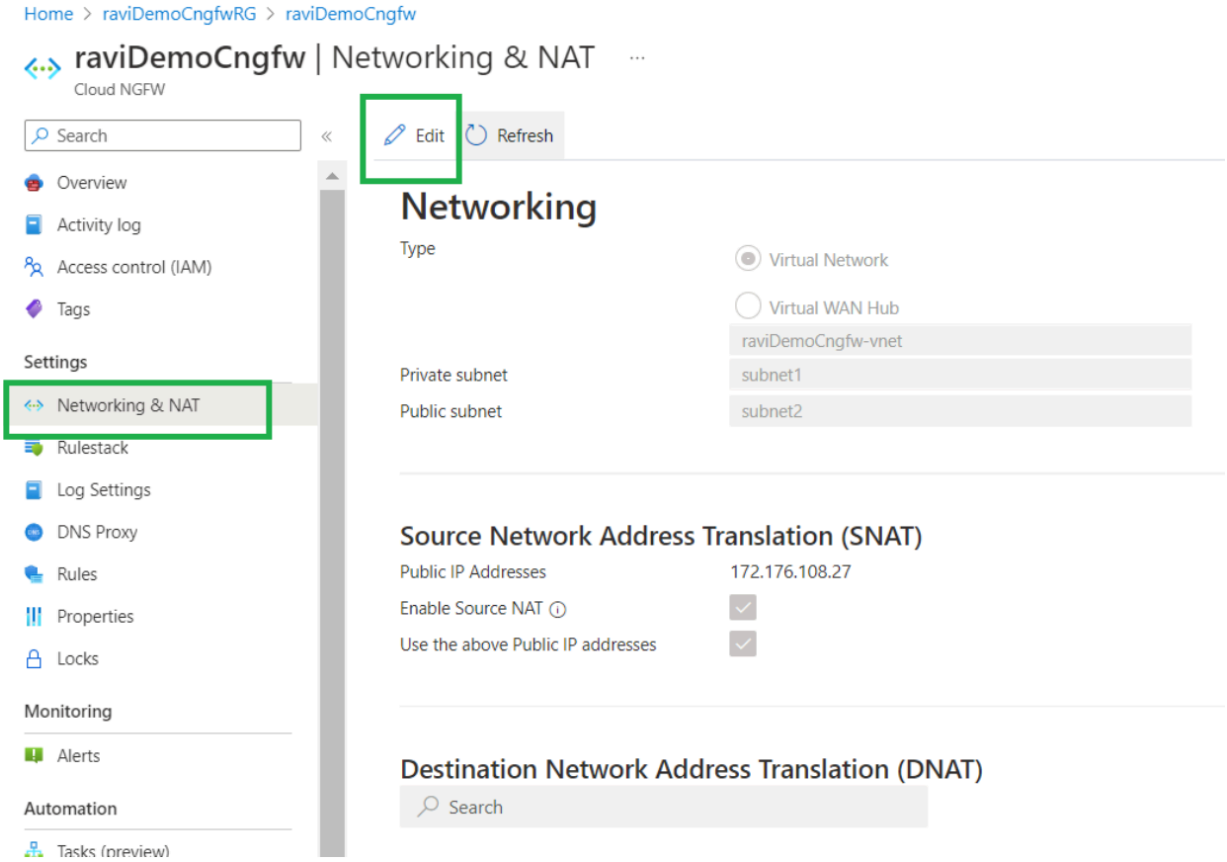


Konfigurieren einer Quell- und Ziel-NAT-Regel

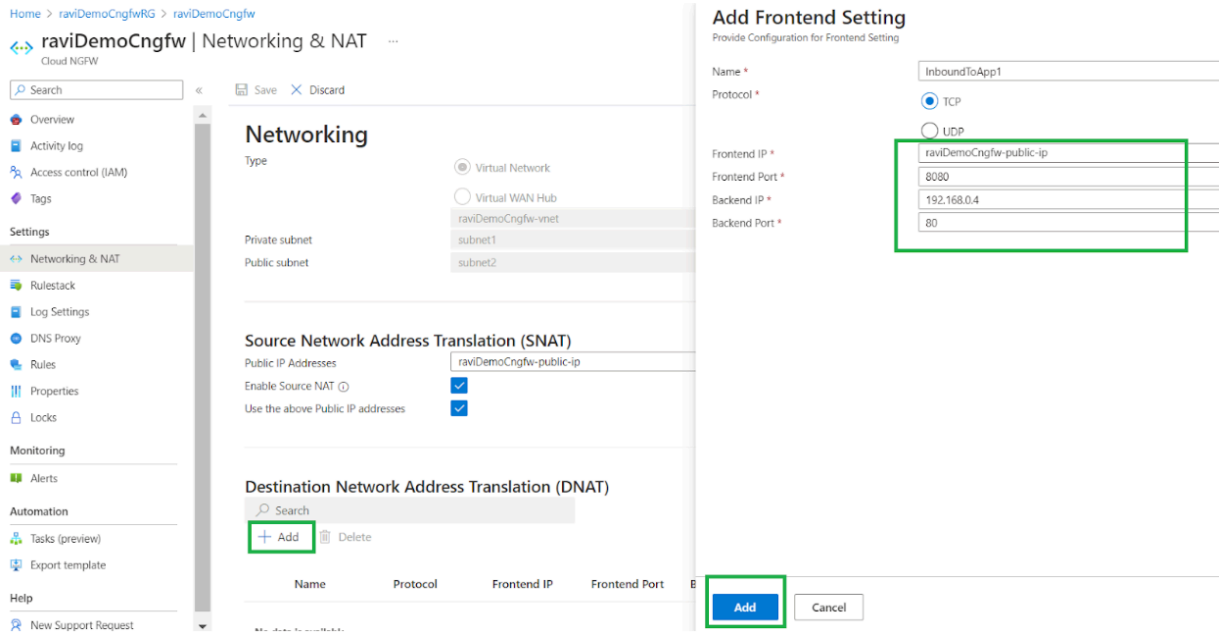
Sie können eine Ziel-NAT-Regel für den eingehenden Datenverkehr konfigurieren.

STEP 1 | Öffnen Sie die Einstellungen **Networking and NAT** für die Cloud NGFW-Ressource. Um festzustellen, ob die Quell-NAT-Einstellung aktiviert ist.

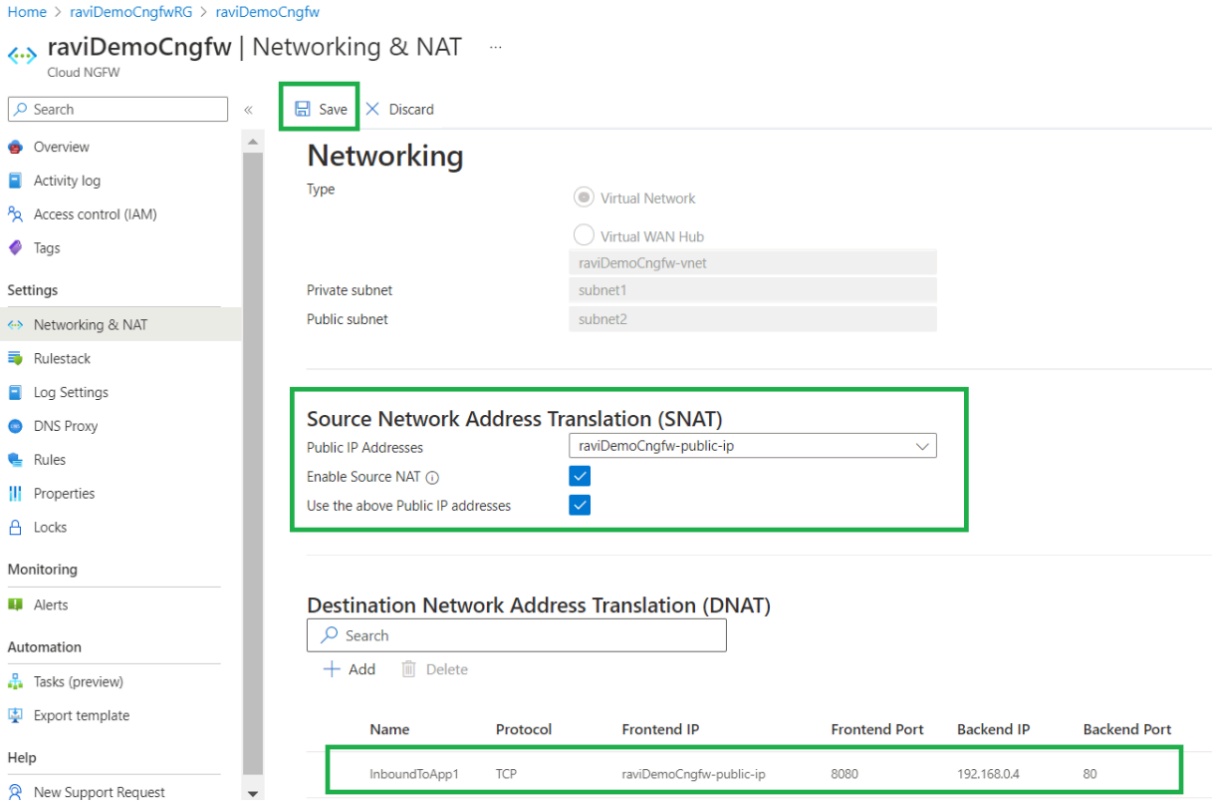
STEP 2 | Klicken Sie auf **Edit**, um die Ziel-NAT-Regel hinzuzufügen.



STEP 3 | Fügen Sie eine Ziel-NAT-Regel hinzu. Die Frontend-IP stellt die öffentliche IP-Adresse dar, die der Cloud NGFW zugeordnet ist. Geben Sie die Frontend-Portnummer ein und klicken Sie auf **Add**.



STEP 4 | Klicken Sie nach dem Hinzufügen der Ziel-NAT-Regel auf **Save**, um die Konfiguration auf der Cloud NGFW-Ressource bereitzustellen.



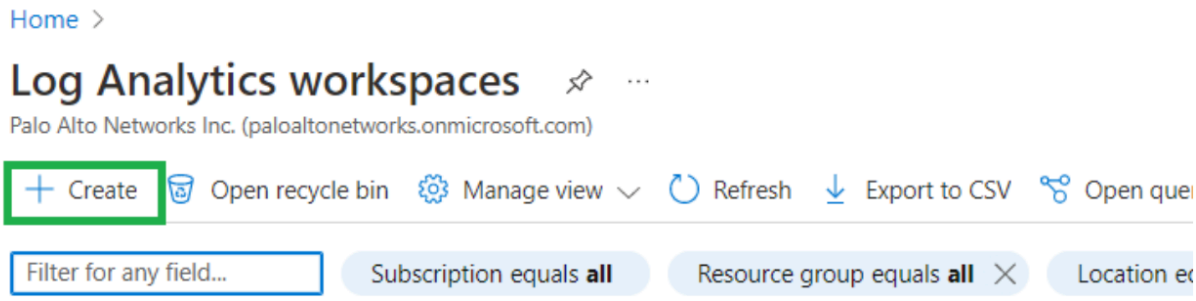
Die Frontend-Adresse wird nun über den konfigurierten Port durch Cloud NGFW umgeleitet. Der eingehende Datenverkehr fließt jetzt durch die Cloud NGFW.

Konfigurieren der Protokollierung

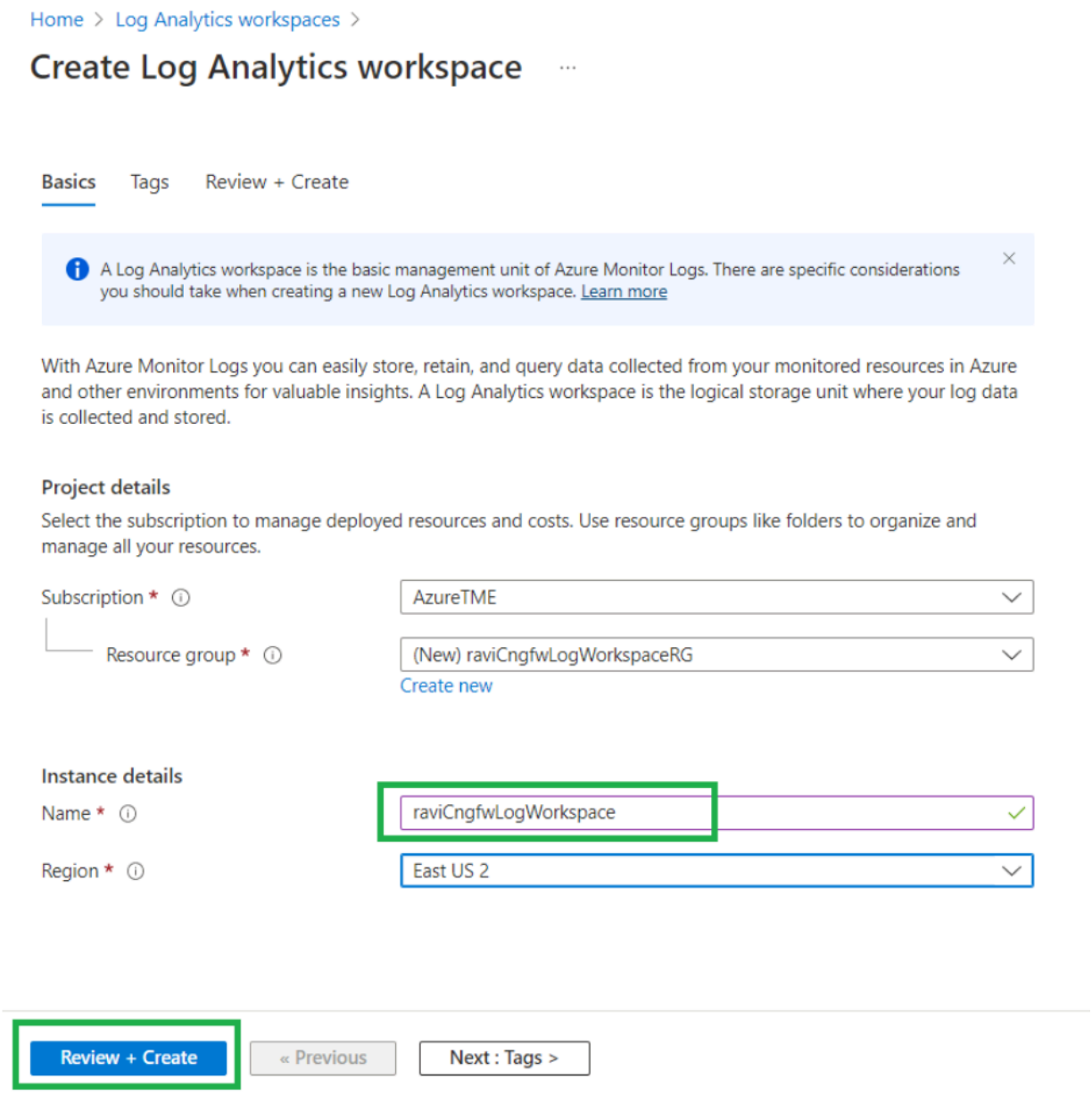
Bevor Sie die Protokollierung in der Cloud NGFW konfigurieren, erstellen Sie den Log Analytics Workspace in Azure.

STEP 1 | Suchen Sie im Azure-Portal nach dem **Azure Log Analytics Workspace**. Klicken Sie auf **Log Analytics Workspace**, um ihn als Dienst hinzuzufügen.

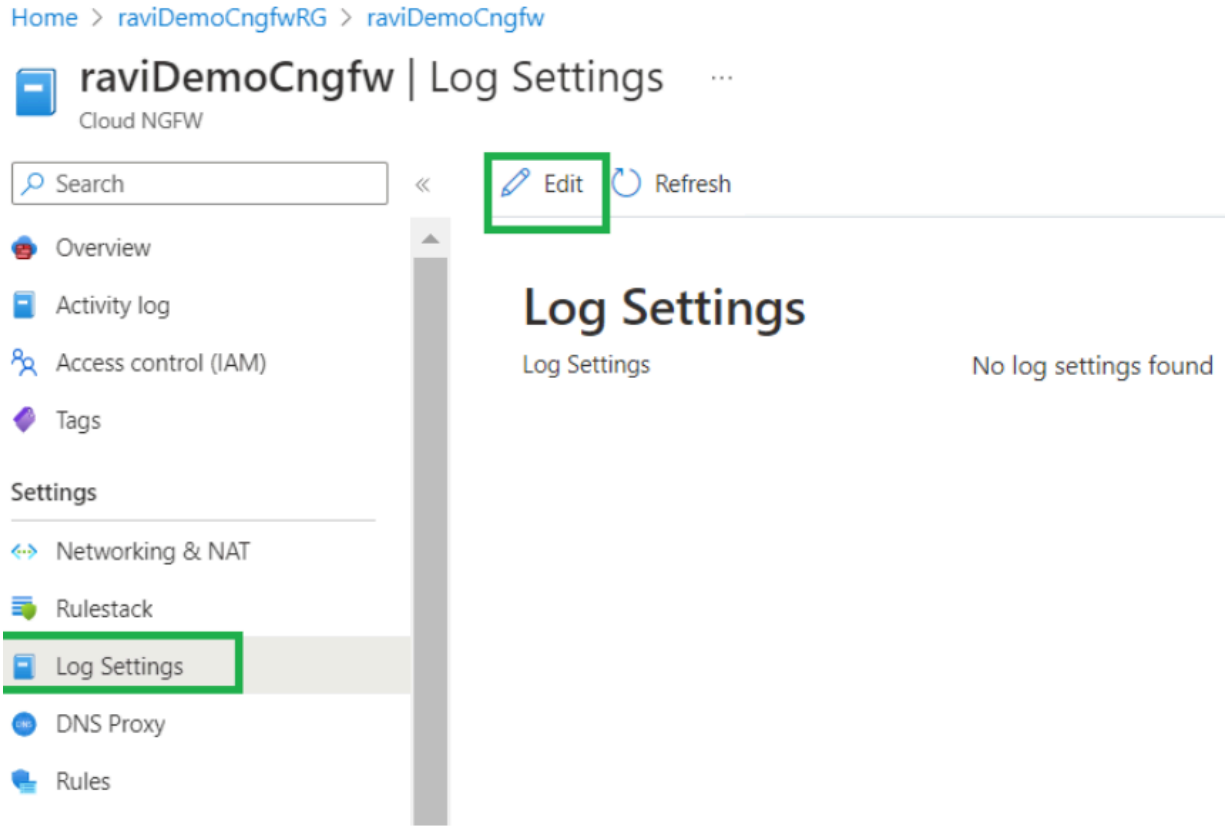
STEP 2 | Klicken Sie auf **Create**, um einen neuen **Log Analytics** Workspace zu erstellen:



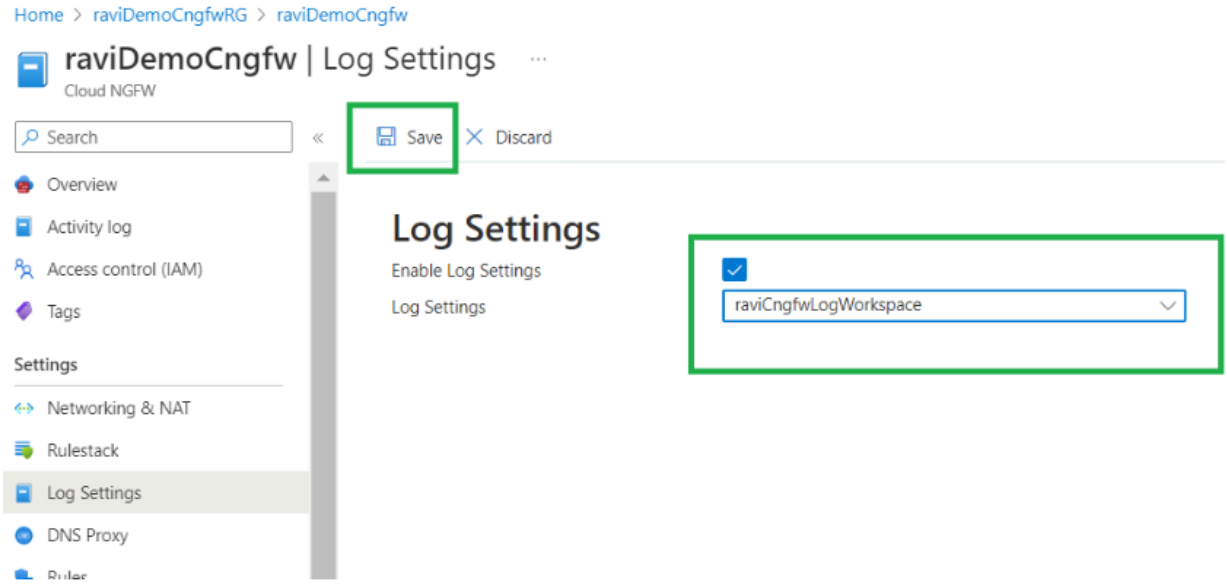
STEP 3 | Geben Sie beim Erstellen des Log Analytics Workspace die Details zu **Instance** an. Wählen Sie den **Name** des Arbeitsbereichs aus dem Drop-down-Menü und legen Sie die **Region** fest.



STEP 4 | Konfigurieren Sie die Protokolleinstellungen in der Cloud NGFW-Ressource. Wählen Sie **Log Settings (Protokolleinstellungen)** aus. Klicken Sie auf **Edit**.



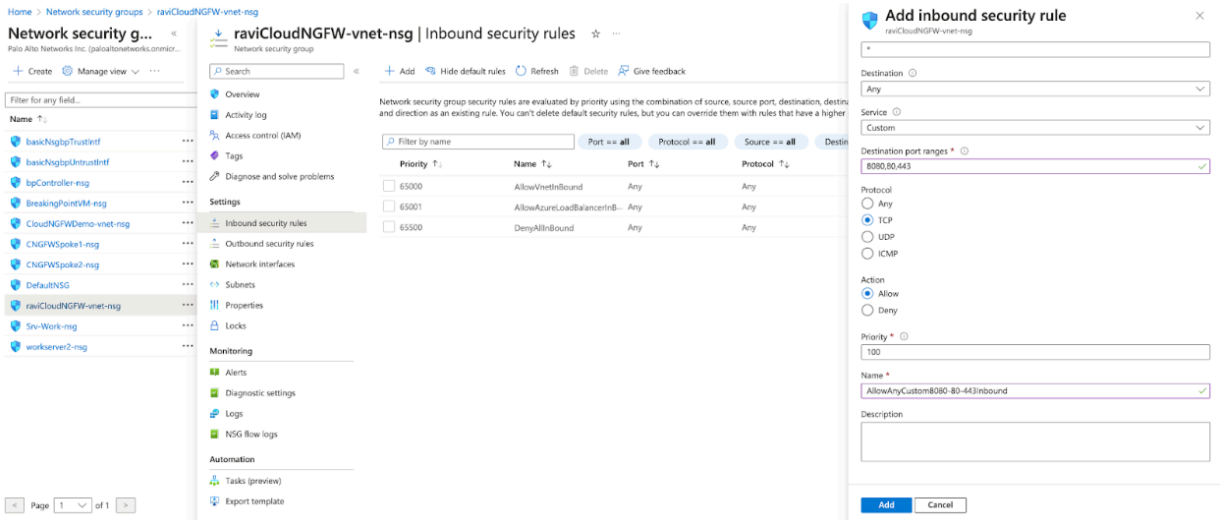
STEP 5 | Wählen Sie im Feld **Log Settings** den zuvor erstellten Log Analytics Workspace aus. Klicken Sie dann auf **Save**.



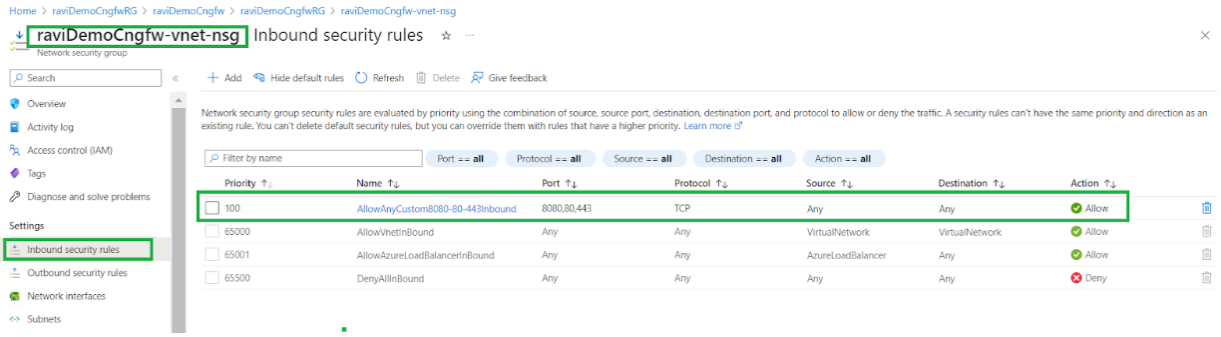
Aktualisieren der Netzwerksicherheitsgruppe

Aktualisieren Sie die Netzwerksicherheitsgruppe, die im Rahmen der Cloud NGFW-Bereitstellung erstellt wurde. Diese Sicherheitsgruppe ist als Teil des vNET im Cloud NGFW-Abonnement sowohl mit dem privaten als auch mit dem öffentlichen Subnetz verknüpft.

STEP 1 | Erlauben Sie Datenverkehr als Teil der NAT-Regelkonfiguration des Frontends (Ziel). Erlauben Sie HTTP- und HTTPS-Verkehr, sodass von Anwendungs-vNETs aus über die Cloud NGFW auf das Internet zugegriffen werden kann.



STEP 2 | Klicken Sie auf **Add**, um diese Eingangssicherheitsregel zu integrieren:



Konfigurieren von vNET-Peering

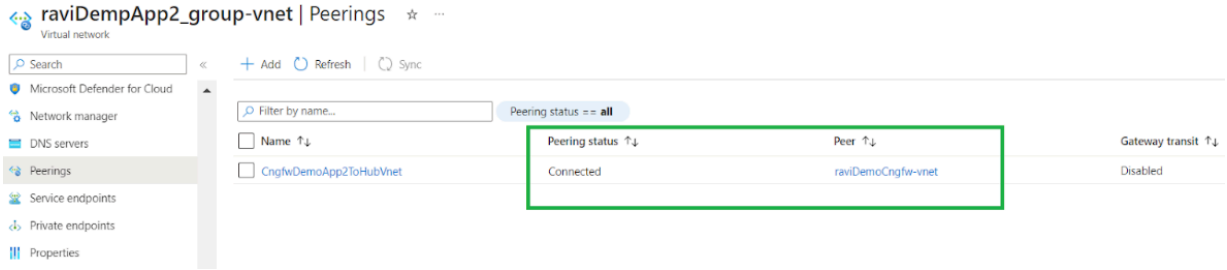
So konfigurieren Sie vNET-Peering:

STEP 1 | Suchen Sie Ihr vNET und wählen Sie **Peerings** aus.

STEP 2 | Klicken Sie auf **Add**, um ein neues Peering zu erstellen.

STEP 3 | Geben Sie einen Namen für das Peering an und behalten Sie die Standardeinstellungen bei.

STEP 4 | Wählen Sie das Hub-vNET aus, für das Sie ein Peering herstellen möchten. Beim Bereitstellen der Cloud NGFW in einem vNET unter Verwendung eines vorhandenen vNET-Hubs sollte die Mindestgröße /25 betragen. Sie müssen über 2 Subnetze mit der Mindestgröße /26 verfügen. Diese Subnetze müssen an den Dienst **PaloAltoNetworks.Cloudngfw/firewalls** delegiert werden.



STEP 5 | Konfigurieren Sie vNET-Peering zwischen zusätzlichen vNETs, indem Sie die in diesem Abschnitt beschriebenen Schritte wiederholen.

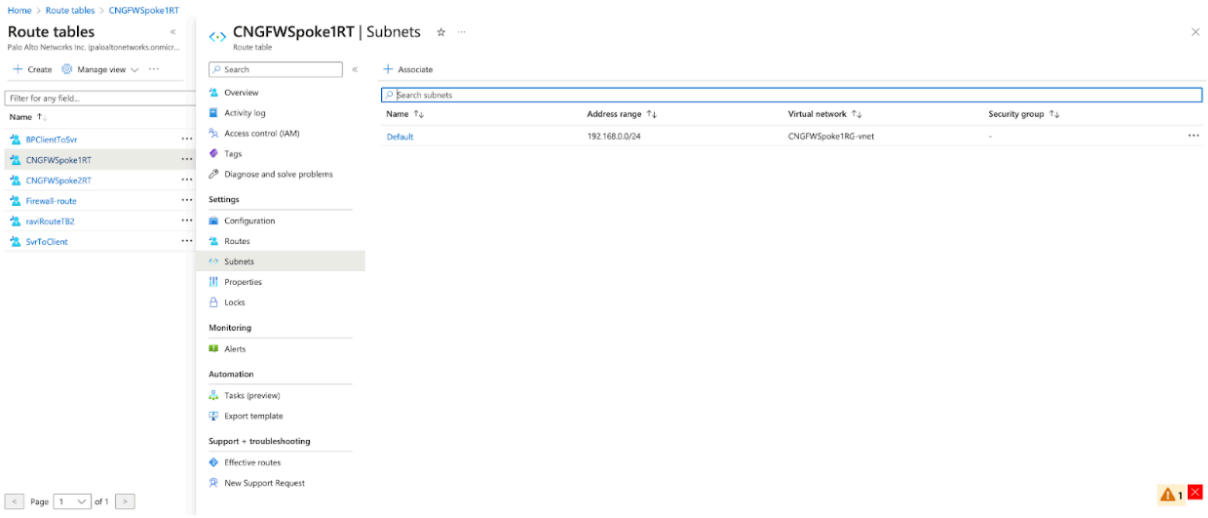
Fügen Sie eine Routing-Tabelle hinzu, um den Datenverkehr durch die Cloud NGFW zu leiten.

STEP 1 | Suchen Sie in der Suchleiste des Azure-Portals nach der **Route table**.

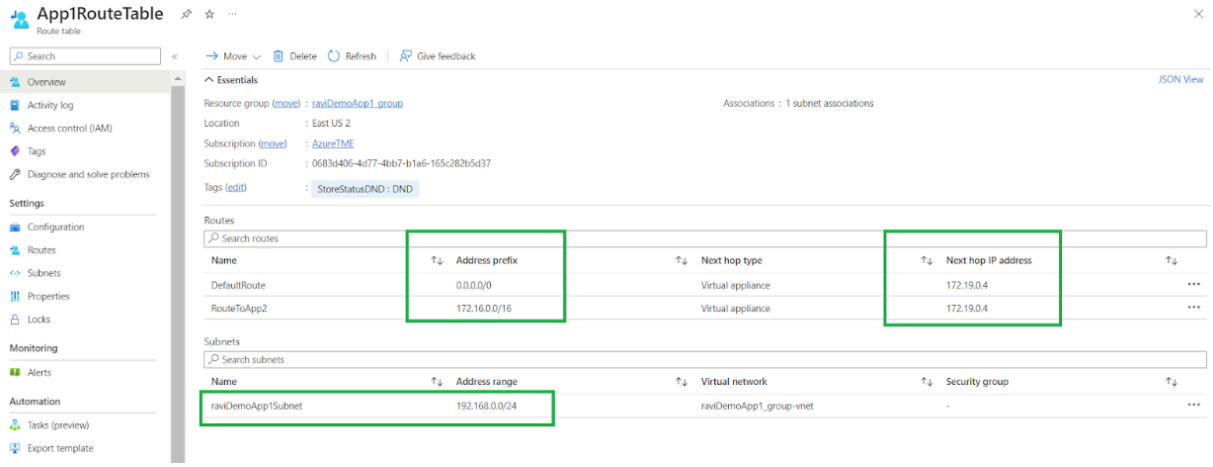
STEP 2 | Klicken Sie auf **Create**, um eine neue Routing-Tabelle zu erstellen.

STEP 3 | Füllen Sie die Felder der Routing-Tabelle aus und klicken Sie dann auf **Review+create**.

STEP 4 | Wählen Sie nach dem Erstellen der Routing-Tabelle den Abschnitt **Subnets** aus und ordnen Sie die Tabelle dem Subnetz zu.

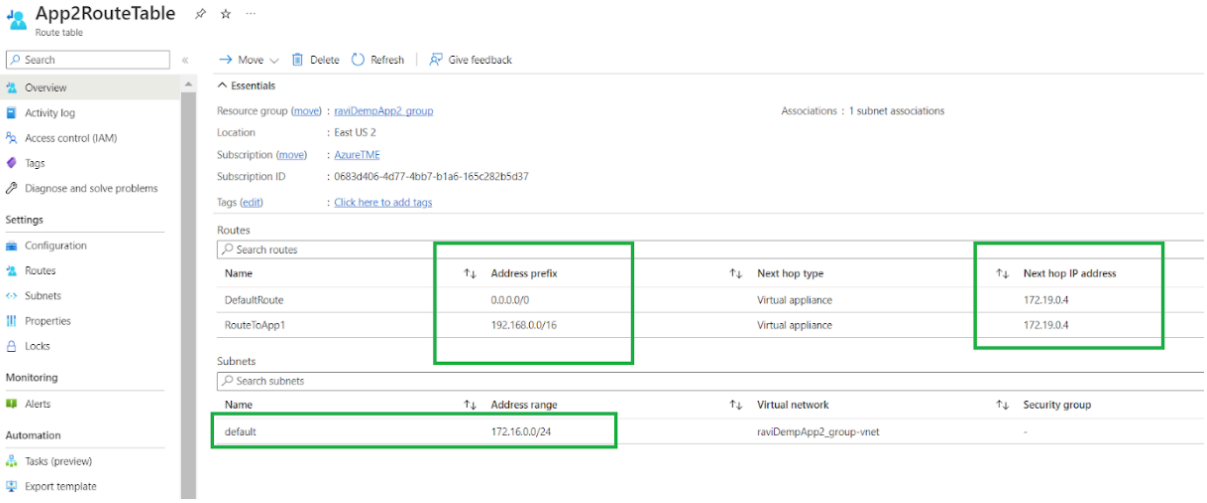


STEP 5 | Konfigurieren Sie die Standardroute für ausgehenden Datenverkehr und routen Sie ihn in Richtung des Subnetzes (für Ost-West-Datenverkehr) mit dem nächsten Hop als private IP-Adresse der Cloud NGFW.



STEP 6 | Ordnen Sie eine oder mehrere Routing-Tabellen einem anderen Subnetz aus dem vNET zu. Konfigurieren Sie eine Standardroute (für ausgehenden Datenverkehr) und routen Sie ihn zu einem

anderen Subnetz (für Ost-West-Datenverkehr) mit dem nächsten Hop als private IP-Adresse der Cloud NGFW.



Bereitstellen der Cloud NGFW in einem vWAN

Die Cloud NGFW kann nahtlos im vWAN-Hub als skalierbare Firewall-Lösung bereitgestellt werden, um den Datenverkehr zwischen kritischen Workloads zu sichern, die in einem globalen Hybridnetzwerk zwischen Azure und vor Ort gehostet werden. Weitere Informationen zu Azure vWAN und den verfügbaren Features und Fähigkeiten finden Sie in der Azure Virtual WAN-Dokumentation.

Beachten Sie Folgendes, wenn Sie Cloud NGFW in einem vWAN bereitstellen:

- Für eine NGFW-Ressource wird eine private IP-Adresse verwendet. Konfigurieren Sie für vWAN-Umgebungen die vWAN-Hub-Routing-Richtlinie so, dass der Datenverkehr für den Dienst *gezielt gesteuert* wird. Das heißt, der Datenverkehr verlässt eine Schnittstelle und kehrt zurück, bevor er ins Internet gelangt.
- Die Bereitstellung eines neuen vWAN-Hubs kann ungefähr 30 Minuten dauern. Sie können den Status eines neu erstellten vWAN-Hubs im Feld **Routing Status** im Abschnitt **Essentials** von **Overview** überprüfen.

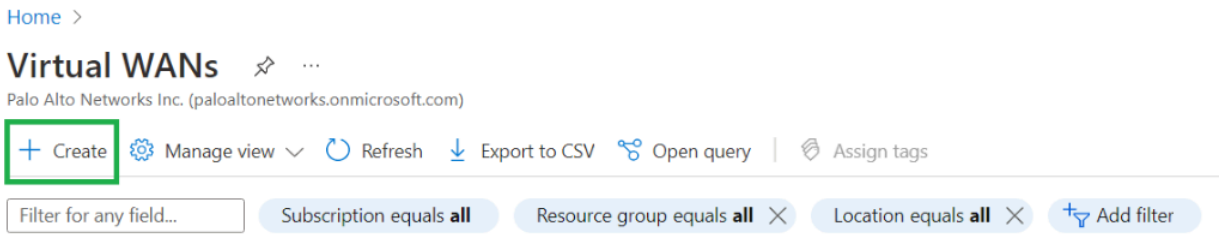
Die Cloud NGFW für die Azure vWAN-Bereitstellung:

- Ist mithilfe des SaaS-Frameworks vollständig in das Azure Virtual WAN integriert.
- Wird direkt im virtuellen vWAN-Hub bereitgestellt.
- Nutzt Routing-Absichten und Richtlinien, um zu steuern, welcher Datenverkehr vom Cloud NGFW-Dienst überprüft wird.
- Ermöglicht die Durchsetzung einheitlicher Sicherheitsrichtlinien für den Datenverkehr zwischen Hubs und Regionen

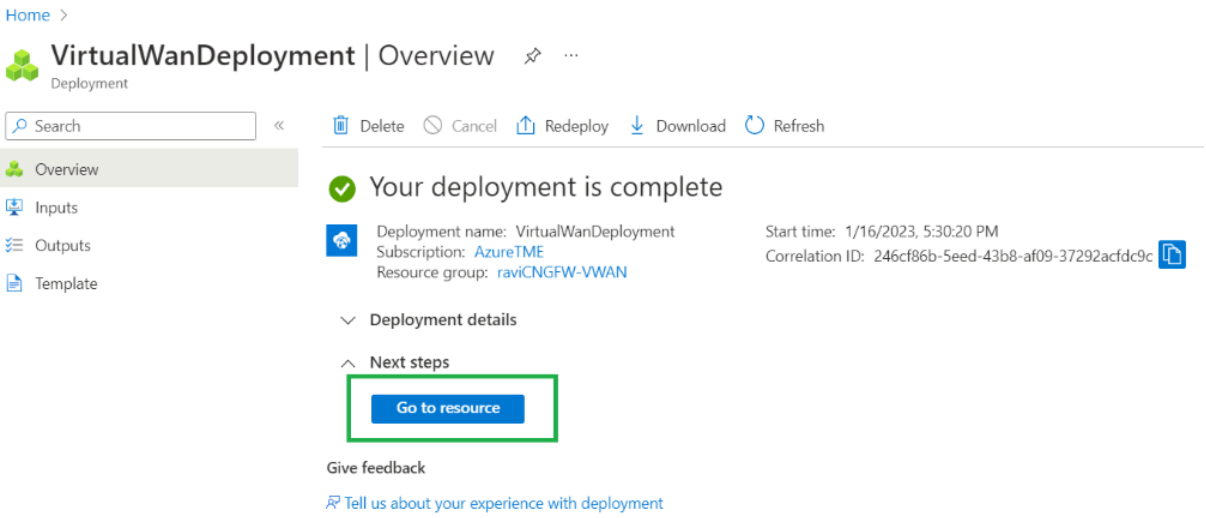
Voraussetzungen

Um Cloud NGFW in einem vWAN bereitzustellen, benötigen Sie ein Azure-Abonnement. Dieses Abonnement sollte über eine **Eigentümer-** oder **Mitwirkenden**-Rolle verfügen.

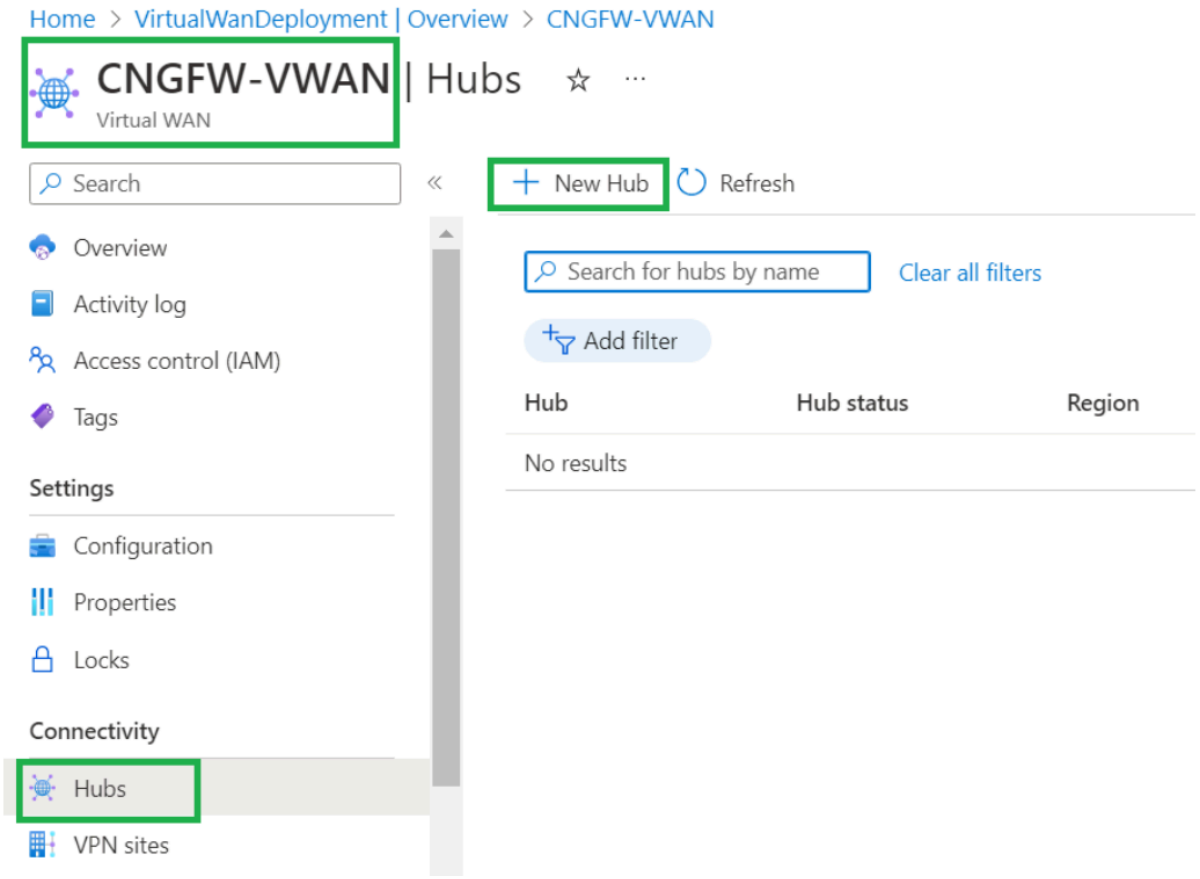
STEP 1 | Melden Sie sich beim Azure-Portal an und suchen Sie nach **Virtual WAN**. Klicken Sie auf **Create**, um einen virtuellen WAN-Dienst zu erstellen.



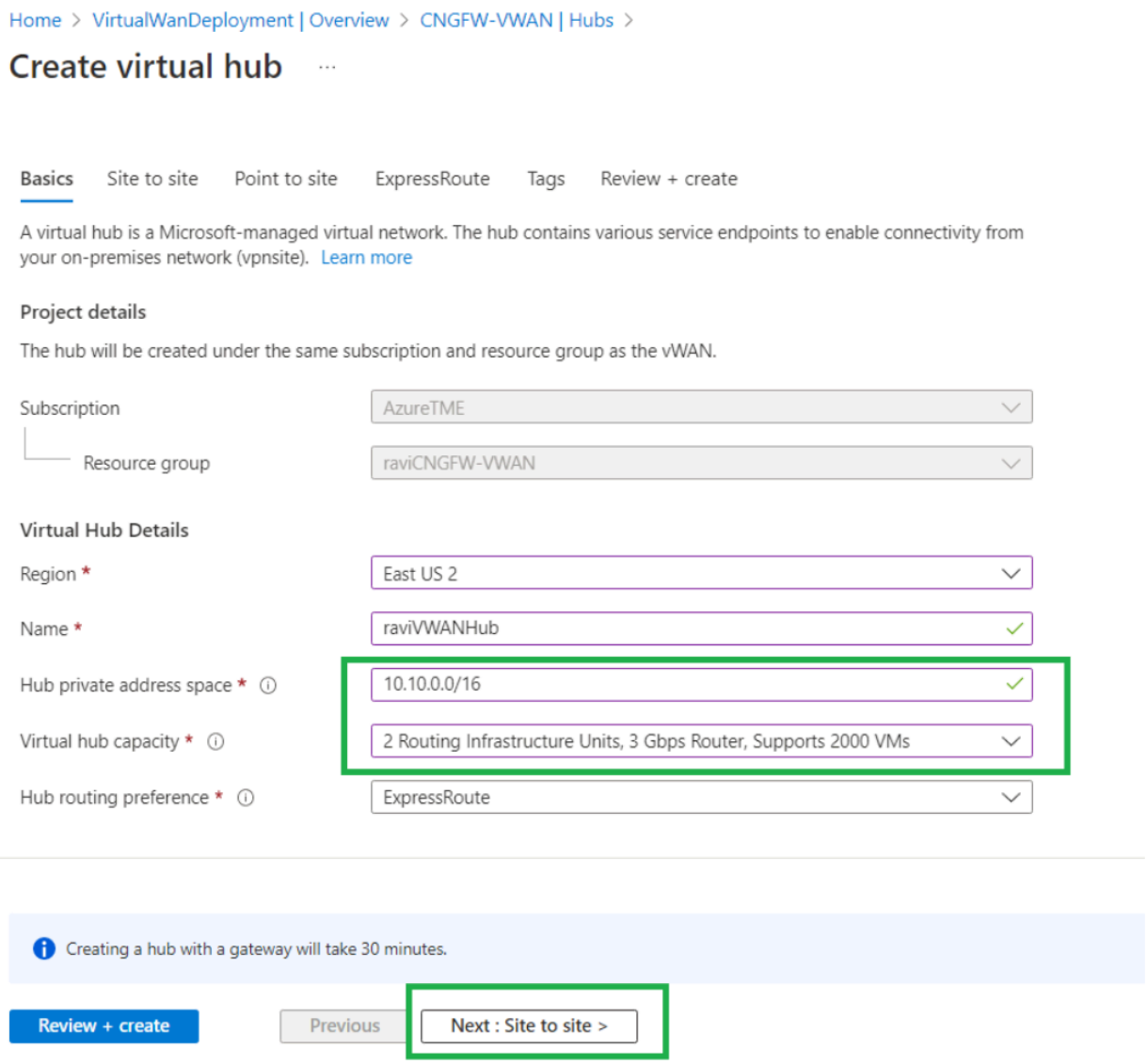
STEP 2 | Klicken Sie nach der erfolgreichen Erstellung des Virtual WAN-Dienstes auf **Go to resource**.



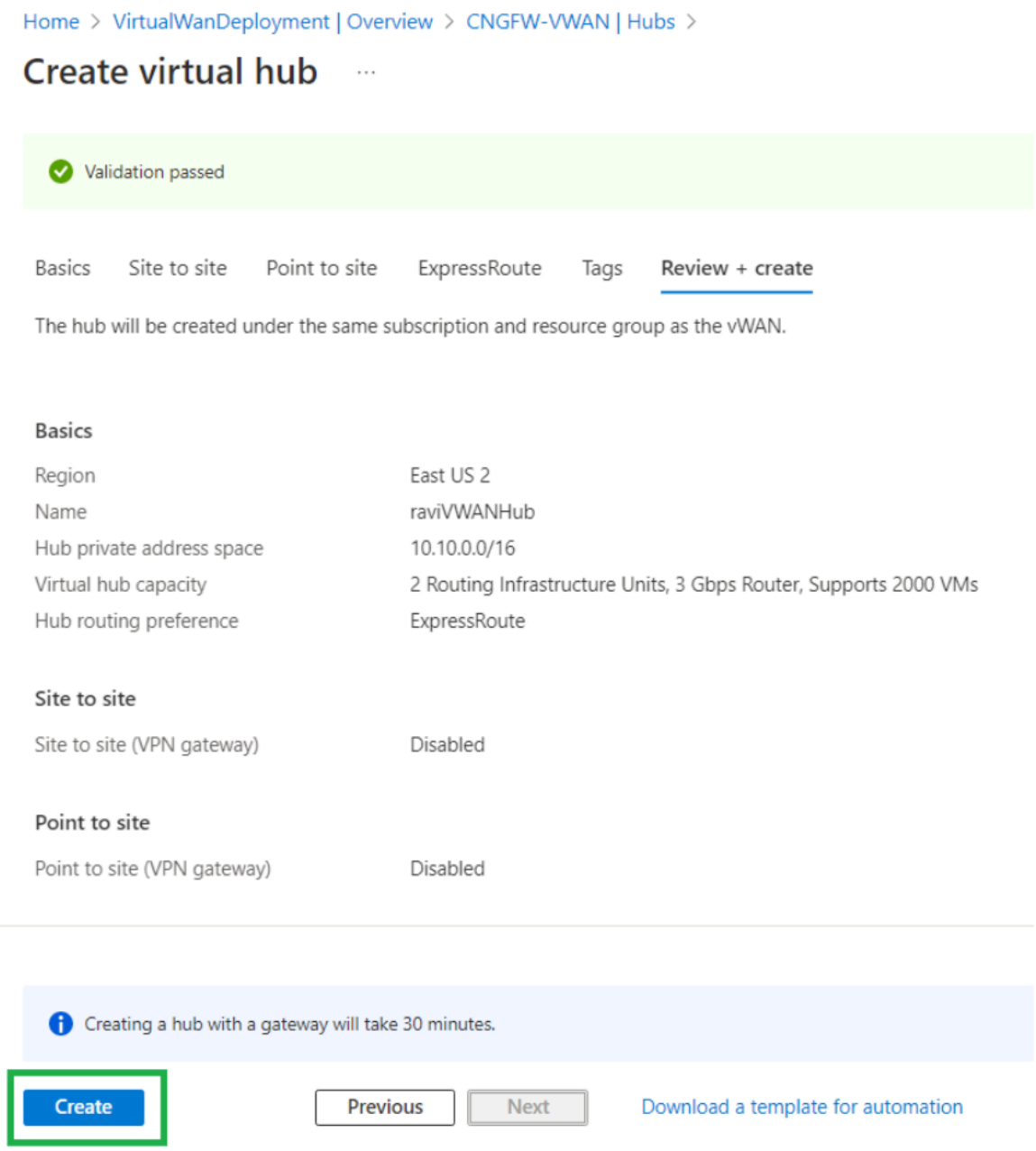
STEP 3 | Fügen Sie dem von Ihnen erstellten virtuellen WAN einen Hub hinzu. Wählen Sie **Connectivity** > **Hubs** aus. Klicken Sie auf **New Hub**.



STEP 4 | Konfigurieren Sie die **Virtual Hub Details**. Geben Sie die **private Hub-Adresse** und **die virtuelle Hub-Kapazität** an und klicken Sie dann auf **Next: Site to Site**.

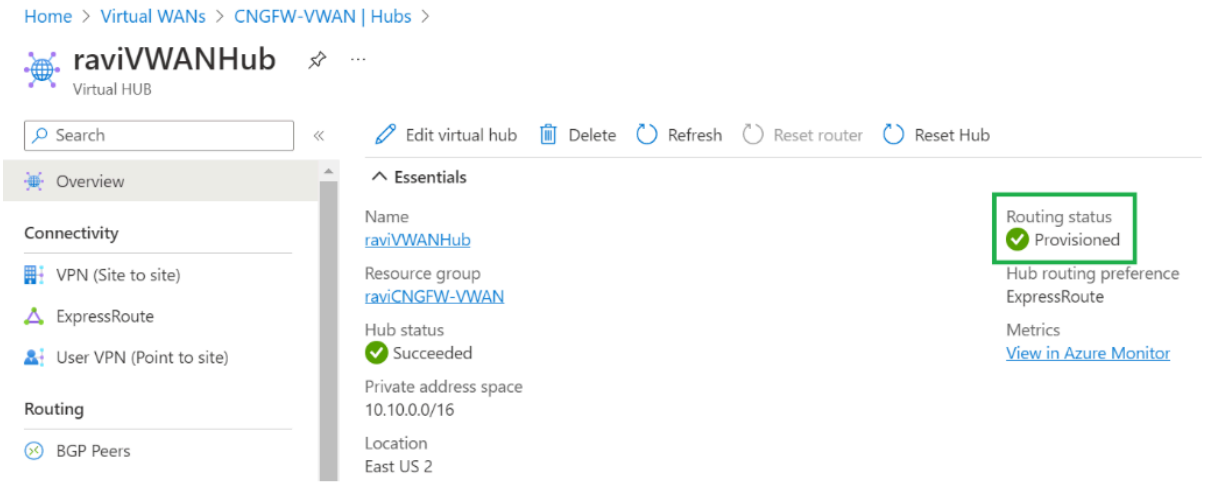


STEP 5 | Klicken Sie nach der Validierung der Konfiguration auf **Create**, um den virtuellen WAN-Hub zu erstellen.



STEP 6 | Überprüfen Sie, ob der **Routing Status Provisioned** lautet.

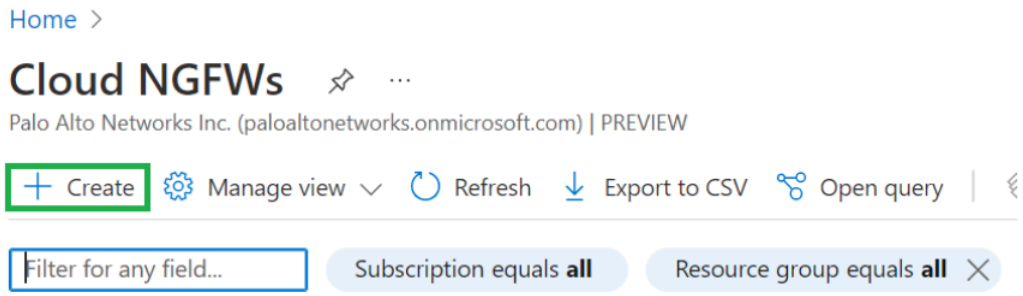
*Die Bereitstellung eines neuen vWAN-Hubs kann ungefähr 30 Minuten dauern. Verwenden Sie die Seite **Overview**, um den Routing-Status anzuzeigen.*



STEP 7 | Melden Sie sich beim Azure-Portal an und suchen Sie nach **Cloud NGFWs by Palo Alto Networks**.

STEP 8 | Klicken Sie auf **Cloud NGFWs by Palo Alto Networks**, um mit der Erstellung des Cloud NGFW-Dienstes für Azure von Palo Alto Networks zu beginnen.

STEP 9 | Klicken Sie im Bildschirm **Cloud NGFWs** auf **Create**. Diese Zielseite ist bereits mit Cloud NGFW-Instanzen ausgefüllt, wenn Sie die Ressource zuvor erstellt haben.

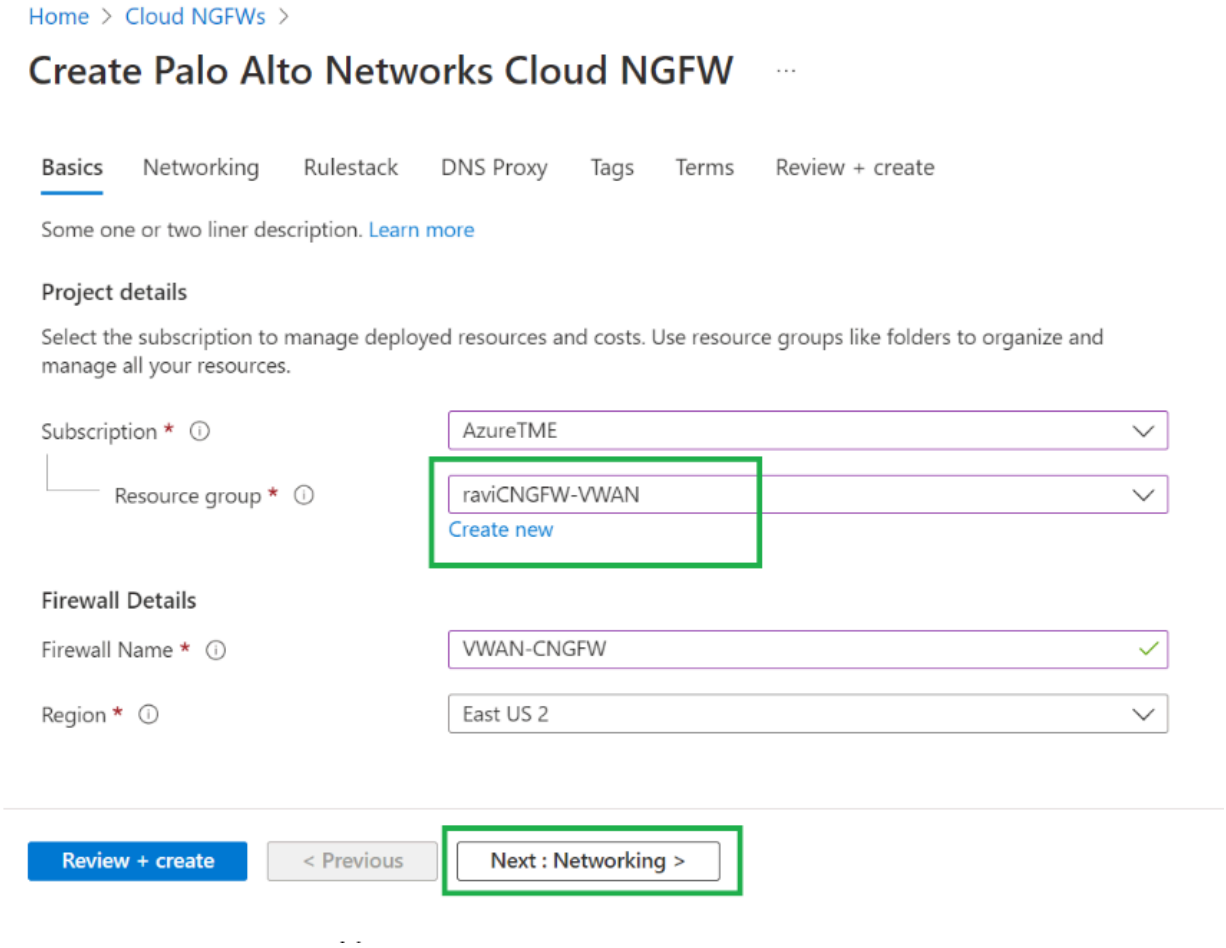


STEP 10 | Geben Sie im Bildschirm **Create Palo Alto Networks Cloud NGFW** im Abschnitt **Project details** grundlegende Konfigurationsinformationen ein.

Verwenden Sie die Informationen in der folgenden Tabelle, um **Projektdetails** anzugeben.

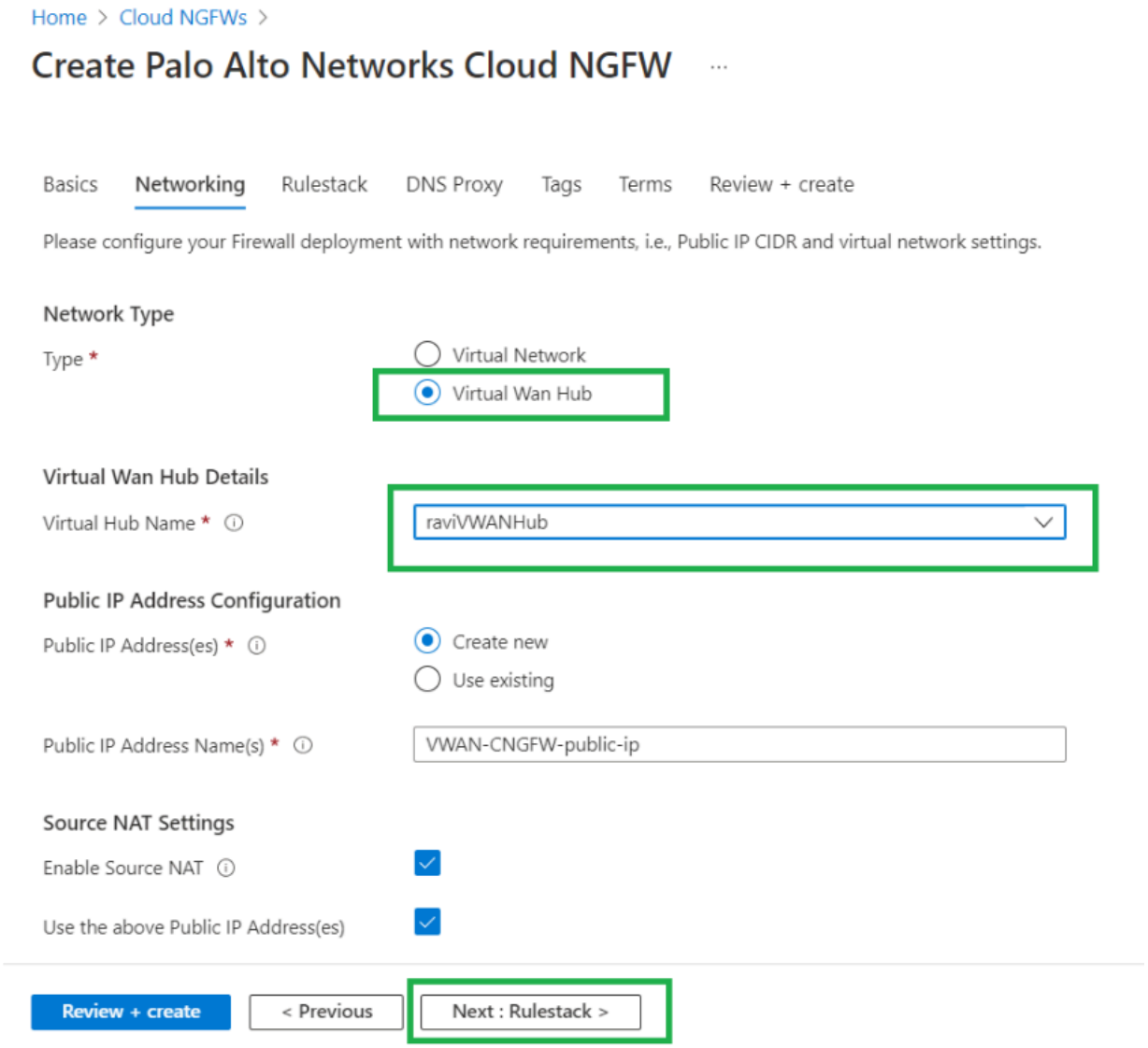
Feld	Beschreibung
Abonnement	Wird automatisch basierend auf dem während der Anmeldung verwendeten Abonnement ausgewählt.
Ressourcengruppe	Verwenden Sie eine der vorhandenen Ressourcengruppen oder erstellen Sie eine neue (mit der Option **Create New**), in der die Cloud NGFW-Ressource erstellt wird.
Firewallname	Name der Cloud NGFW Firewall-Ressource.

Feld	Beschreibung
Region	Region, in der Cloud NGFW bereitgestellt wird.

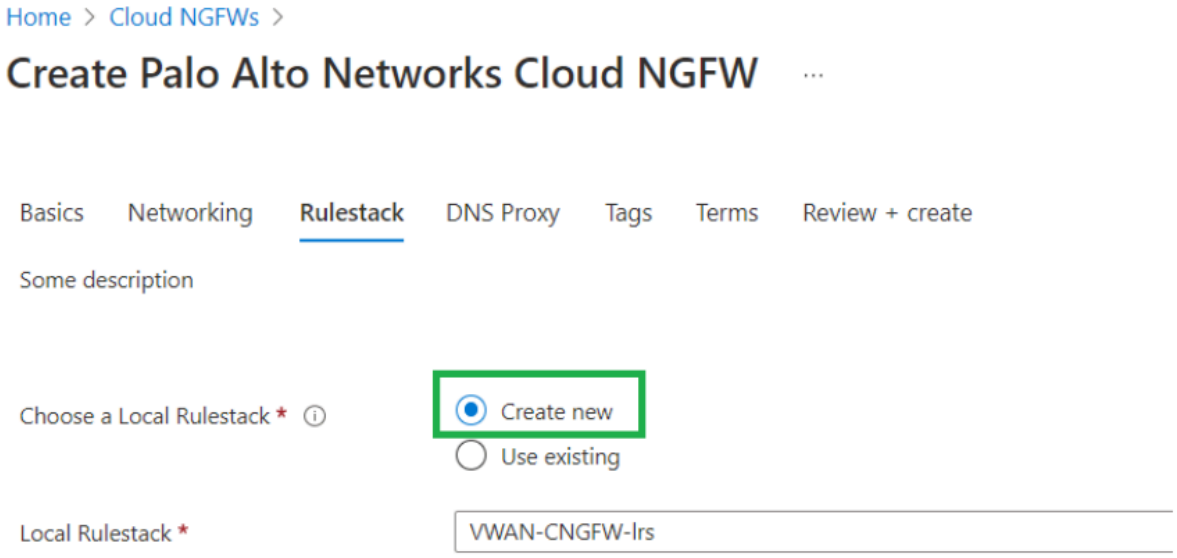


STEP 11 | Klicken Sie auf **Next: Networking**. Geben Sie Informationen zu Ihrer Netzwerkumgebung an. Wählen Sie den **virtuellen WAN-Hub** für den **Netzwerktyp** aus. Wählen Sie im Abschnitt **Virtual WAN Hub Details** aus dem Drop-down-Menü den **Namen des virtuellen Hubs** aus, den Sie zuvor

erstellt haben. Geben Sie **öffentliche IP-Adressen** und die Option **Source NAT** an, wenn für den ausgehenden Datenverkehr im Internet eine Adressübersetzung verwendet wird.

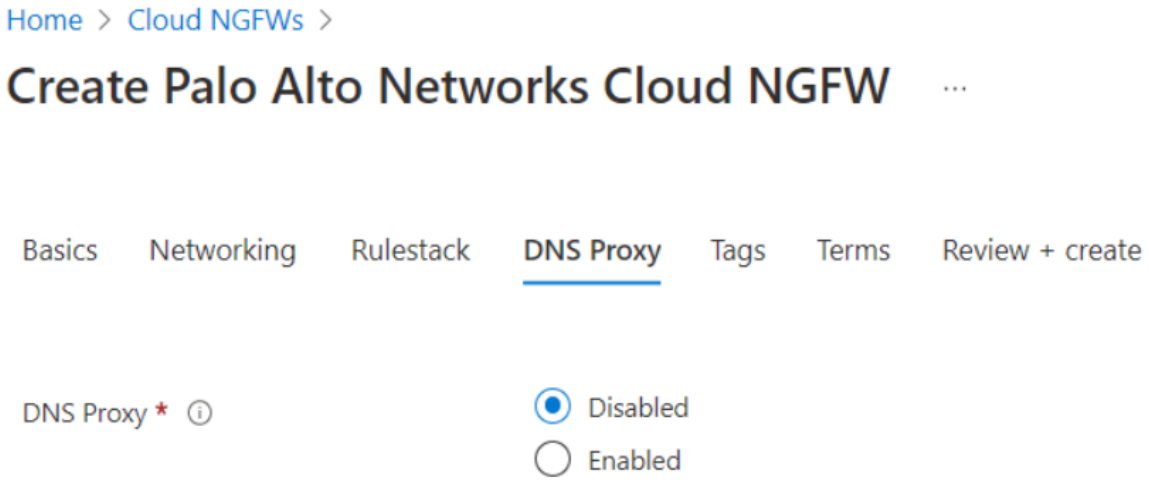


STEP 12 | Klicken Sie auf **Next: Rulestack**, um einen lokalen Regelstapel zu erstellen, in dem Regeln definiert werden. Dies ist ein Platzhalter für die Erstellung lokaler Regelstapel. Klicken Sie auf **Create new** oder **Use existing** (wenn bereits ein lokaler Regelstapel vorhanden ist, wählen Sie ihn aus dem Drop-down-Menü aus). Nachdem Sie die Cloud NGFW-Ressource erstellt haben, können Sie diesen Regelstapel ändern, um Regeln, FQDN und die Präfixliste hinzuzufügen oder zu bearbeiten.



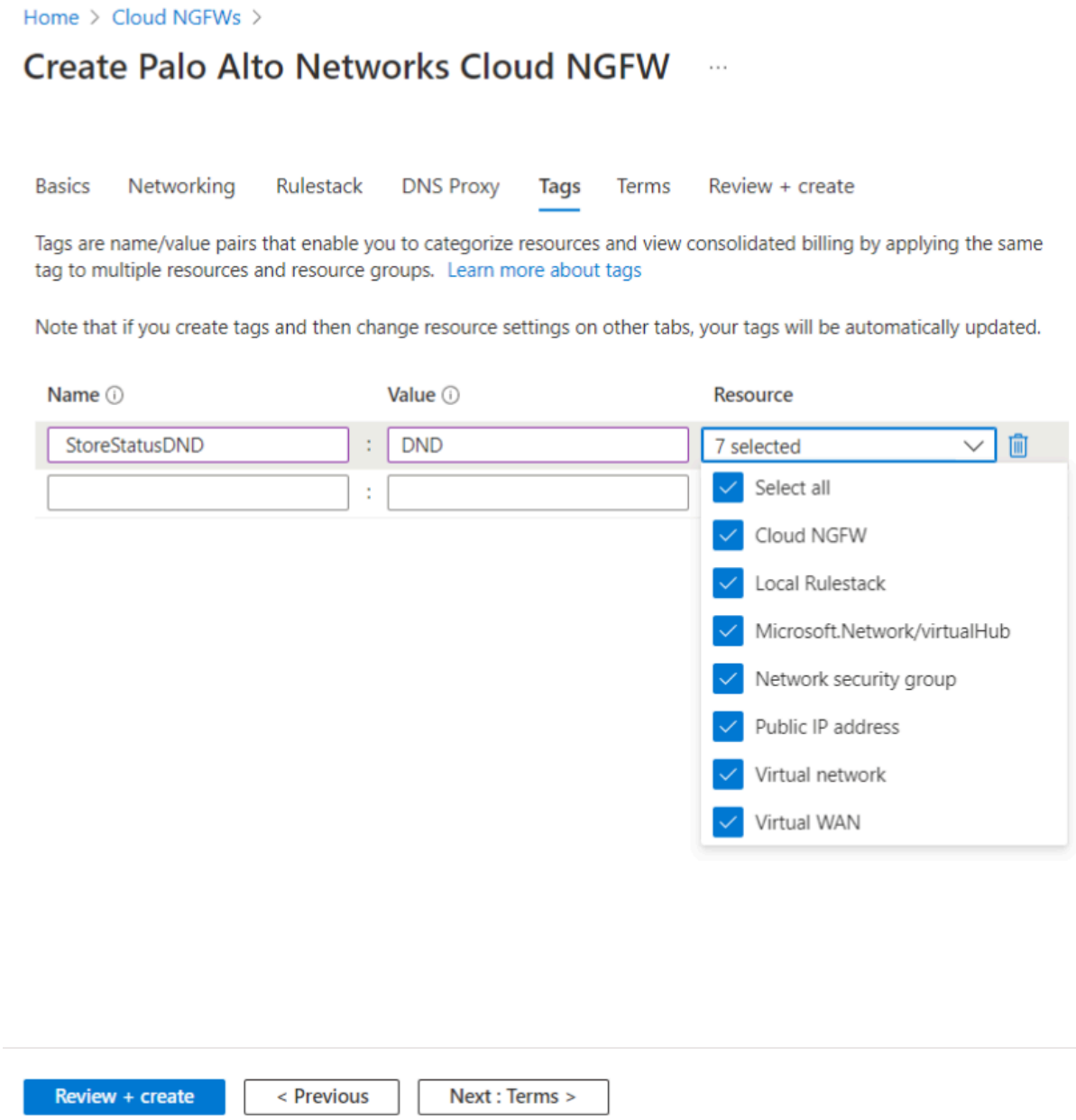
STEP 13 | Klicken Sie auf **Next: DNS Proxy**. Standardmäßig ist der DNS-Proxy deaktiviert. Sie können die Cloud NGFW so konfigurieren, dass sie den gesamten DNS-Verkehr überprüft, indem sie als Proxy für vWAN-Ressourcen fungiert. Wenn der DNS-Proxy konfiguriert ist, leitet er die DNS-

Anforderung an den standardmäßigen Azure-DNS-Server oder an einen von Ihnen angegebenen DNS-Server weiter.



STEP 14 | Klicken Sie auf **Next: Tags**, um Tags für Ihre Azure-Anforderungen anzugeben. Tags sind vordefinierte Bezeichnungen, die Ihnen dabei helfen können, die Sicherheitslücken in Ihrer Umgebung zu verwalten und die konsolidierte Abrechnung im Zusammenhang mit Ihrem

Azure-Konto anzuzeigen. Sie werden zentral definiert und können auf Sicherheitslücken und als Richtlinienausnahmen festgelegt werden.



Tags werden wie folgt verwendet:

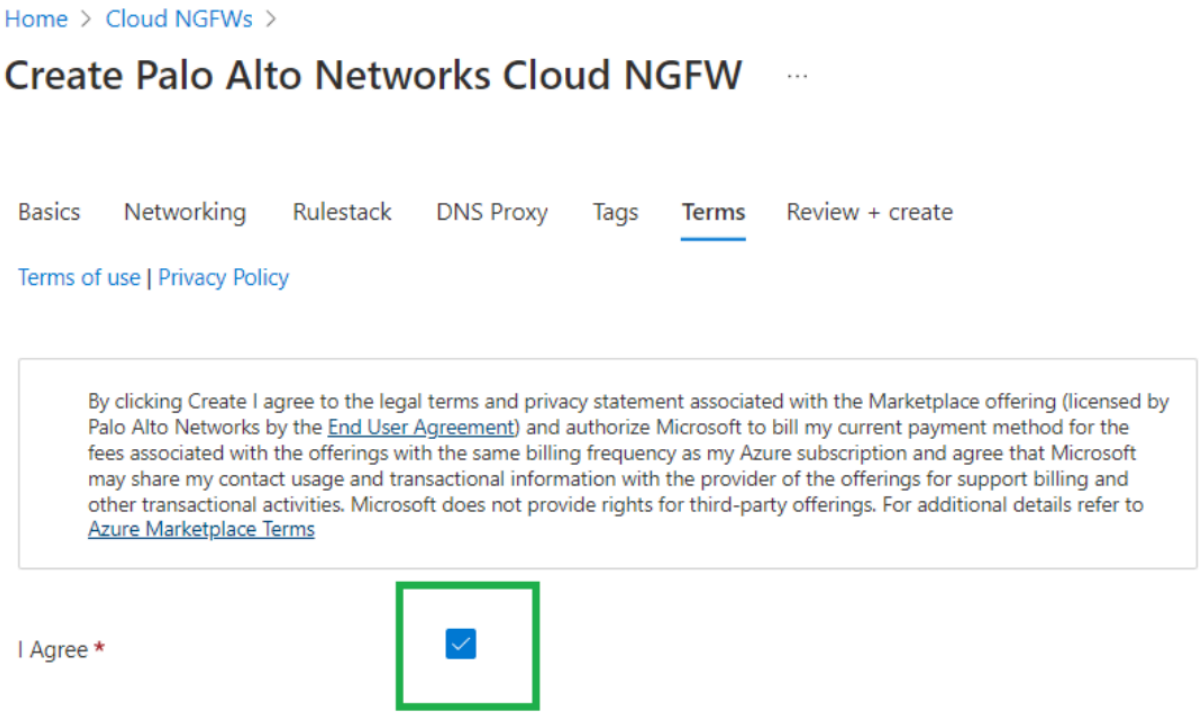
- Kennzeichnung der Sicherheitslücken. Sie sind eine praktische Möglichkeit, die Sicherheitslücken in Ihrer Umgebung zu kategorisieren.
- Richtlinienausnahmen. Sie können Teil Ihrer Regeln sein, um gezielt auf markierte Sicherheitslücken einzuwirken.
- Die konsolidierte Abrechnung für Ihr Azure-Konto anzeigen.

  Tags sind nützlich, wenn Sie große Containerbereitstellungen mit mehreren Teams haben, die in derselben Umgebung arbeiten. Beispielsweise könnten sich verschiedene Teams mit unterschiedlichen Arten von Sicherheitslücken befassen. Anschließend können Sie Tags festlegen, um Verantwortlichkeiten für Sicherheitslücken zu definieren. Andere Verwendungsmöglichkeiten wären, den Status der Behebung der Sicherheitslücke festzulegen oder Sicherheitslücken zu markieren, die ignoriert werden sollen, wenn es sich um ein bekanntes Problem handelt, das in naher Zukunft nicht behoben werden kann.

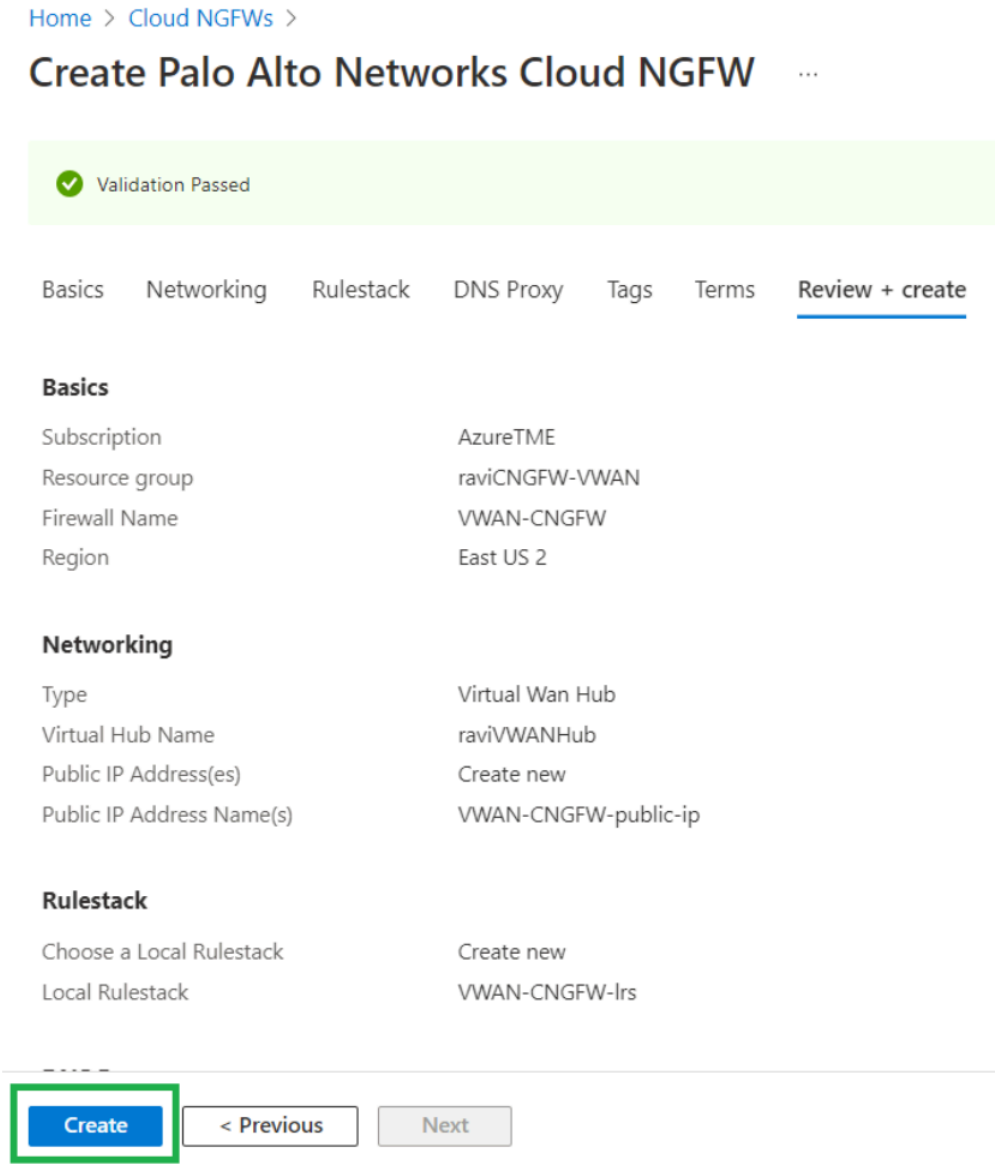
  

  Sie können beliebig viele Tags definieren. Informationen zum Erstellen von Tags für Ihr Azure-Konto finden Sie unter Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen und -Verwaltungshierarchie.

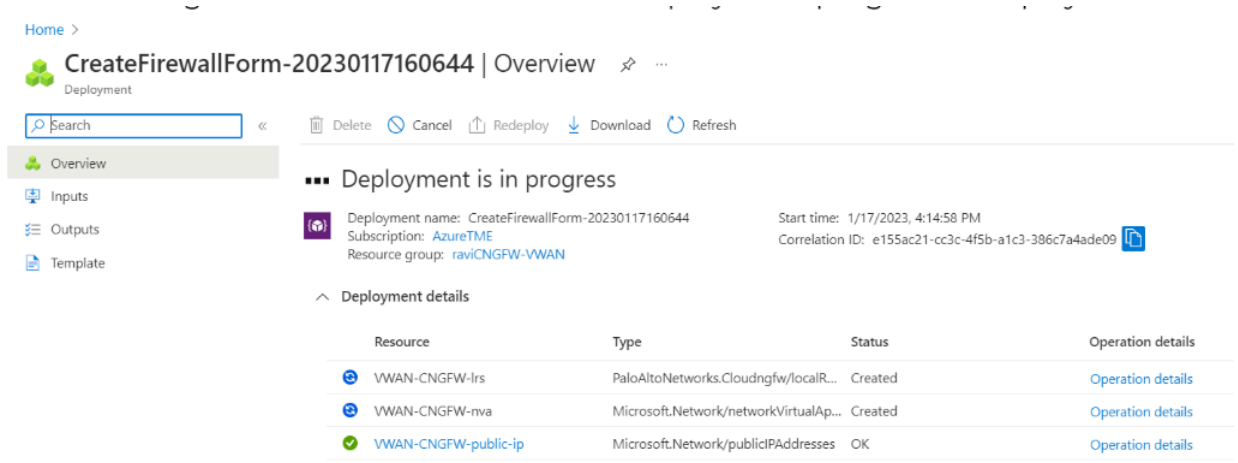
STEP 15 | Klicken Sie auf **Next: Terms** und akzeptieren Sie die Bedingungen für die Bereitstellung.



STEP 16 | Klicken Sie auf **Review + create**, um Ihr Azure-Abonnement für die Cloud NGFW-Ressource zu validieren. Die Ressource wird zuerst validiert und dann erstellt. Auf dem Bildschirm wird **Validation Passed** angezeigt. Klicken Sie auf **Create**, um den Cloud NGFW-Dienst bereitzustellen:

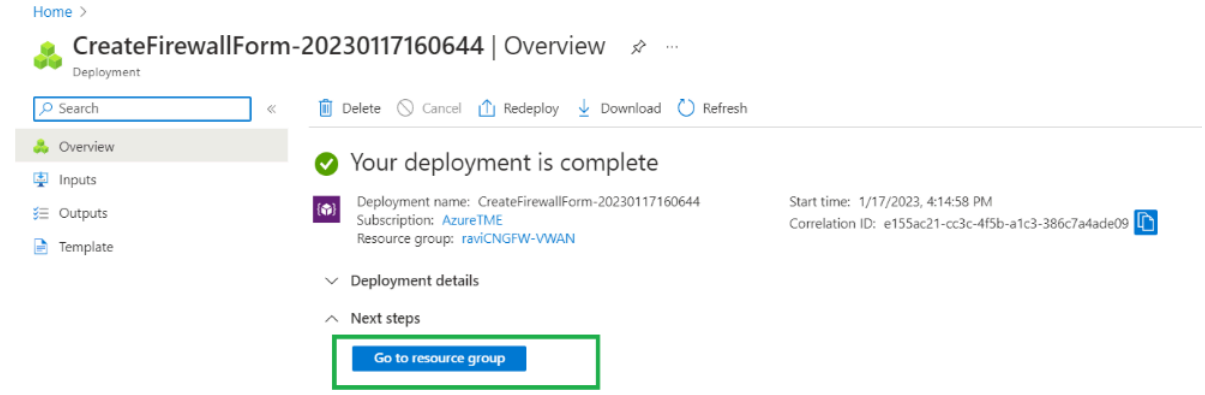


Nach dem Erstellen des Cloud NGFW-Dienstes wird der Bereitstellungsfortschritt angezeigt.

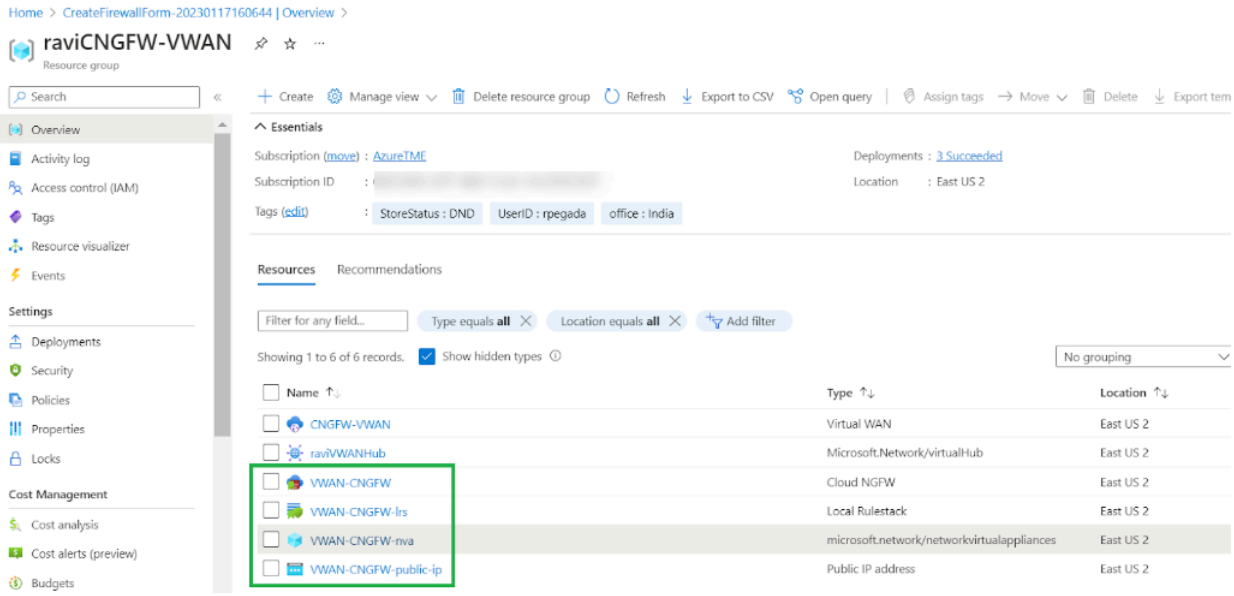


Die Bereitstellung einer Cloud NGFW-Ressource dauert ungefähr 30 Minuten.

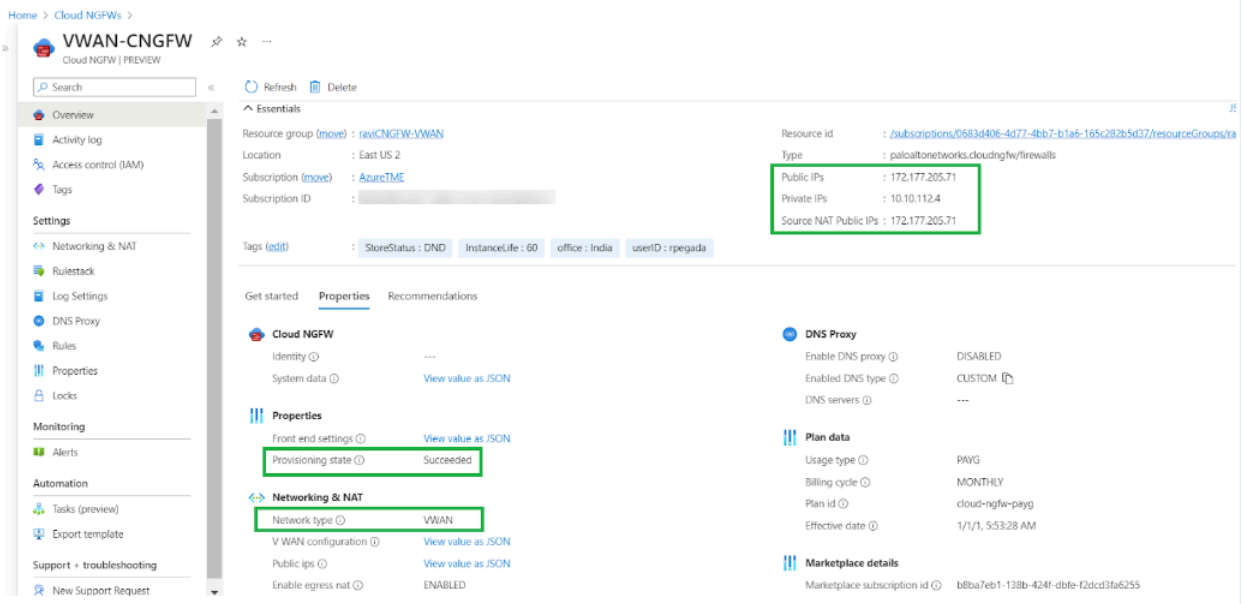
Bei einer erfolgreichen Bereitstellung wird der folgende Bildschirm angezeigt.



STEP 17 | Es werden vier Ressourcen erstellt, darunter Cloud NGFW, ein lokaler Regelstapel, eine öffentliche IP-Adresse und die Cloud-nva.



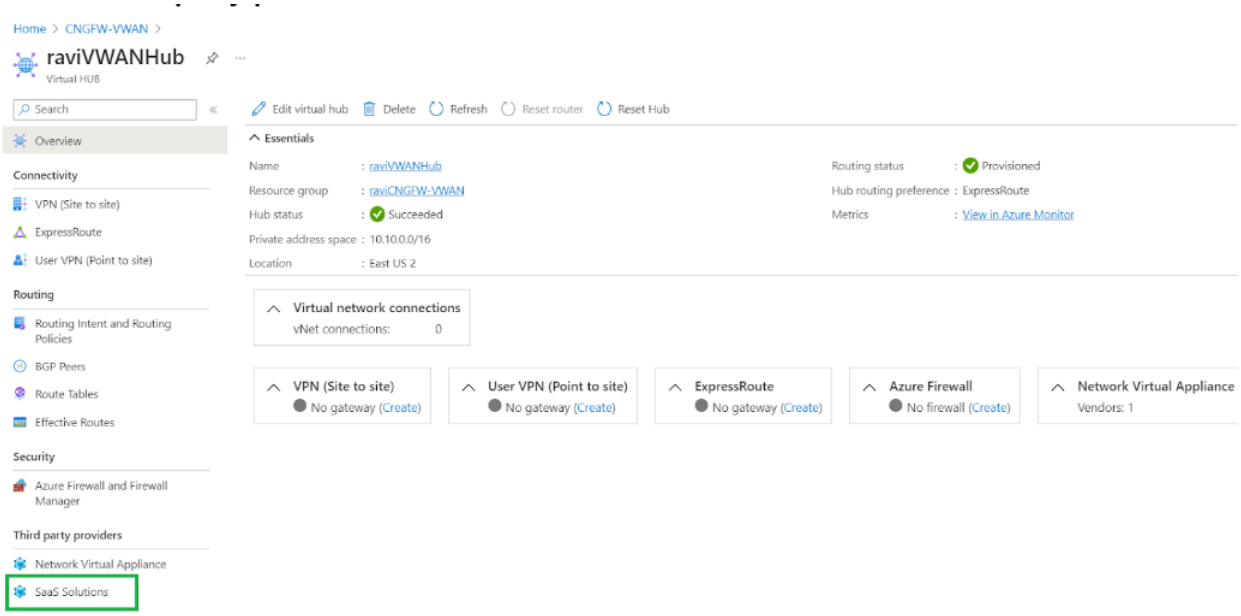
STEP 18 | Nachdem Sie die Cloud NGFW-Ressource erstellt haben, wählen Sie sie aus, um zu überprüfen, ob der Bereitstellungsstatus „Succeeded“ lautet. Auf dieser Seite werden auch die öffentlichen und privaten IP-Adressen angezeigt, die mit dem Cloud NGFW-Dienst verknüpft sind. Stellen Sie sicher, dass der Netzwerktyp vWAN ist.



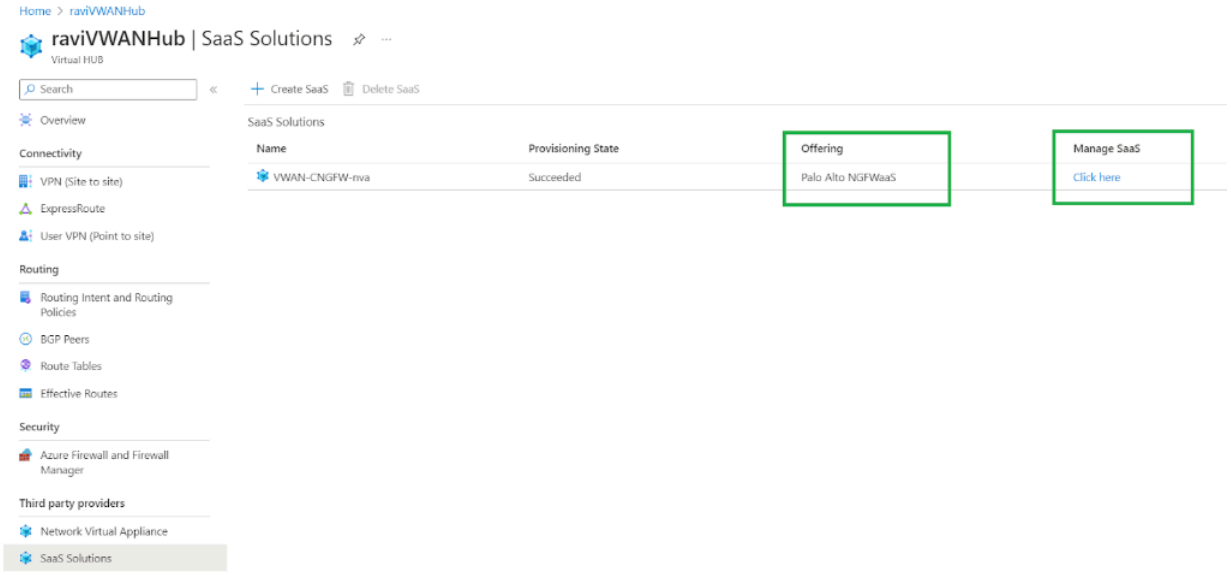
Überprüfen der Bereitstellung der Cloud NGFW in einem vWAN

Nachdem Sie den Cloud NGFW-Dienst für den vWAN-Netzwerktyp erfolgreich erstellt haben, überprüfen Sie, ob die Cloud NGFW als SaaS-Lösung für das vWAN hinzugefügt wurde.

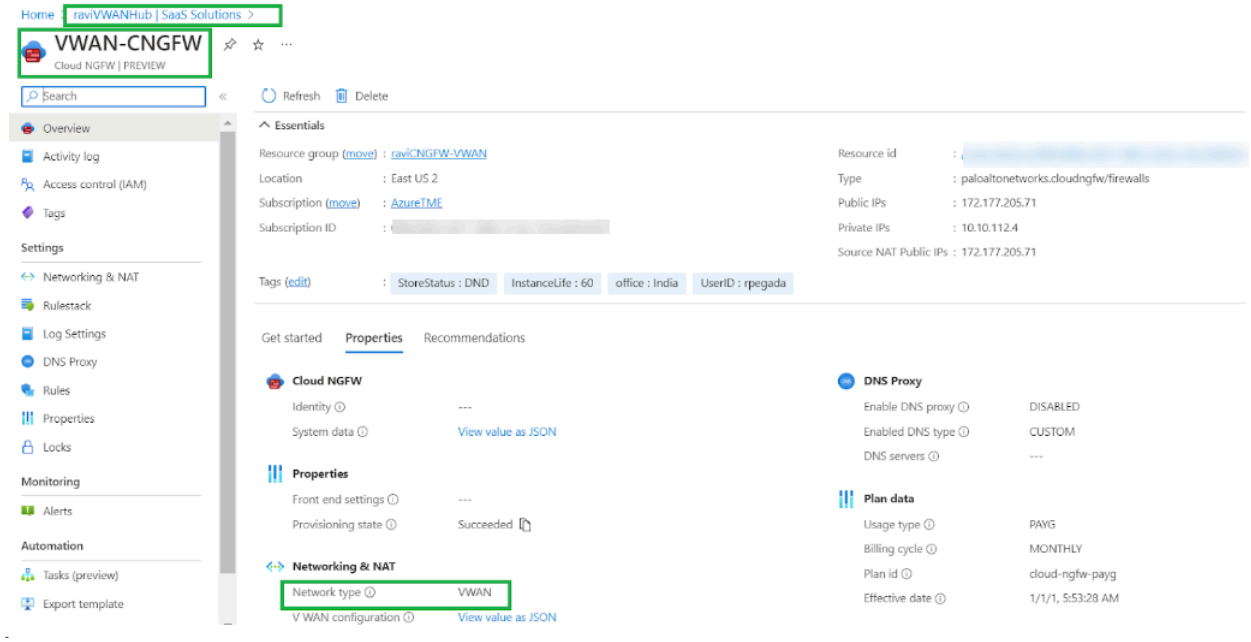
STEP 1 | Gehen Sie zu dem virtuellen Hub, der beim Erstellen des Cloud NGFW-Dienstes verwendet wurde. Klicken Sie im Abschnitt **Third party providers** auf **SaaS Solutions**.



STEP 2 | Überprüfen Sie, ob die Cloud NGFW erstellt wurde; sie wird diesem Hub als SaaS-Lösung hinzugefügt. Wählen Sie im Abschnitt **SaaS Solutions** die Option **Click here** aus.



Informationen zur vWAN-Bereitstellung werden angezeigt.



Beispielkonfiguration nach vWAN-Bereitstellung

Nach der Bereitstellung

Führen Sie nach dem Überprüfen der Bereitstellung die folgenden Aufgaben aus:

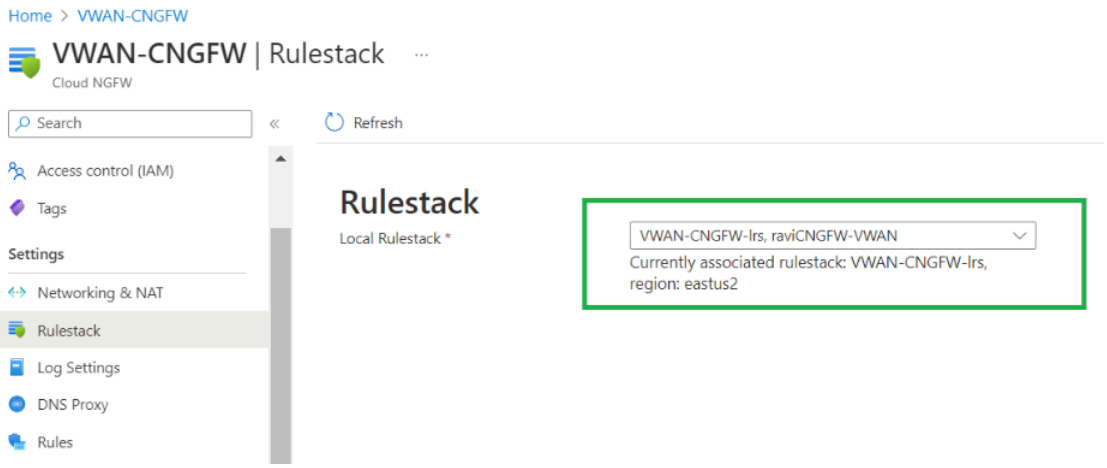
- Erstellen oder Aktualisieren eines Regelstapels
- Quell-/Ziel-NAT-Regel für die Cloud NGFW
- Konfigurieren der Protokollierung

- Hinzufügen von Anwendungs-vNETs als virtuelle Netzwerkverbindungen zum Virtual WAN
- Konfigurieren von vWAN Hub Routing Intent und Routing-Richtlinien

Erstellen oder Aktualisieren eines Regelstapels

So aktualisieren Sie einen vorhandenen Regelstapel:

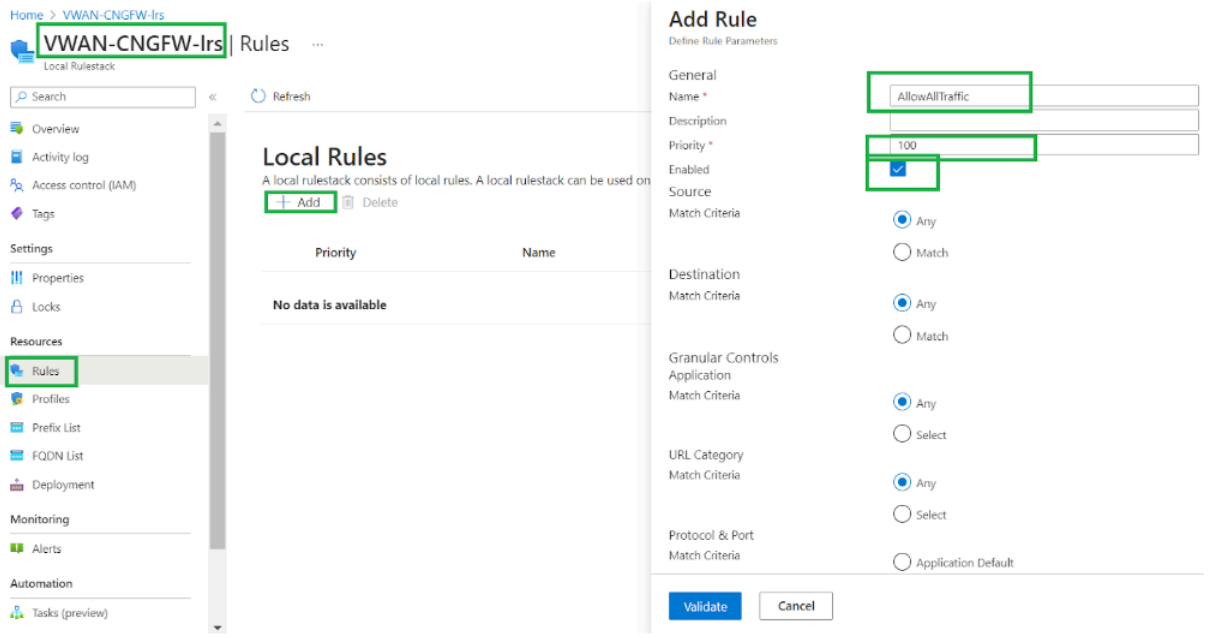
STEP 1 | Klicken Sie in der ARM-Konsole (Azure Resource Manager) für die Cloud NGFW-Ressource, die Sie konfigurieren möchten, auf **Rulestacks**. Der mit dem Cloud NGFW-Dienst verknüpfte Regelstapel wird zusammen mit der Ressourcengruppe angezeigt.



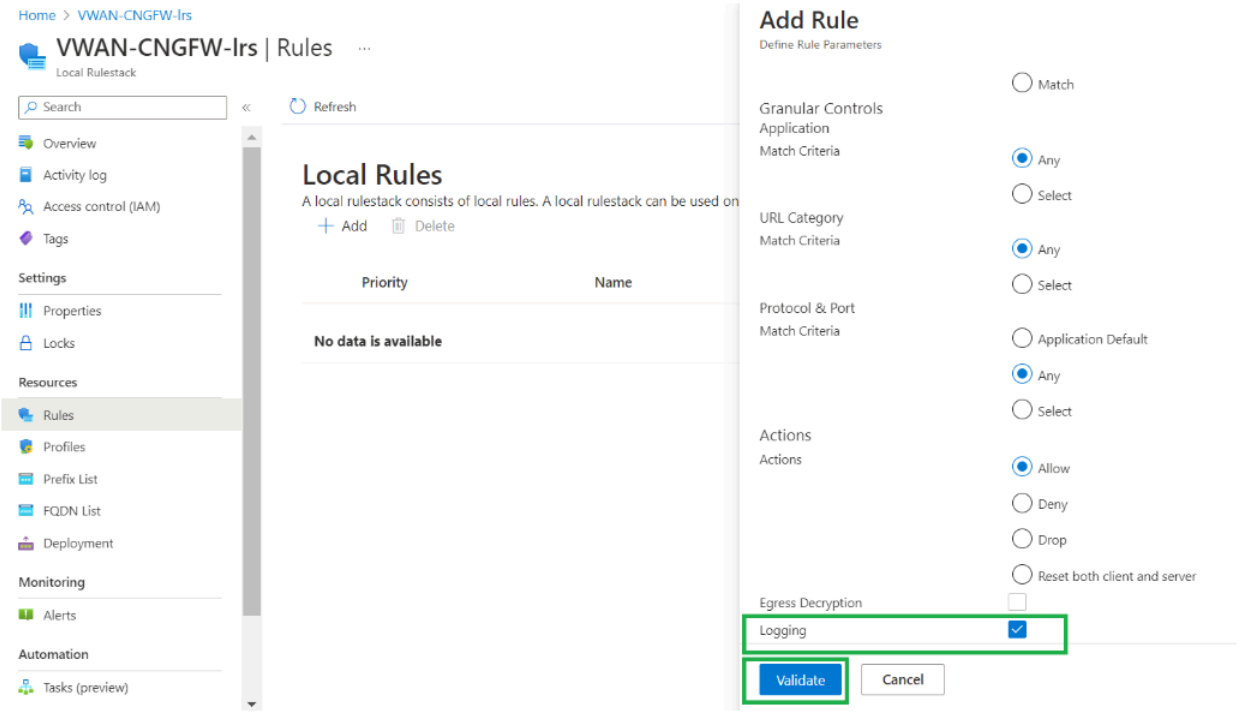
STEP 2 | Ändern Sie den Regelstapel, um Firewall-Regeln hinzuzufügen. Diese Regeln lassen einen gewissen Datenverkehr zu, während bestimmter Datenverkehr blockiert wird. Standardmäßig blockiert Cloud NGFW den gesamten Datenverkehr. Suchen Sie mit der globalen Suchoption des Azure-Portals nach dem lokalen Regelstapel, den Sie zuvor erstellt haben.

STEP 3 | Wählen Sie den zuvor erstellten lokalen Regelstapel aus, der Ihrem Cloud NGFW-Abonnement zugeordnet ist. Wählen Sie dann **Rules** aus.

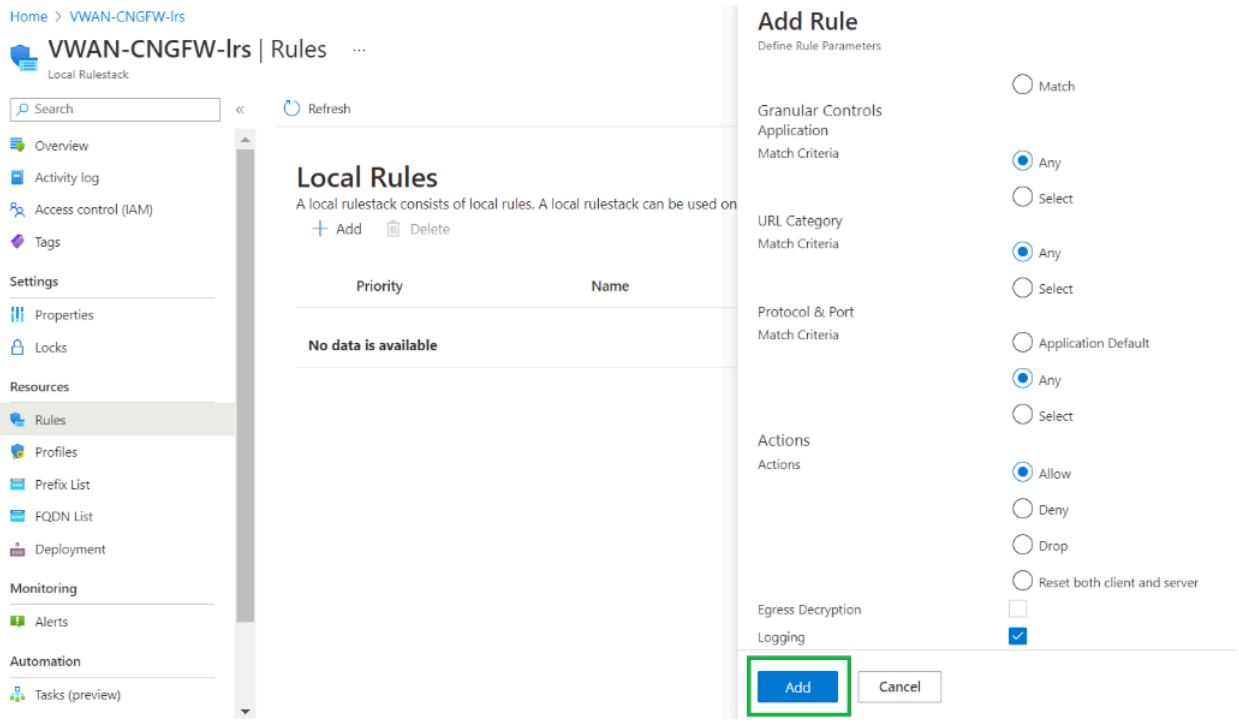
STEP 4 | Klicken Sie im Abschnitt **Local Rules** auf **Add**. Ändern Sie im Fenster **Add Rule** die Regeln. Fügen Sie z. B. eine Regel hinzu, die Datenverkehr zulässt. Füllen Sie die Pflichtfelder aus und verwenden Sie die Standardeinstellungen für die restlichen Felder.



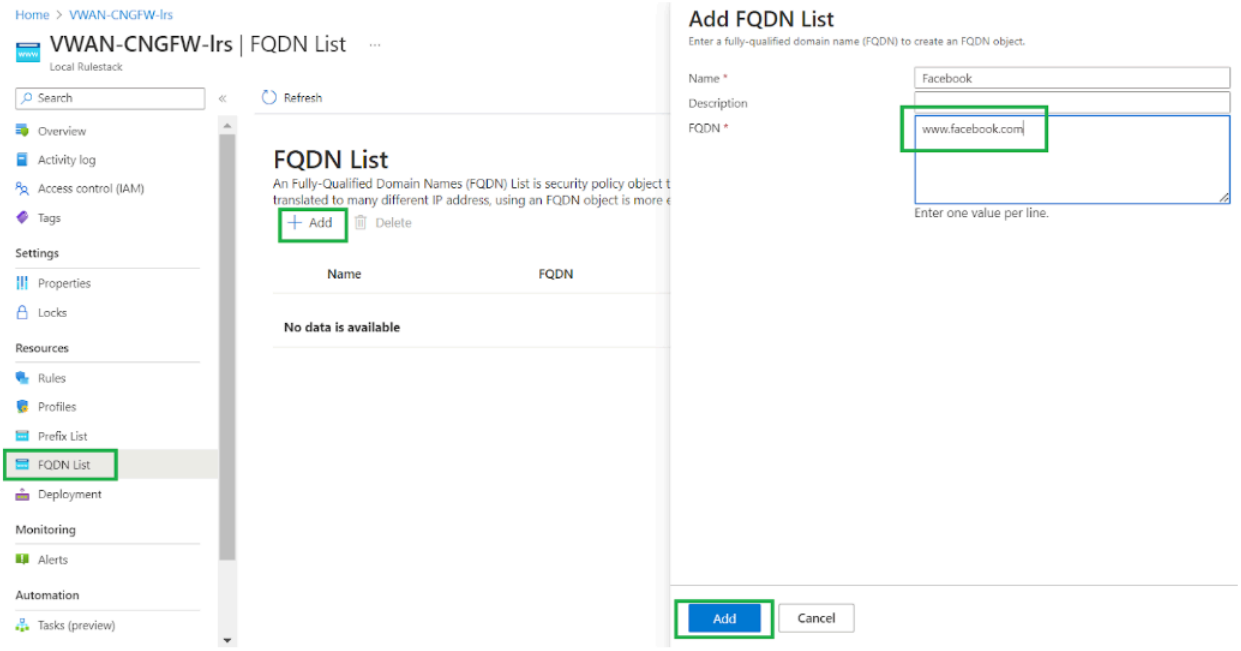
STEP 5 | Aktivieren Sie die Protokollierung für die Regel. Wählen Sie im Fenster „Add Rule“ die Option **Logging** aus.



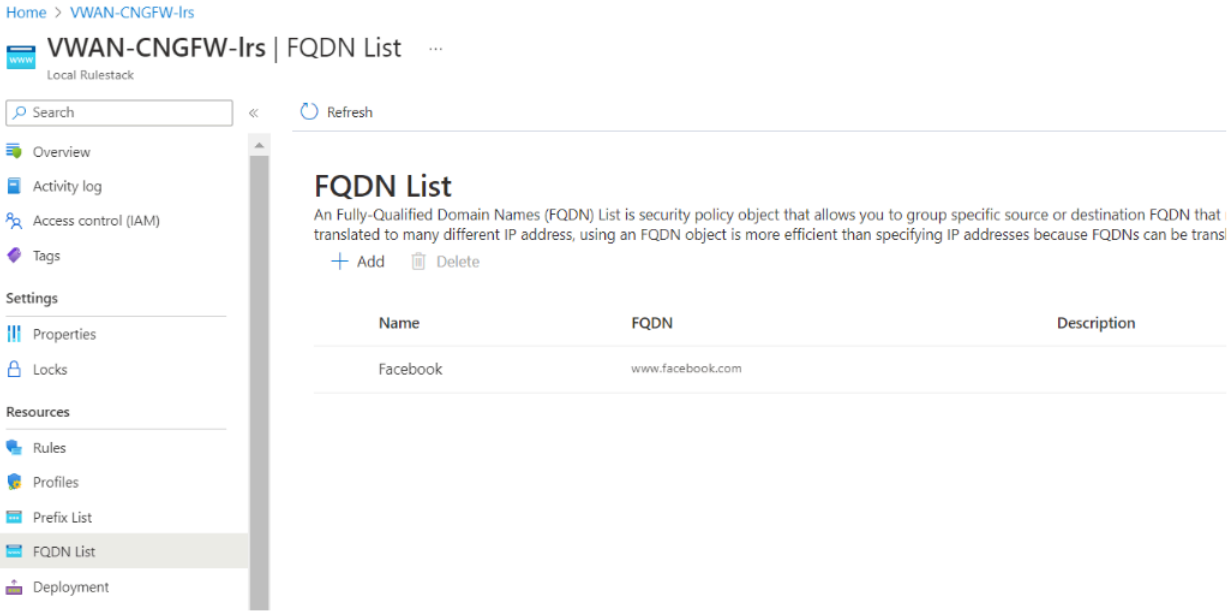
STEP 6 | Klicken Sie auf **Validate**, dann auf **Add**, um die Regel zum Regelstapel hinzuzufügen.



STEP 7 | Fügen Sie eine **FQDN-Liste** hinzu, die eine URL angibt. Geben Sie dann eine Aktion an, die ausgeführt werden soll. Sie können z. B. eine Aktion auf die FQDN-Regel anwenden, um Datenverkehr zu unterbinden, der auf die URL „www.facebook.com“ zugreifen möchte.



Vergewissern Sie sich, dass die von Ihnen eingegebene URL in der FQDN-Liste angezeigt wird.

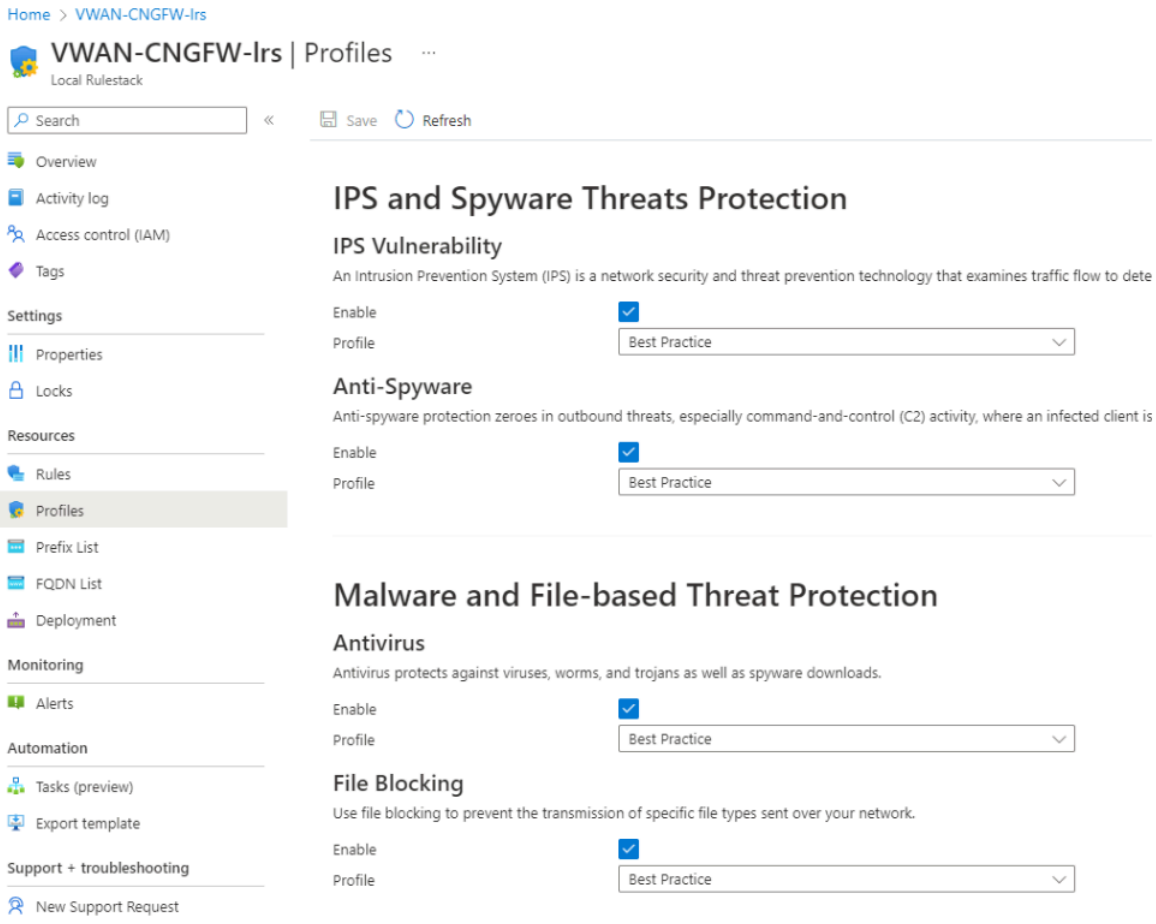


STEP 8 | Kehren Sie zurück zur Einstellungsseite **Rules** und fügen Sie eine Regel hinzu, die der neu erstellten FQDN-Liste entspricht. Legen Sie die Aktion auf **Drop traffic** fest.

Beide Regeln werden auf der Seite „Local Rules“ angezeigt.

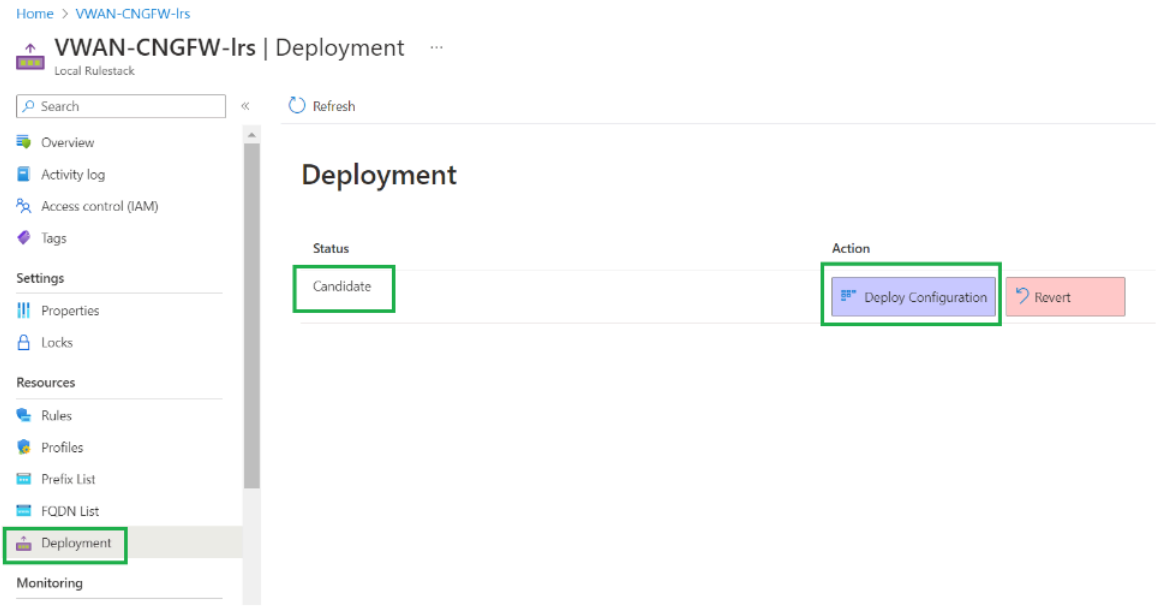
STEP 9 | Als Teil des Cloud NGFW-Dienstes sind Sicherheitsprofile standardmäßig mit Best-Practice-Konfigurationen aktiviert. Der Datenverkehr wird mit den besten Sicherheitsprofilen gesichert,

wenn Sie den Dienst starten und bereitstellen. Wählen Sie **Profiles** aus, um diese Sicherheitsprofile anzuzeigen.

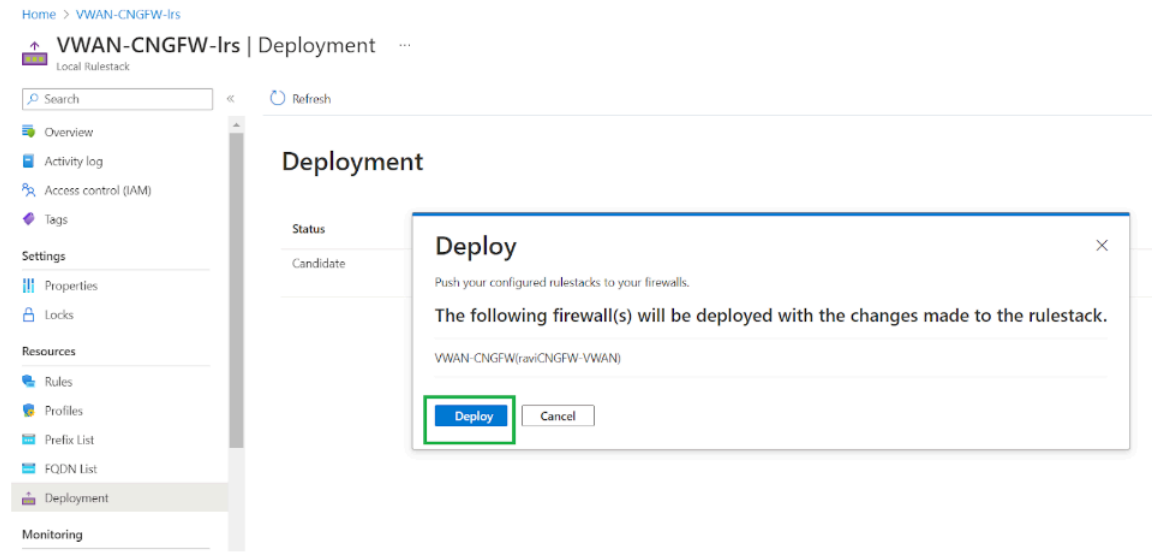


STEP 10 | Nachdem Sie die Regeln geändert haben, stellen Sie sie auf dem lokalen Regelstapel bereit, der mit dem Cloud NGFW-Dienst verknüpft ist. Klicken Sie auf **Deployment**. Der Bereitstellungsstatus wird als **Candidate (Kandidat)** angezeigt. Dies bedeutet, dass die Konfiguration erstellt, aber noch nicht bereitgestellt wurde. Klicken Sie auf **Deploy Configuration**, um die Konfiguration auf dem

Cloud NGFW-Dienst bereitzustellen. **Sie müssen diesen Schritt ausführen, um den Regelstapel bereitzustellen**.



STEP 11 | Nachdem Sie auf **Deploy Configuration** geklickt haben, werden in einer Meldung die Firewalls angezeigt, die dem Regelstapel zugeordnet sind. Klicken Sie auf **Deploy**, um diesen Regelstapel auf allen zugeordneten Firewalls zu konfigurieren, die den Regelstapel verwenden.



Nach der erfolgreichen Bereitstellung der Konfiguration wird der Bereitstellungsstatus als „Running“ angezeigt (die Cloud NGFW und der lokale Regelstapel wurden erfolgreich bereitgestellt).

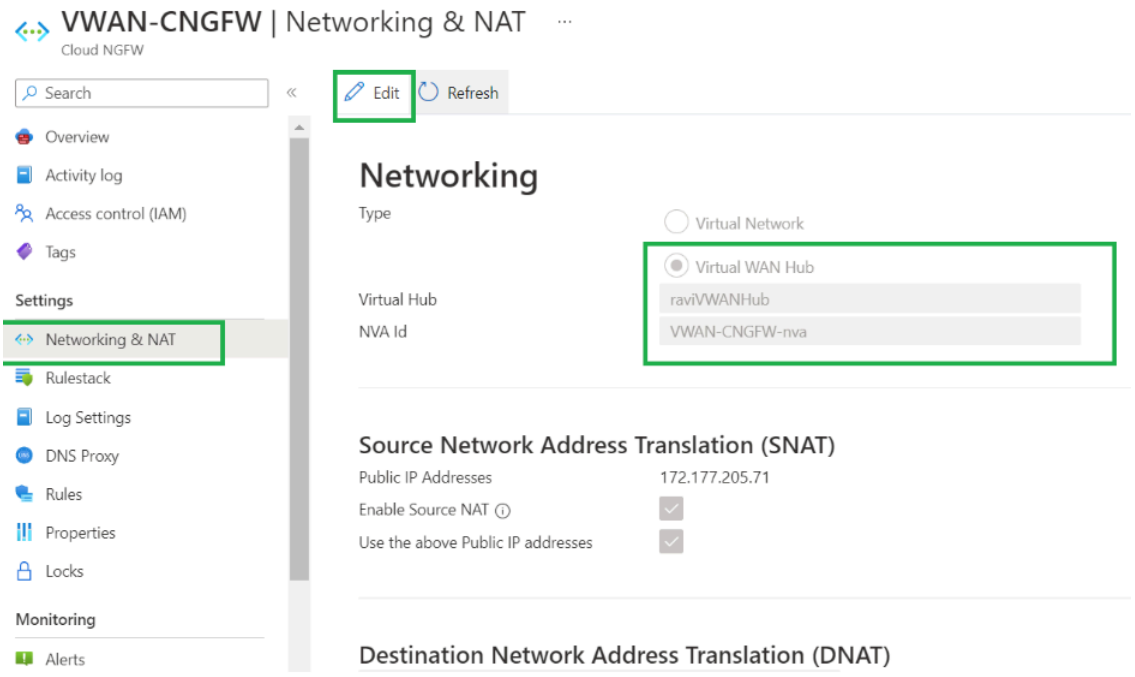
Quell-/Ziel-NAT-Regel für die Cloud NGFW

Konfigurieren Sie eine Ziel-NAT-Regel mit Frontend-Konfiguration auf der Cloud NGFW, um eingehenden Datenverkehr an eine Anwendung im vWAN weiterzuleiten.

STEP 1 | Öffnen Sie den Einstellungsbildschirm **Networking & NAT** für die Cloud NGFW-Ressource. Ermitteln Sie in diesem Bildschirm, ob der Netzwerktyp **Virtual WAN Hub** und der Status des Felds

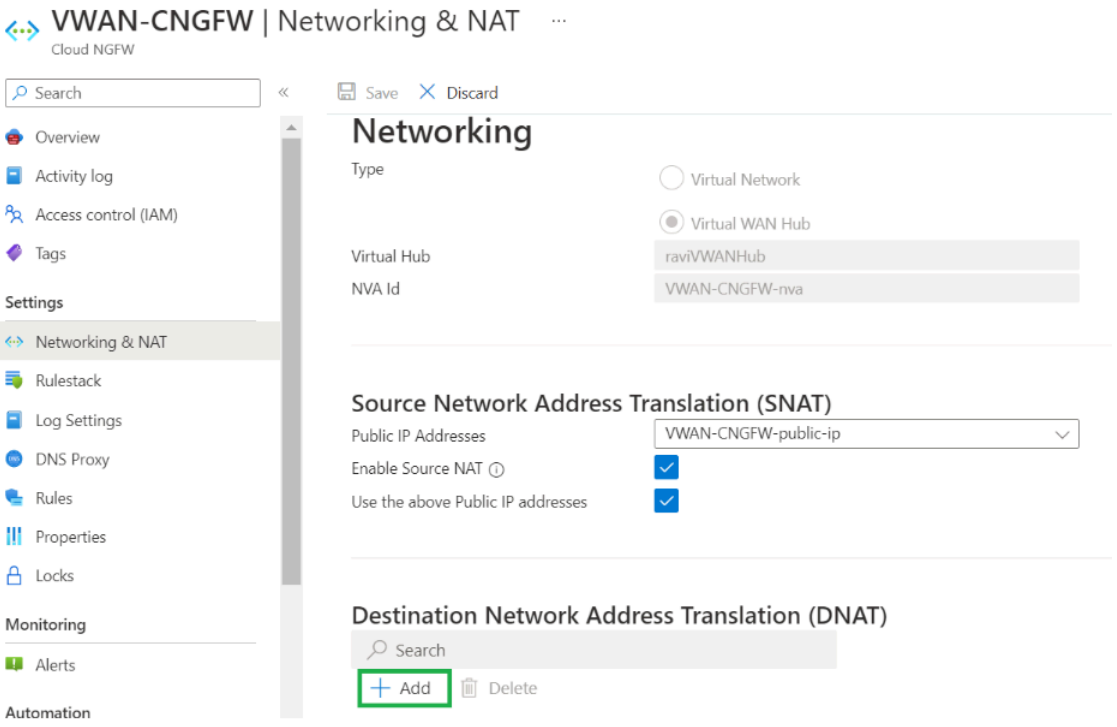
Source NAT (aktiviert oder deaktiviert) ist. Wenn „Source NAT“ aktiviert wurde, wird es in diesem Bildschirm angezeigt.

STEP 2 | Klicken Sie auf **Edit**, um die Ziel-NAT-Regel hinzuzufügen.



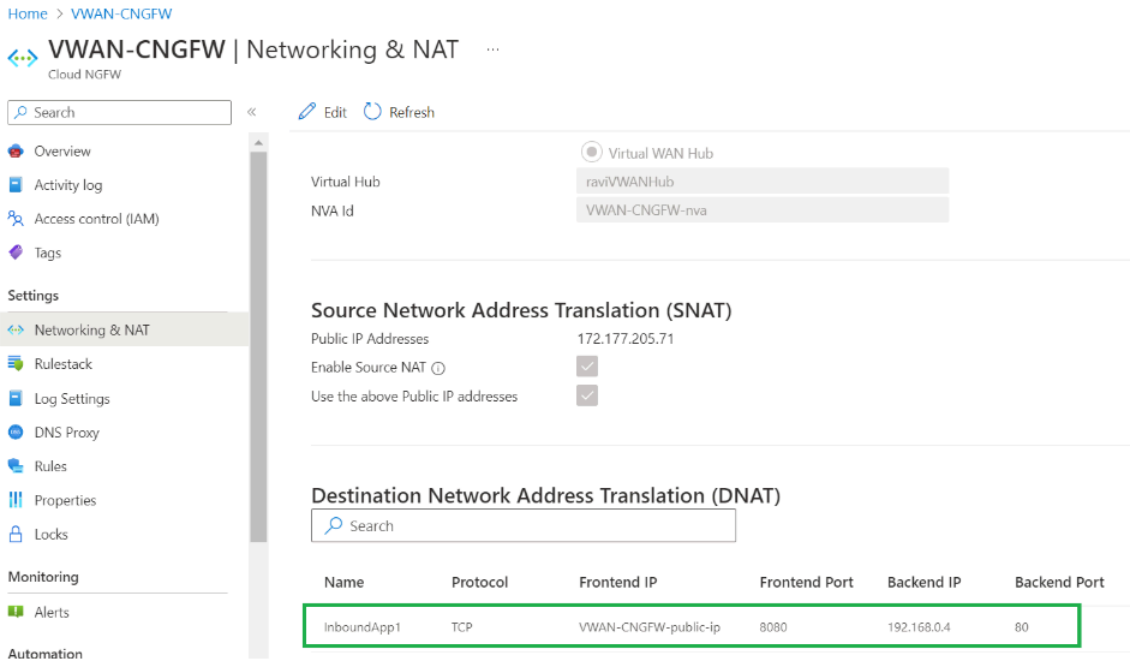
STEP 3 | **Fügen** Sie eine Ziel-NAT-Regel für die Frontend-Konfiguration hinzu. Die Frontend-IP-Adresse stellt die öffentliche IP-Adresse dar, die der Cloud NGFW zugeordnet ist. Verwenden Sie das Drop-down-Menü, um die Adresse auszuwählen.

STEP 4 | Fügen Sie der Regel Informationen zu Frontend-Einstellungen hinzu, und klicken Sie auf **Add**.



Nachdem Sie die Ziel-NAT-Regel hinzugefügt haben, klicken Sie auf „Save“, um die Konfiguration auf der Cloud NGFW-Ressource bereitzustellen.

Nach dem erfolgreichen Speichern der Konfiguration werden im Feld „Destination Network Address Translation (DNAT)“ die Aktualisierungen angezeigt. Die Adresse „http://frontendIP:8080“ wird über die Cloud NGFW an die angegebene Anwendung auf dem angegebenen Port umgeleitet. Eingehender Datenverkehr fließt jetzt durch die Cloud NGFW.



Konfigurieren der Protokollierung

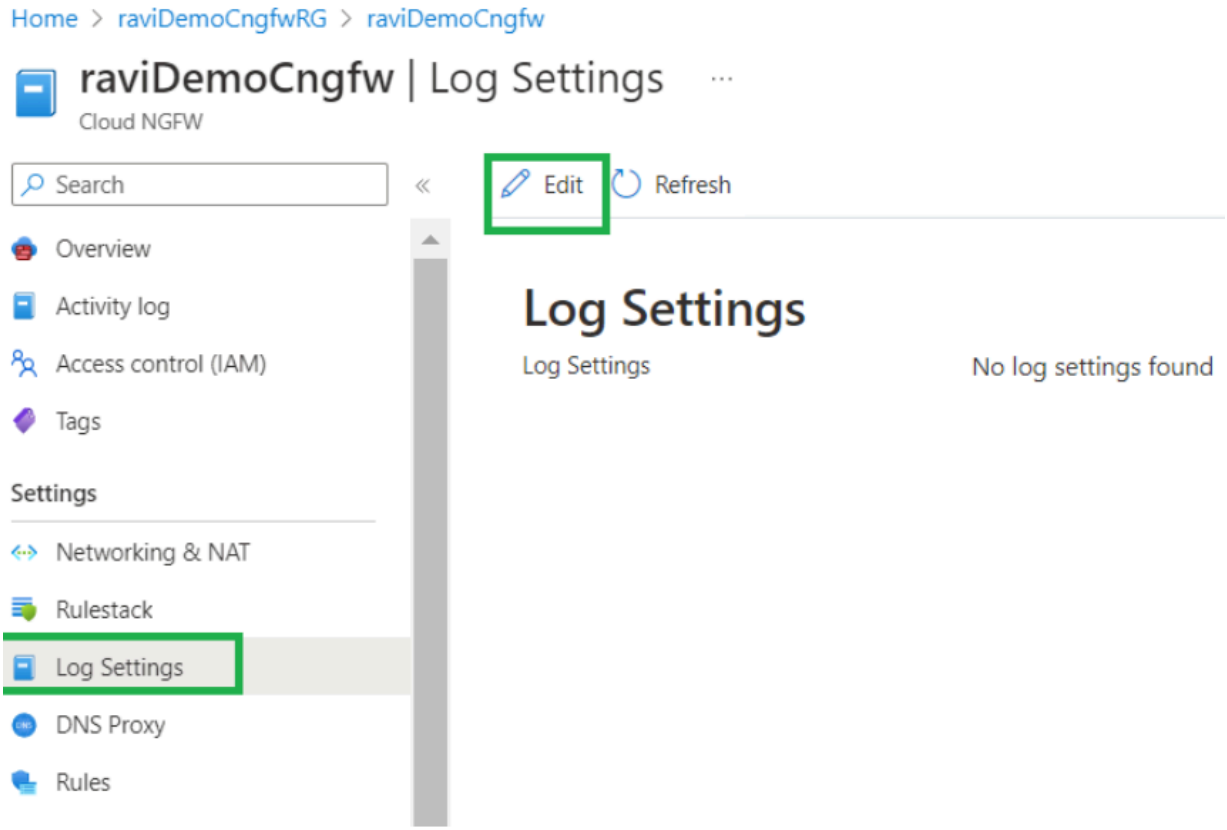
Bevor Sie die Protokollierung in der Cloud NGFW konfigurieren, erstellen Sie den **Log Analytics** Workspace in Azure.

STEP 1 | Suchen Sie im Azure-Portal nach dem **Azure Log Analytics Workspace**. Klicken Sie auf **Log Analytics Workspace**, um ihn als Dienst hinzuzufügen.

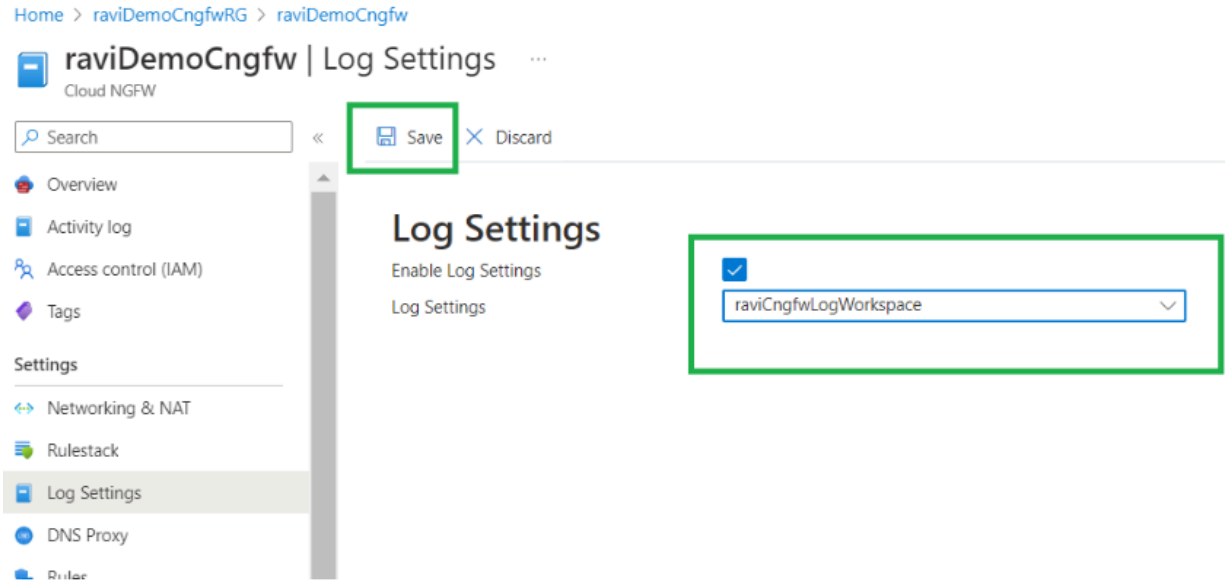
STEP 2 | Klicken Sie auf **Create**, um einen neuen **Log Analytics** Workspace zu erstellen.

STEP 3 | Geben Sie beim Erstellen des Log Analytics Workspace die Details zu **Instance** an. Wählen Sie den **Name** des Arbeitsbereichs aus dem Drop-down-Menü und legen Sie die **Region** fest.

STEP 4 | Konfigurieren Sie die Protokolleinstellungen in der Cloud NGFW-Ressource. Wählen Sie **Log Settings (Protokolleinstellungen)** aus. Klicken Sie auf **Edit**.



STEP 5 | Wählen Sie im Feld **Log Settings** den zuvor erstellten Log Analytics Workspace aus. Klicken Sie dann auf **Save**.

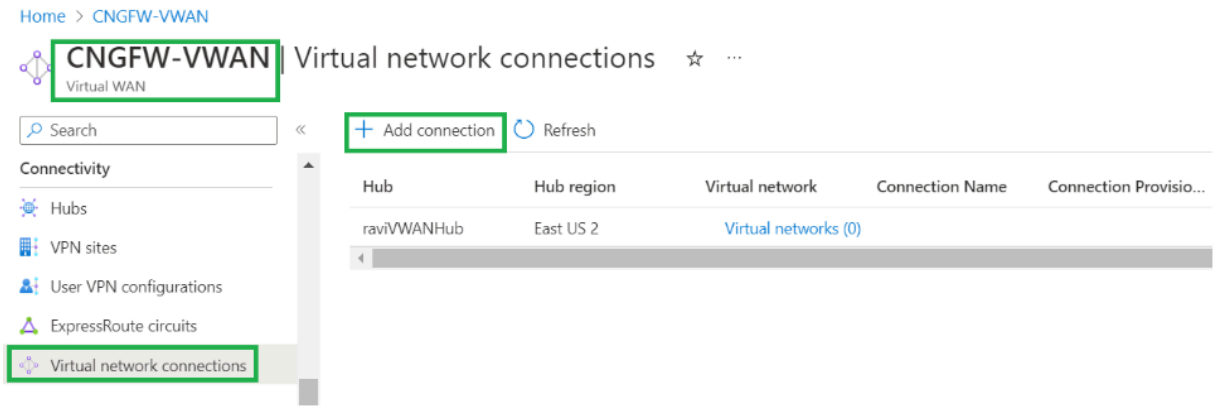


Hinzufügen von Anwendungs-vNETs als virtuelle Netzwerkverbindungen zum Virtual WAN

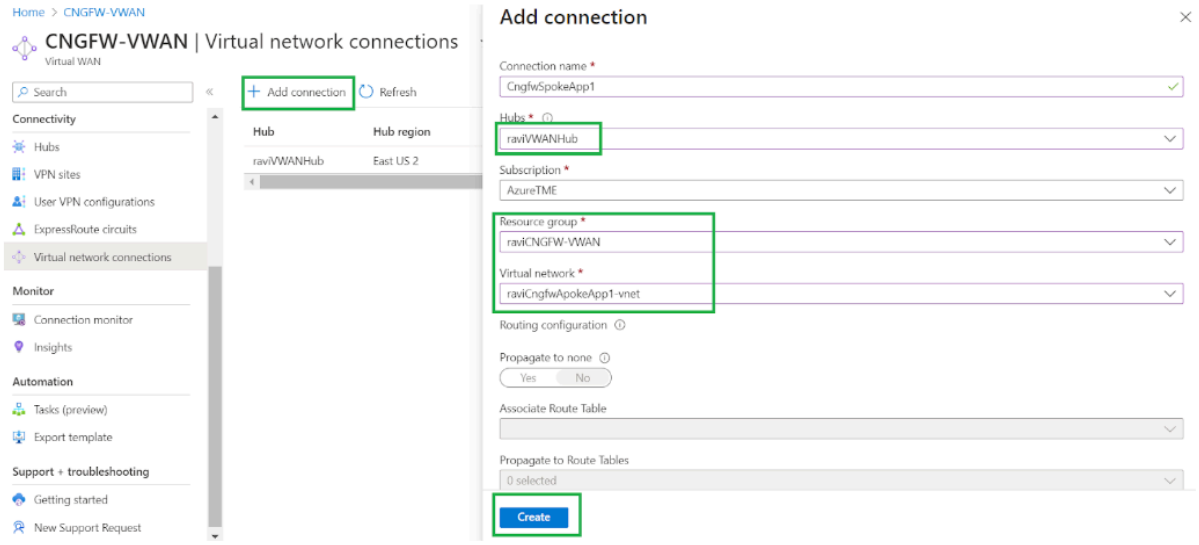
Fügen Sie dem virtuellen WAN-Hub ein Anwendungs-vNET als virtuelle Netzwerkverbindung hinzu.

STEP 1 | Wählen Sie in Ihrer vWAN-Ressource **Virtual Network Connections** aus.

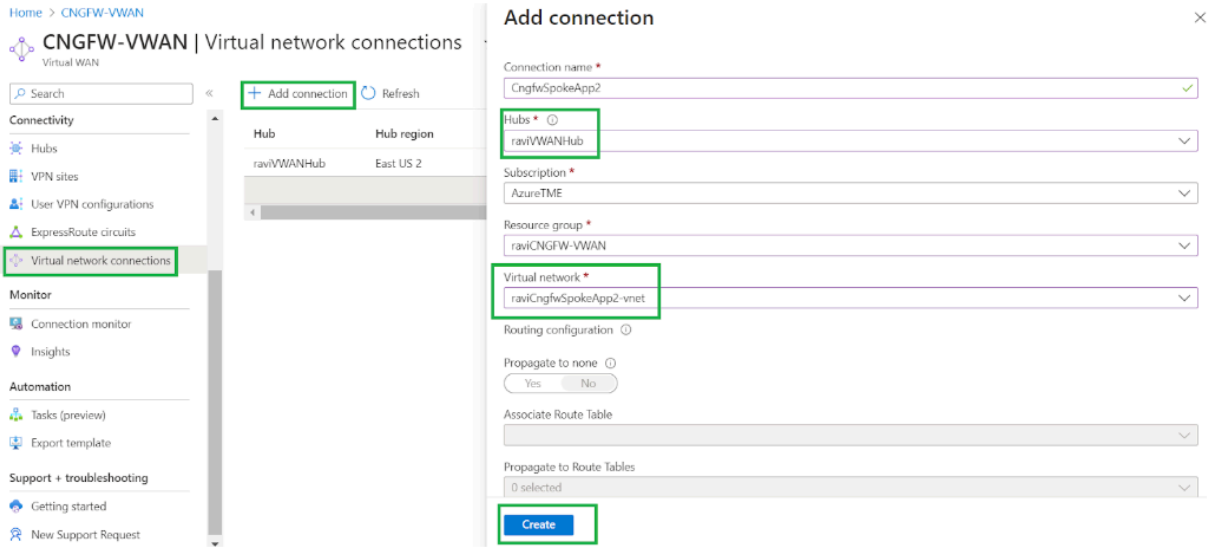
STEP 2 | Klicken Sie auf **Add connection**.



STEP 3 | Wählen Sie das vNET aus, das Sie als **virtuelles Netzwerk** konfigurieren möchten. Klicken Sie dann auf **Create**.



STEP 4 | Wählen Sie ein anderes vNET für das zweite virtuelle Netzwerk aus und klicken Sie dann auf **Create**.



STEP 5 | Nachdem Sie die virtuellen Netzwerke erfolgreich mit dem vHub verbunden haben, stellen Sie sicher, dass der Status **Connected** lautet.

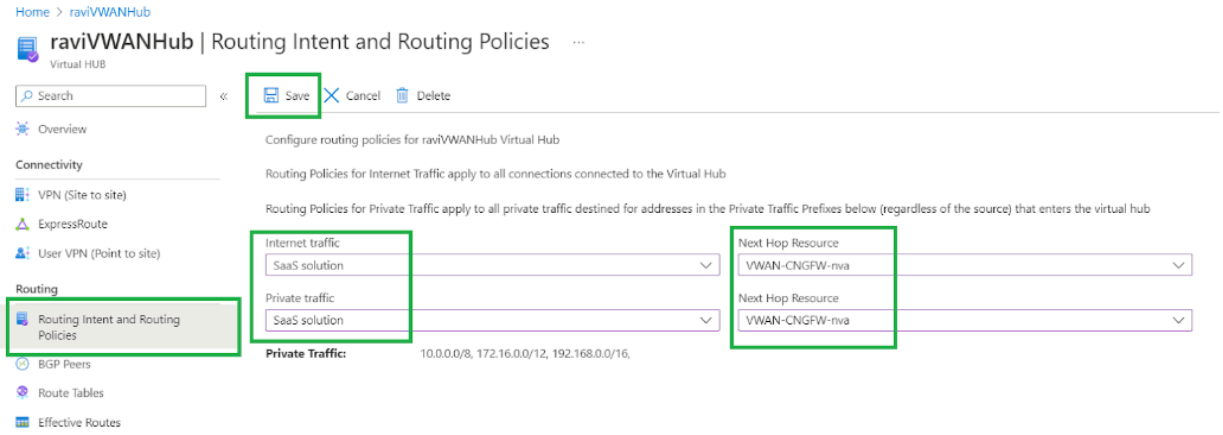
Konfigurieren von vWAN Hub Routing Intent und Routing-Richtlinien

Routing-Richtlinien innerhalb des virtuellen WAN-Hubs werden verwendet, um Datenverkehr über den Cloud NGFW-Dienst weiterzuleiten. Um internetgebundenen Datenverkehr und privaten Datenverkehr (spoke-to-spoke) weiterzuleiten, müssen Sie den nächsten Hop als vWAN Cloud NGFW konfigurieren.

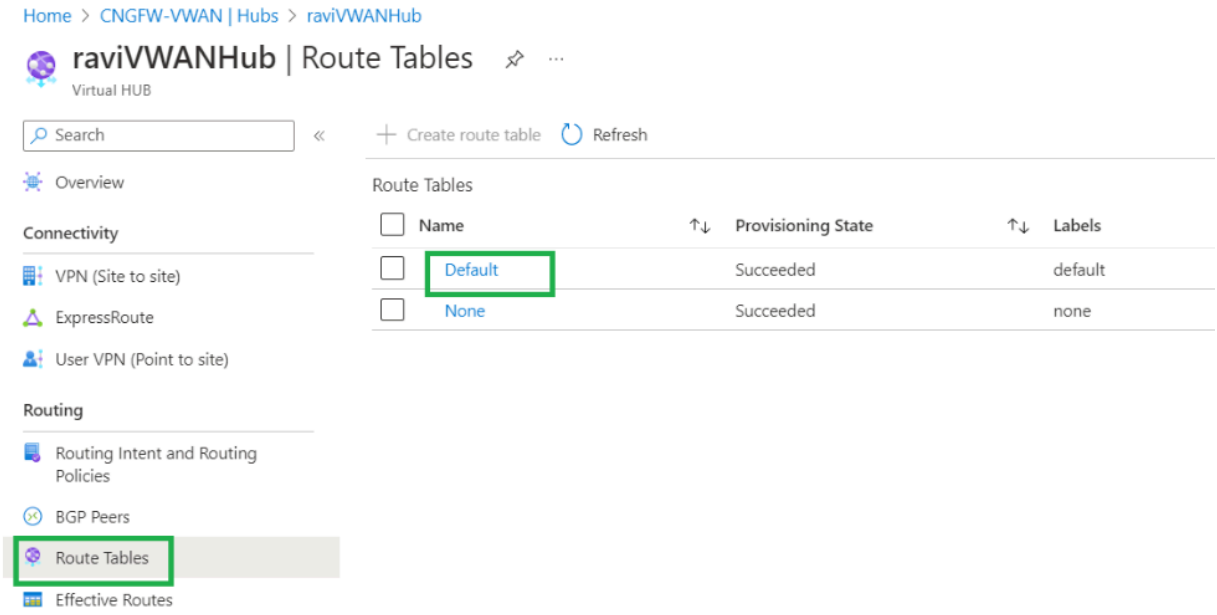
vWAN-Routing-Absicht, Routing-Richtlinien und SaaS-Funktionen werden derzeit von Microsoft für das Azure-Portal entwickelt. Das Zielverfügbarkeitsdatum für jede Region, in der Cloud NGFW verfügbar ist, ist Dienstag, der 9. Mai 2023.

STEP 1 | Wählen Sie in Ihrer vWAN-Ressource **Routing Intent and Routing Policies** aus.

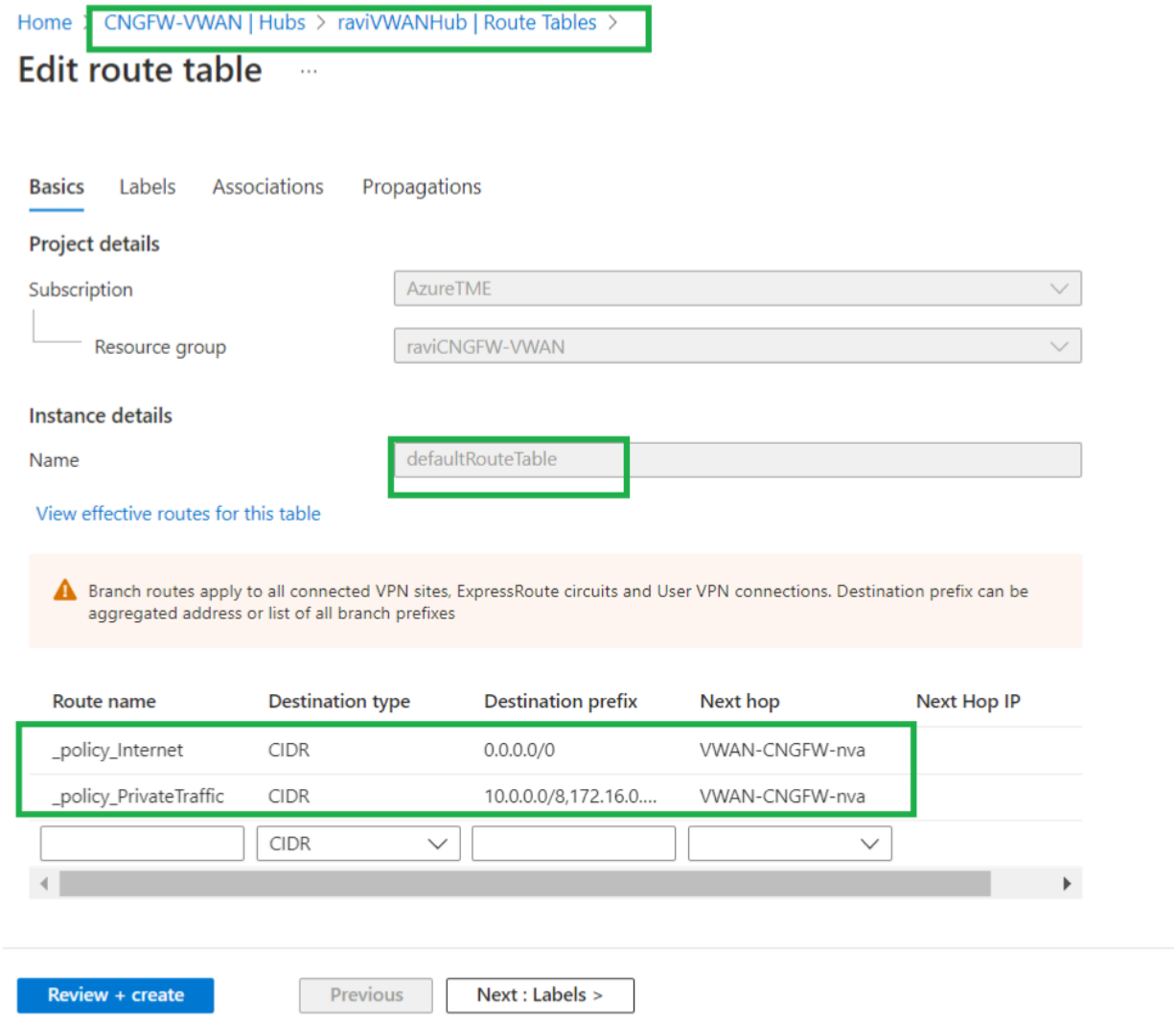
STEP 2 | Wählen Sie den „Internet traffic“ und die „Next Hop Resource“ aus den Drop-down-Menüs aus und klicken Sie dann auf **Save**.



STEP 3 | Überprüfen Sie nach dem Konfigurieren der Routing-Richtlinien, ob die Routing-Tabelle aktualisiert wurde, um den Datenverkehr über Cloud NGFW zu leiten. Klicken Sie auf **Route Tables** und wählen Sie **Default** im Abschnitt **Route Tables** aus.



Sie können die Routing-Tabelle **bearbeiten**, um Details zu den Routen bereitzustellen, die der Standard-Routing-Tabelle zugeordnet sind. Datenverkehr, der über das Internet oder zu anderen vNETs geleitet wird, wird über die Cloud NGFW geleitet.



STEP 4 | Wählen Sie ein anderes vNET für das zweite virtuelle Netzwerk aus und klicken Sie dann auf **Create**.

STEP 5 | Nachdem Sie die virtuellen Netzwerke erfolgreich mit dem virtuellen WAN-Hub verbunden haben, stellen Sie sicher, dass der Status **Connected** lautet.

Native Richtlinienverwaltung mit Regelstapeln in Cloud NGFW

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

- Informationen zu Regelstapeln und Regeln in Cloud NGFW für Azure
- Regelstapel in Cloud NGFW für Azure erstellen
- Sicherheitsregelobjekte in Cloud NGFW für Azure
- Sicherheitsdienste in Cloud NGFW für Azure

Informationen zu Regelstapeln und Regeln in Cloud NGFW für Azure

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 setzt es Ihre Regeln durch, um Ihren Datenverkehr zuzulassen oder zu verweigern. Zweitens führt sie eine Inhaltsprüfung bezüglich des zulässigen Datenverkehrs basierend auf Ihren Angaben in den Sicherheitsprofilen durch. Ein Regelstapel enthält eine Reihe von Sicherheitsregeln, zugehörigen Objekten und Profilen.

Ein lokaler Regelstapel besteht aus lokalen Regeln, die zum Definieren von Regeln für bestimmte Anwendungen oder Benutzer verwendet werden. Der Kontoadministrator verknüpft diese Regeln mit einer NGFW-Ressource für das Azure-Konto.

Regelstapel in Cloud NGFW für Azure erstellen

In Cloud NGFW können Sie Regelstapel erstellen, wenn Ihnen die **LocalRuleStackAdmin**-Rolle zugewiesen wurde.

Führen Sie die folgenden Schritte aus, um einen Regelstapel zu erstellen.

STEP 1 | Klicken Sie auf der Microsoft Azure-Startseite auf das Symbol für **Local Rulestack**. Alternativ können Sie auf den gewünschten Regelstapel zugreifen, indem Sie in der Suchleiste der Homepage danach suchen.

STEP 2 | Klicken Sie auf **Create (Erstellen)**.

STEP 3 | Wählen Sie **Subscription** und **Resource Group** aus den jeweiligen Drop-down-Menüs im Abschnitt „Project details“ auf der Registerkarte **Basics** aus.

STEP 4 | Geben Sie einen beschreibenden **Name** für Ihren Regelstapel ein.

STEP 5 | Geben Sie die unterstützte **Region** für Ihren Regelstapel ein.

STEP 6 | Klicken Sie auf die Registerkarte **Tags**.

1. Geben Sie **Name** und **Value** ein.
2. Klicken Sie auf **Review+create**.

STEP 7 | Überprüfen Sie die von Ihnen ausgewählten Regelstapel-Optionen und klicken Sie auf **Create**.

Sicherheitsregelobjekte in Cloud NGFW für Azure

Ein Sicherheitsregelobjekt ist ein einzelnes Objekt oder eine kollektive Einheit, in der diskrete Identitäten wie IP-Adressen, vollqualifizierte Domänennamen (FQDN) 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.
- **Certificate** – Ein Zertifikatsobjekt ist ein Verweis auf ein TLS-Zertifikat, das im Azure Key Vault in Ihrem Azure-Konto gespeichert ist und bei der ausgehenden Entschlüsselung verwendet wird.

  Bei der Verwendung von Azure Key Vault für die ausgehende Entschlüsselung ist die PAN-OS-Version 11.0.x erforderlich.

Präfixliste in Cloud NGFW für Azure 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 | Klicken Sie auf der Startseite auf das Symbol **Local Rulestacks** und wählen Sie einen zuvor erstellten Regelstapel aus, für den Sie eine Präfixliste konfigurieren möchten.

STEP 2 | Klicken Sie im linken Bereich auf **Prefix List** und dann auf **Add**. Der Bereich zum Hinzufügen der Präfixliste wird geöffnet.

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 **Add (Hinzufügen)**.

FQDN-Liste in Cloud NGFW für Azure 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 | Klicken Sie auf der Startseite auf das Symbol **Local Rulestacks** und wählen Sie einen zuvor erstellten Regelstapel aus, für den Sie die FQDN-Liste konfigurieren möchten.

STEP 2 | Klicken Sie im linken Bereich auf **FQDN List** und dann auf **Add**. Der Bereich zum Hinzufügen der FQDN-Liste wird geöffnet.

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 **Add (Hinzufügen)**.

Zertifikat zu Cloud NGFW für Azure hinzufügen

Cloud NGFW verwendet Zertifikate, um die ausgehende Entschlüsselung zu ermöglichen. Diese Zertifikate werden im Azure Key Vault gespeichert.

Für die Entschlüsselung werden derzeit nur selbstsignierte und von der Stammzertifizierungsstelle signierte Zertifikate unterstützt. Verbundene Zertifikate werden nicht unterstützt.

Bei der Verwendung von Azure Key Vault für die ausgehende Entschlüsselung ist die PAN-OS-Version 11.0.x erforderlich.

STEP 1 | Klicken Sie auf der Startseite auf das Symbol **Local Rulestacks** und wählen Sie einen zuvor erstellten Regelstapel aus, für den Sie ein Zertifikat erstellen möchten.

STEP 2 | Klicken Sie im linken Bereich auf **Certificates** und dann auf **Add**. Der Bereich „Add Certificate List“ wird geöffnet.

STEP 3 | Geben Sie einen beschreibenden **Namen** für Ihr Zertifikat ein.

STEP 4 | (optional) Geben Sie eine Beschreibung für Ihr Zertifikat ein.

STEP 5 | Wenn das Zertifikat selbstsigniert ist, wählen Sie **Self Signed Certificate** aus.

STEP 6 | Wenn das Zertifikat nicht selbstsigniert ist, rufen Sie die Zertifikat-URI ab, indem Sie zu **Azure Key Vault** > **-Zertifikaten** navigieren und die URI der geheimen Kennung in die **Zertifikat-URI** kopieren und einfügen.

STEP 7 | (optional) Wählen Sie im Feld **Certificate source** die entsprechende Option aus: **Select from Key vault** aus oder **Paste URI**.

STEP 8 | Klicken Sie auf **Add (Hinzufügen)**.

STEP 9 | Erstellen Sie eine verwaltete Identität in derselben Ressourcengruppe wie der Key Vault. Siehe Create a user-assigned managed identity.

STEP 10 | Navigieren Sie zu **Azure Key Vault**> **Access Policies**.

STEP 11 | Klicken Sie auf **Create**, um eine Zugriffsrichtlinie zu konfigurieren, die der in **Schritt 9** erstellten verwalteten Identität den **Beauftragten der Key Vault-Zertifikate** und den **Benutzer der geheimen Key Vault-Schlüssel** zuweist.

Sicherheitsregeln in Cloud NGFW für Azure 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 Azure 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.

STEP 1 | Klicken Sie auf der Startseite auf das Symbol **Local Rulestacks** und wählen Sie einen zuvor erstellten Regelstapel aus, zu dem Sie Regeln hinzufügen möchten.

STEP 2 | Klicken Sie auf **Rules** und dann auf **Add**.

STEP 3 | Geben Sie im Abschnitt „General“ einen beschreibenden **Name** 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**, **Match** oder **Exclude** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von der Quelle anhand der Regel ausgewertet.
2. Wenn Sie **Match** auswählen, geben Sie IP-Adresse (CIDR), Präfixliste, Länder, intelligente Feeds oder die dynamische Präfixliste an.

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

1. Wählen Sie **Any**, **Match** oder **Exclude** aus.

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig vom Ziel anhand der Regel ausgewertet.
2. Wenn Sie **Match** wählen, geben Sie Präfixliste, FQDN-Liste und Länder an.

STEP 9 | Stellen Sie die granulare Steuerung ein.

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, geben Sie die Anwendungen an.

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

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

   Wenn Sie **Any (Beliebig)** auswählen, wird der Datenverkehr unabhängig von der URL ausgewertet.
2. Wenn Sie **Select** auswählen, wählen Sie eine der **Predefined Categories** aus dem Drop-down-Menü aus.

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

1. Wählen Sie **application-default**, **Any** oder **Select** aus.

   Wenn Sie **Any** 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** entscheiden, wählen Sie das Protokoll aus der Drop-down-Liste aus und geben Sie die Portnummer ein. Sie können eine einzelne Portnummer angeben.

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**, **Deny**, **Drop** oder **Reset both client and server**.
2. Aktivieren Sie die **Egress Decryption**.
3. Aktivieren Sie **Logging (Protokollierung)**.

STEP 13 | Klicken Sie auf **Add (Hinzufügen)**.

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

Sicherheitsdienste in Cloud NGFW für Azure

Cloud NGFW verwendet Ihre Regelstapeldefinitionen, um Ihren VNet-Datenverkehr (Azure Virtual Network) 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** –(standardmäßig aktiviert und basierend auf Best Practices vorkonfiguriert) Ein Sicherheitslückenprofil für ein 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.

  Best Practice-Konfiguration

  Die folgende Best-Practice-Konfiguration für Sicherheitslücken ist in Cloud NGFW für Azure standardmäßig aktiviert.

Signatur Schweregrad	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.

Best Practice-Konfiguration

Die folgende Best-Practice-Konfiguration für Anti-Spyware ist in Cloud NGFW für Azure standardmäßig aktiviert.

Signatur Schweregrad	Aktion
Kritisch	Beide zurücksetzen

Signatur Schweregrad	Aktion
Hoch	Beide zurücksetzen
Mittel	Beide zurücksetzen
Informativ	Standard
Niedrig	Standard

Signaturen für IPS-Sicherheitslücken und Anti-Spyware

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

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

Bedrohungskategorie	Beschreibung
	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-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

Bedrohungskategorie	Beschreibung
	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 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

Bedrohungskategorie	Beschreibung
	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 hängen meist mit Malware und Cyberangriffen zusammen. Hacking-Tools können auch auf harmlose Weise eingesetzt werden, z. B. für Red- and Blue-Team-Übungen, Penetrationstests und Forschung und Entwicklung. Die Verwendung oder der Besitz dieser Tools ist in manchen Ländern illegal, unabhängig von der Nutzungsabsicht.
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.

Bedrohungskategorie	Beschreibung
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. Web-Shells müssen zuerst von einem bösartigen Akteur auf dem kompromittierten Host implantiert werden, 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.

  Best Practice-Konfiguration

  Die folgende Best-Practice-Konfiguration für Antivirus ist in Cloud NGFW für Azure standardmäßig aktiviert.

Protokoll	Aktion
FTP	Beide zurücksetzen

Protokoll	Aktion
HTTP	Beide zurücksetzen
HTTP2	Beide zurücksetzen
IMAP	Beide zurücksetzen
POP3	Alarm
SMB	Beide zurücksetzen
SMTP	Beide zurücksetzen

- **File Blocking** – (standardmäßig aktiviert und basierend auf Best Practices vorkonfiguriert) Mithilfe von Dateiblockierungsprofilen können Sie bestimmte Dateitypen identifizieren, 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.

Best Practice-Konfiguration

Die folgende Best-Practice-Konfiguration für die Dateiblockierung ist in Cloud NGFW für Azure standardmäßig aktiviert.

Dateitypen	Anwendung	Richtung	Aktion
Alle riskanten Dateitypen: • 7z • bat • cab • chm • class • cpl • dll • exe • flash • hip • hta	Alle	Beides (Upload und Download)	Blockieren

Dateitypen	Anwendung	Richtung	Aktion
• msi • Multi-Level-Encoding • ocx • PE • pif • rar • scr • tar • torrent • vbe • wsf • verschlüsselt-rar • verschlüsselt-zip			
Alle übrigen Dateitypen	Alle	Beides (Upload und Download)	Alarm

Antivirus-Signaturen

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).

Bedrohungskategorie	Beschreibung
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). • 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 – (standardmäßig aktiviert und basierend auf Best Practicesvorkonfiguriert) Mit URL-Filterprofilen können Sie überwachen und steuern, wie Benutzer über HTTP und HTTPS auf das Internet 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.

Best Practices-Konfiguration

Die URL-Filterung ist standardmäßig aktiviert und verwendet eine auf Best Practices basierende Sicherheitsrichtlinie.

URL-Kategorien	Websitezugriff	Übermittlung von Anmeldeinformationen
Schädliche und ausbeuterische Kategorien: • Erwachsener • Command-and-Control • Urheberrechtsverletzung • Dynamische DNS • Extremismus • Malware • Geparkt • Phishing • Proxy-Vermeidung und Anonymisierung • Unbekannt	Blockieren	Blockieren
Alle anderen URL-Kategorien	Alarm	Alarm

Vordefinierte URL-Kategorien für Cloud NGFW für Azure

In der folgenden Tabelle werden die vordefinierten URL-Kategorien beschrieben, die in Cloud NGFW für Azure 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.

URL-Kategorie	Beschreibung
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 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.

URL-Kategorie	Beschreibung
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 oder keinen Inhalt präsentieren, API-Zugriff gewähren, der nicht für die Anzeige durch Endbenutzer vorgesehen ist, oder eine Authentifizierung erfordern, ohne andere Inhalte anzuzeigen, die auf eine andere Kategorisierung schließen lassen. Sollte keine Websites enthalten, die Fernzugriff ermöglichen, wie etwa webbasierte VPN-Lösungen, webbasierte E-Mail-Dienste oder Seiten zum Phishing identifizierter Anmeldeinformationen.
Neu registrierte Domäne	Neu registrierte Domänen werden häufig absichtlich oder durch Domänengenerierungsalgorithmen generiert und für bösartige Aktivitäten verwendet.
Geparkt	Von Einzelpersonen registrierte Domänen, die oft später für Anmeldedaten-Phishing verwendet werden. Diese Domänen können legitimen Domänen ähneln, z. B. pal0alto0netw0rks.com, mit der Absicht, Anmelde-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

URL-Kategorie	Beschreibung
	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. 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,

URL-Kategorie	Beschreibung
	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 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 mit persönlichen Finanzinformationen oder Finanzberatung, wie etwa Online-Banking, Kredite, Hypotheken, Schuldenverwaltung, Kreditkarten- und Versicherungsunternehmen. Umfasst keine Websites mit Bezug zu Wertpapiermärkten, Maklerdiensten oder Handelsdienstleistungen. Umfasst Websites zum Umtausch

URL-Kategorie	Beschreibung
	von Fremdwährungen. Umfasst Websites zum Umtausch von Fremdwährungen.
Glücksspiel	Lotterie- oder Glücksspiel-Websites, die den Tausch von echtem und/oder virtuellem Geld ermöglichen. Verwandte Websites, die Informationen, Tutorials oder Ratschläge zum Glücksspiel, einschließlich Wettquoten und Tippgemeinschaften, bereitstellen. Unternehmenswebsites von Hotels und Casinos, die kein Glücksspiel ermöglichen, 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, Gesundheitsproblemen sowie traditionellen und nicht traditionellen Tipps, Heilmitteln und Behandlungen. Umfasst außerdem Websites für verschiedene medizinische Fachrichtungen, Praxen und Einrichtungen (wie Fitnessstudios und Fitnessclubs) sowie Fachleute. Websites zu Krankenversicherungen und Schönheitsoperationen sind ebenfalls enthalten.
Haus und Garten	Informationen, Produkte und Dienstleistungen in Bezug auf Hausreparatur und -wartung, Architektur, Design, Bau, Dekoration und Gartenarbeit.
Jagen und Fischen	Jagd- und Angeltipps, Anleitungen, Verkauf von dazugehöriger Ausrüstung und Utensilien.
Internetkommunikation und Telefonie	Websites, die Dienste für Video-Chats, Instant Messaging oder Telefoniefunktionen unterstützen oder bereitstellen.
Internetportale	Websites, die als Ausgangspunkt für Benutzer dienen, normalerweise durch die gesammelte Darstellung einer breiten Palette von Inhalten und Themen.

URL-Kategorie	Beschreibung
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 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.

URL-Kategorie	Beschreibung
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, 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

URL-Kategorie	Beschreibung
	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.
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.

URL-Kategorie	Beschreibung
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 kostenpflichtig 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-Bildung und -Schulung sowie entsprechende Materialien anbieten. Kann Fahr-/ Verkehrsschulen, Schulungen am Arbeitsplatz usw. umfassen.
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.
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.

DNS-Sicherheit in Cloud NGFW für Azure aktivieren

Domain Name Service (DNS) ist ein wichtiges und grundlegendes Internetprotokoll, wie in den wichtigsten RFCs für das Protokoll beschrieben. Böswillige Akteure haben 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 Ihrem Netzwerk kompromittiert und dann DNS-Lookup verwendet, um Daten aus dem Netzwerk an eine Domäne zu senden, die er kontrolliert. Bösartige Akteure können außerdem schädliche Daten/Nutzlasten über DNS in die Netzwerk-Workloads einschleusen. Im Laufe der Jahre wurden im Rahmen der Untersuchungen der Unit 42 von Palo Alto Networks unterschiedliche Arten von DNS-Missbrauch entdeckt.

Mit Cloud NGFW für Azure können Sie Ihren vNet- und vWAN-Datenverkehr vor erweiterten DNS-basierten Bedrohungen schützen, indem die Domänen überwacht und gesteuert werden, die von Ihren Netzwerkressourcen abgefragt werden. Mit Cloud NGFW für Azure können Sie den Zugriff auf die Domänen verweigern, die Palo Alto Networks für bösartig oder verdächtig hält, und alle anderen Abfragen zulassen.

Zu diesem Zweck nutzt Cloud NGFW den DNS-Sicherheitsdienst 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). Der DNS-Sicherheitsdienst verteilt diese DNS-Signaturen dann an Ihre Cloud NGFW-Ressourcen, um proaktiv vor Malware zu schützen, die DNS für Command-and-Control (C2) und Datendiebstahl verwendet.

Wenn die DNS-Sicherheit aktiviert ist, führt die Cloud NGFW für jede DNS-Sicherheitskategorie die folgenden Aktionen aus.

Kategorie	Protokollschweregrad	Aktion
Anzeigenverfolgungsdomänen	Informativ	Zulassen
Command-and-Control-Domänen (C2)	Hoch	Blockieren
Dynamic DNS-Domänen (DDNS)	Informativ	Zulassen
Grayware-Domänen	Niedrig	Blockieren
Malware-Domänen	Mittel	Blockieren
Neu registrierte Domänen	Informativ	Zulassen
Geparkte Domänen	Informativ	Zulassen
Phishing-Domänen	Niedrig	Blockieren

Kategorie	Protokollschweregrad	Aktion
Proxy-Vermeidung und Anonymisierer	Niedrig	Blockieren

Um den DNS-Verkehr zu überprüfen, müssen Sie den DNS-Proxy auf Ihrer Cloud NGFW für Azure aktivieren.

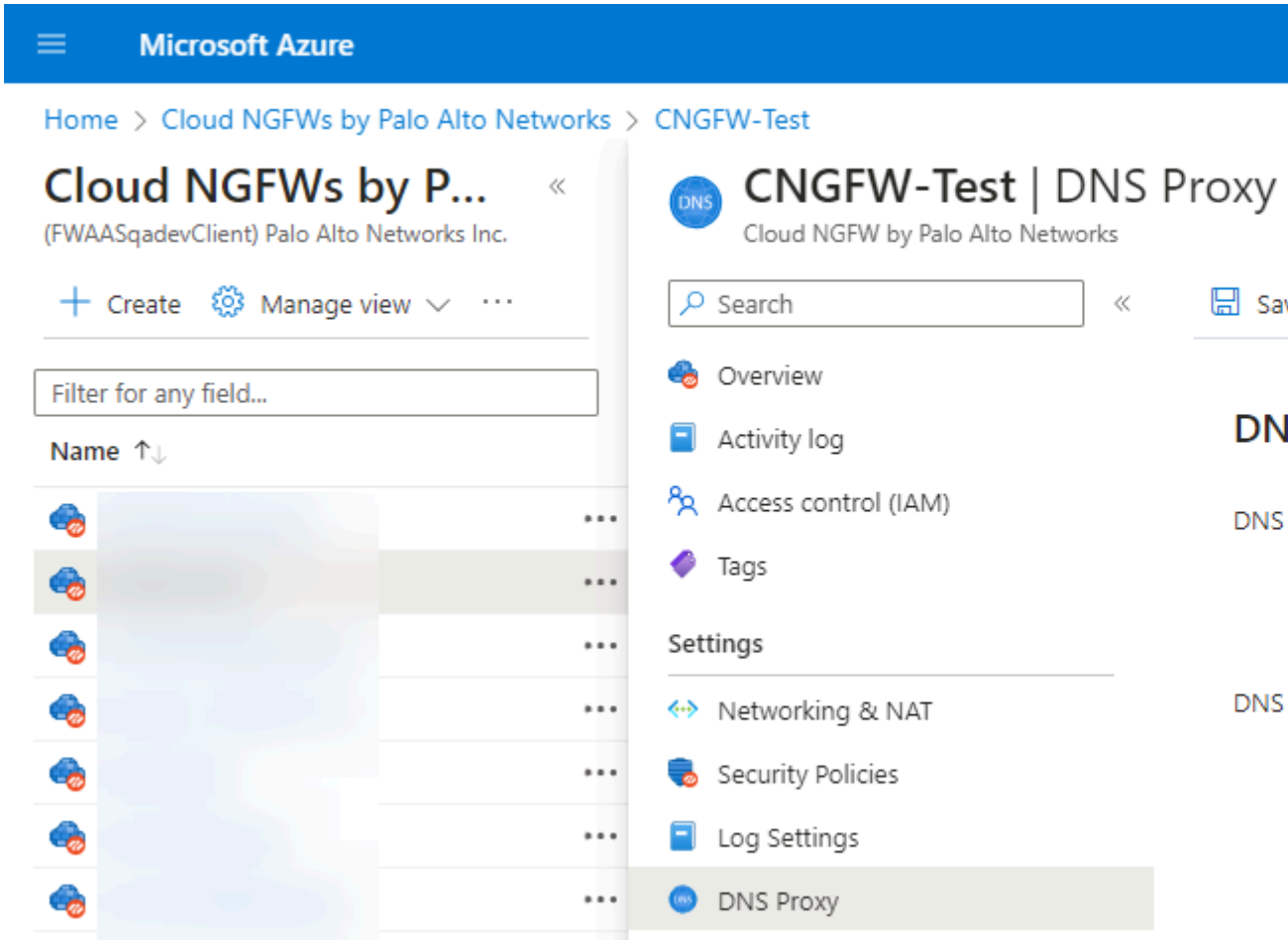
STEP 1 | Melden Sie sich beim Azure-Portal an.

STEP 2 | Klicken Sie unter „Azure Services“ auf das Symbol „Cloud NGFWs“.

STEP 3 | Wählen Sie Ihre Cloud NGFW-Instanz aus.

STEP 4 | DNS-Proxy aktivieren.

1. Wählen Sie **Settings** > **DNS Proxy** aus.
2. Wählen Sie das Optionsfeld **Enabled** aus.
3. Verwenden Sie den Standard-DNS-Server oder wählen Sie **Custom** aus und geben Sie einen zuvor in Ihrem virtuellen Netzwerk konfigurierten DNS-Server an.
4. Klicken Sie auf **Save (Speichern)**.

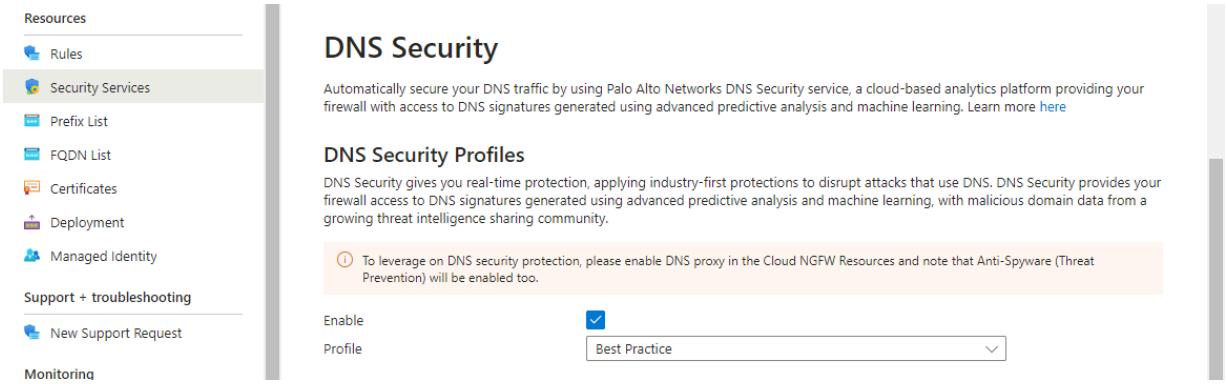


STEP 5 | Navigieren Sie zum lokalen Regelstapel, der Ihrer Cloud NGFW-Instanz zugeordnet ist.

STEP 6 | Wählen Sie **Security Services** aus.

STEP 7 | Aktivieren Sie **DNS Security**.

Zum Aktivieren der DNS-Sicherheit muss auch Anti-Spyware aktiviert sein. Darüber hinaus müssen sowohl die DNS-Sicherheit als auch Anti-Spyware auf Best Practices eingestellt sein.



Ausgehende Entschlüsselung in Cloud NGFW für Azure 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 Verwendung von Azure Key Vault für die ausgehende Entschlüsselung ist die PAN-OS-Version 11.0.x erforderlich.

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 Ihr VNet 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 Profiles** > **Egress Decryption** aus.

STEP 3 | Wählen Sie ein Zertifikat aus.

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

Zertifikat zu Cloud NGFW für Azure hinzufügen, *wenn Sie dies noch nicht getan haben.*

Das Zertifikat und der private Schlüssel werden im Azure Key Vault gespeichert, und der Workload verwendet diese Informationen, um den Datenverkehr zu entschlüsseln.

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

```
Zertifikat: Daten: Version: 3 (0x2) Seriennummer: 4121 (0x1019)
 Signature Algorithm: sha256WithRSAEncryption Issuer: C=US,
 ST=Washington, L=Seattle, O=Example Company Root CA, OU=Corp,
```



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

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

PKCS8 ist das unterstützte Zertifikatformat.

Vertrauenswürdige Zertifikate können nicht selbstsigniert werden, aber das nicht vertrauenswürdige Zertifikat kann selbstsigniert oder von einer Zertifizierungsstelle signiert sein.

STEP 4 | Navigieren Sie zum zuvor erstellten **Regelstapel** und gehen Sie zur Seite **Managed Identity**.

STEP 5 | Wählen Sie im Drop-down-Menü **Enable MI** die verwaltete Identität aus, die dem Key Vault zugeordnet wurde.

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

Eingehende Entschlüsselung in Cloud NGFW für Azure 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 VNets eine vollständige Sichtbarkeit der Identität der Quelle.

Sie müssen das Webzertifikat und den privaten Schlüssel als eine `pem`- oder `pfx`-Datei verknüpfen und in den Azure Key Vault hochladen, um eine SSL-Eingangsprüfung 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.

Sie dürfen das Zertifikat und den Schlüssel nicht separat in den Azure Key Vault hochladen.

-

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.
- **Priority** – 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.

- Legen Sie die **Übereinstimmungskriterien für Anwendungen** fest, die die Regel zulassen oder blockieren soll.

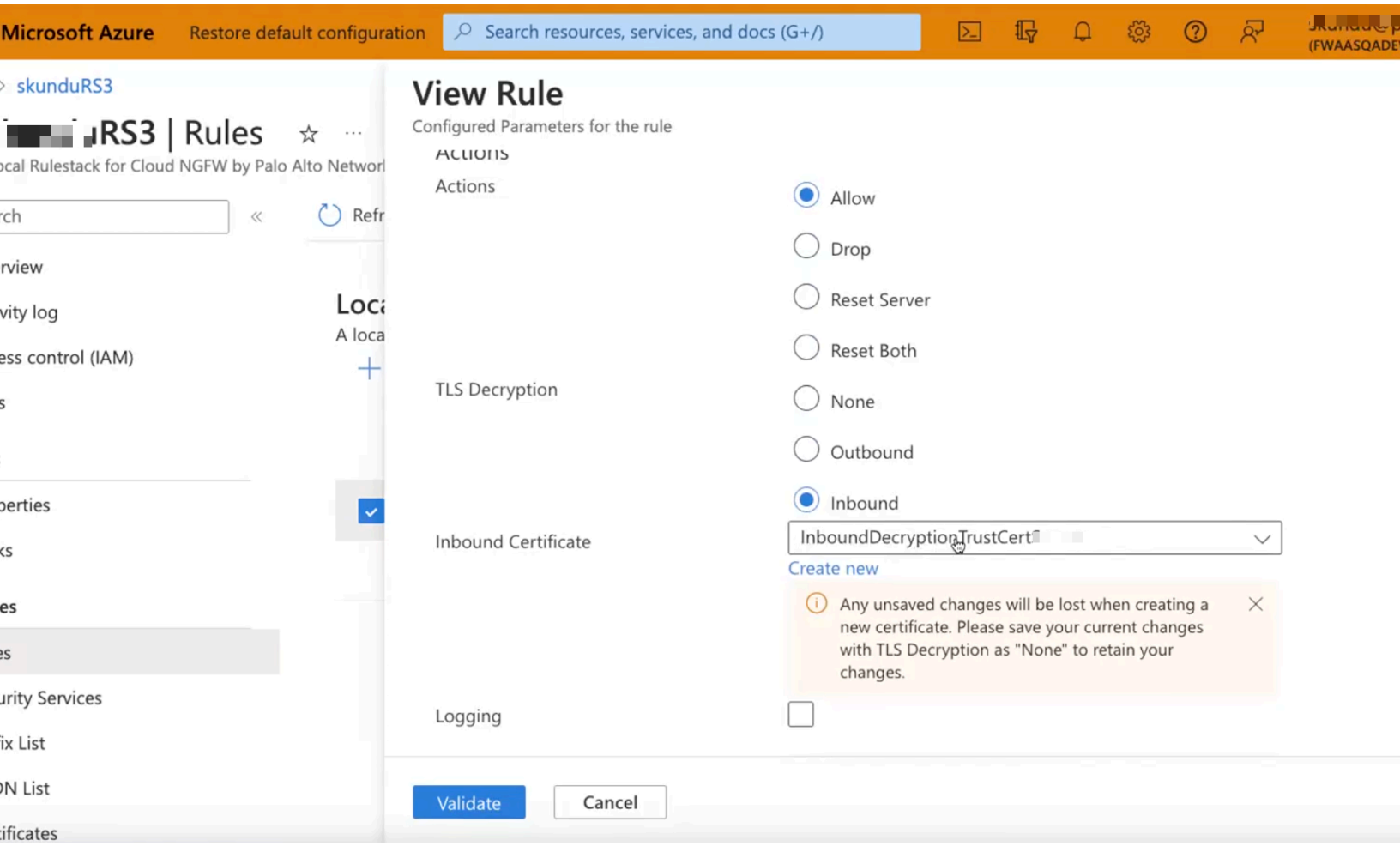
  *Sie können TLS-Entschlüsselungsregeln mit **Applications–Any** oder nur **SSL–Match** erstellen.*

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

  Schritt 6: Festlegen von **A**

- **Allow (Zulassen)** – Datenverkehr zulassen.
- **Drop** – 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 6 | 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 Azure-Ressourcenname (ARN) des Geheimnisses muss beim Erstellen des Zertifikatobjekts im Zertifikat-ARN verwendet werden.*
- *PKCS8 ist das unterstützte Zertifikatformat.*
- *Die eingehende Entschlüsselung unterstützt selbstsignierte und von der Stammzertifizierungsstelle signierte Zertifikate, aber keine verketteten 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 7 | Wählen Sie **Logging** aus, um die Protokollierung zu aktivieren.

STEP 8 | Klicken Sie auf **Validate**.

STEP 9 | Klicken Sie auf **Config ActionsDeploy ConfigurationCommit**, um die Regel in der laufenden Konfiguration der Firewall zu speichern.

Panorama-Richtlinienverwaltung

Verwenden Sie die Informationen in diesem Abschnitt, um Cloud NGFW für Azure mit der virtuellen Panorama-Appliance von Palo Alto Networks zu konfigurieren und zu integrieren.

Panorama-Integration

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

In diesem Dokument erfahren Sie, wie Sie Cloud NGFW für Azure 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 Hardware-Firewalls, virtuellen Firewalls und Cloud-Firewalls. Dies erhöht die Betriebseffizienz bei der Verwaltung und Wartung eines hybriden Firewallnetzwerks.

Wie funktioniert die Integration?

Wenn Sie über das Azure-Portal eine Cloud NGFW-Ressource erstellen, haben Sie die Möglichkeit, Ihre Sicherheitsrichtlinien mit Palo Alto Networks Panorama zu verwalten. Sie können dann einen gemeinsamen Satz von Sicherheitsregeln zentral auf Cloud NGFW-Ressourcen verwalten, die Sie neben Ihren physischen und virtuellen Firewall-Geräten erstellen, und Sie können Protokollierung, Berichterstellung und Protokollanalyse verwenden – alles von einer Panorama-Konsole aus.

Wenn eine Firewall einen fehlerhaften Zustand erreicht und die Verbindung getrennt wird, wird sie nach einer gewissen Zeit (normalerweise 3 Tage) aus Panorama entfernt. Dadurch wird sichergestellt, dass die Firewall nicht vorzeitig gelöscht wird.

Integrationskomponenten

Die folgenden Palo Alto Networks-Komponenten werden verwendet, um Ihre Cloud NGFW-Ressource in Panorama zu integrieren.

Palo Alto Networks Policy Management ist die primäre und obligatorische Komponente der Lösung. Sie müssen eine **Panorama**-Appliance 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 Azure-Regionen zuzuordnen.

Das **Panorama Azure-Plug-in** ist eine obligatorische Komponente dieser Lösung. Mit dem Panorama Azure-Plug-in können Sie Cloud-Gerätegruppen und Cloud-Vorlagenstapel erstellen, mit denen Sie Richtlinien und Objekte auf mit Panorama verknüpften NGFW-Ressourcen verwalten können.

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 DGs mithilfe der Panorama Azure Plug-in-Benutzeroberfläche, indem Sie die Cloud NGFW-Ressource und die Azure-Regionsinformationen angeben. Cloud DG manifestiert sich als globaler Regelstapel in dieser Region.

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

Cloud-Vorlagenstacks (Cloud Template Stacks, Cloud TS) sind Panorama-Vorlagenstacks für spezielle Zwecke, die es Ihren Sicherheitsregeln in Cloud-Gerätegruppen ermöglichen, auf Objekteinstellungen zu verweisen, die Sie mit Panorama mithilfe von Vorlagen verwalten können. Beim Erstellen einer Cloud-Gerätegruppe können Sie mit dem Panorama Azure-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 der Vorlagenstapel der nativen Panorama-Benutzeroberfläche verwenden, um Ihre Vorlagen zu konfigurieren und sie diesen Cloud-Vorlagenstapeln hinzuzufügen.

Sie können den Namen des Vorlagenstapels nach der Bereitstellung der Cloud NGFW nicht mehr ändern.

- 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.

Sie weisen verwaltete Geräte keinen Cloud-Gerätegruppen und Cloud-Vorlagenstapeln zu.

Integrationsschritte

Die Integration von Cloud NGFW in Panorama erfordert nur wenige Schritte. Sie bereiten zunächst Ihre virtuelle Panorama-Appliance für diese Integration vor, indem Sie das Azure-Plug-in installieren. Nachdem Sie Cloud NGFW erfolgreich verknüpft haben, verwenden Sie Panorama, um Sicherheitsobjekte und -regeln zu verwalten.

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

- Überprüfen Sie, ob Panorama die Voraussetzungen für die Panorama-Integration erfüllt.
- Verknüpfen Sie Panorama mit der Cloud NGFW.

- Verwenden Sie Panorama für die Richtlinienverwaltung in Cloud NGFW.

Beachten Sie Folgendes, wenn Sie Ihre Cloud NGFW-Ressource in Panorama integrieren:

- *Um eine Cloud NGFW-Ressource in ein anderes Panorama zu verschieben, müssen Sie sie erneut bereitstellen.*
- *Wenn Sie nach der Bereitstellung der Cloud NGFW-Ressource einen Protokollsammler hinzufügen, müssen Sie ihn erneut bereitstellen.*
- *Wenn Sie die Panorama-IP-Adresse ändern, muss auch sie erneut bereitgestellt werden.*

Voraussetzungen für die Panorama-Integration

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

- Panorama einrichten.
  - Installieren Sie Panorama mit der Softwareversion 11.0.1-h1 und höher oder 10.2.4-h2 oder höher.
  - Stellen Sie sicher, dass Sie eine registrierte Panorama-Instanz mit Lizenzen mit der erforderlichen Kapazität installiert haben, um Ihre Cloud NGFW für die Azure-Bereitstellung zu unterstützen und sie mithilfe der Supportlizenz im Customer Support Portal (CSP) zu aktivieren.

    Sie müssen das Gerätezertifikat auf dem Panorama-Verwaltungsserver installieren, um Panorama erfolgreich beim Palo Alto Networks Customer Support Portal (CSP) zu authentifizieren und einen oder mehrere Cloud-Dienste zu nutzen.
  - Stellen Sie sicher, dass Sie ein Palo Alto Networks Customer Support Portal-Konto besitzen, bei dem Ihre Organisation die Panorama-Appliance registriert hat.

    Für die Cloud NGFW- und Panorama-Integration sollte die E-Mail-Adresse verwendet werden, die für die Registrierung beim CSP-Konto verwendet wurde. Wenn diese E-Mail-Adresse abweicht, können Sie Cloud NGFW nicht konfigurieren und in Panorama integrieren.
- Installieren Sie das Azure-Plug-in, Version 5.0.0.
- Stellen Sie sicher, dass Sie in Ihrer Panorama-Anwendung über die Rolle eines Panorama-Administrators verfügen.
- Stellen Sie sicher, dass Ihr Netzwerk Datenverkehr zulässt, der auf die folgenden Ports Ihrer virtuellen Panorama-Appliance abzielt, um die Kommunikation zwischen Cloud NGFW und Panorama sicherzustellen: 3978, 28443, 28270.

Konnektivitätsszenarien

Zusätzlich zu den oben aufgeführten Punkten müssen Sie auch berücksichtigen, wie Ihre Cloud NGFW-Ressourcen eine Verbindung zu Panorama herstellen. Um die Cloud NGFW-Richtlinie mit Panorama zu verwalten, muss Panorama über eine Verbindung mit dem VNet verfügen. Abhängig von Ihrer Netzwerktopologie wird die Konnektivität zwischen Panorama und Ihrem VNet jedoch unterschiedlich aktiviert.

- **Privater Netzwerkzugriff mit privater Panorama-IP** – Sie können Panorama direkt in Ihrem privaten Hub-VNet-Subnetz oder in einem anderen VNet bereitstellen, das mit dem Cloud NGFW-VNet verbunden ist.

  Bei der direkten Bereitstellung im privaten Subnetz Ihres Hub-VNet stellt Panorama eine direkte Verbindung mit Ihren Cloud NGFW-Ressourcen her, da sich diese im selben Subnetz befinden. Wenn Sie Panorama in einem VNet bereitstellen, das mit dem privaten Subnetz des Hub-VNet verbunden ist, das mit Cloud NGFW verknüpft ist, ermöglicht das VNet-Peering der Cloud NGFW-Ressource, die private IP-Adresse von Panorama zu erreichen.

- **Panorama-Zugriff über VPN vor Ort** – Wenn Ihre Panorama-Instanz vor Ort bereitgestellt wird, können Cloud NGFW-Ressourcen die private IP-Adresse von Panorama über ein VPN erreichen. Darüber hinaus unterstützt dieses Szenario das VNet-Peering.

  In diesem Szenario wird Panorama in Ihrem lokalen Netzwerk bereitgestellt und verwendet eine VPN-Gateway-Verbindung direkt zum Cloud NGFW-Hub-VNet oder zu einem Hub-VNet, das mit dem Cloud NGFW-Hub-VNet verbunden ist. In jedem Fall muss das Hub-VNet über eine Route verfügen, die auf den VPN-Tunnel mit der privaten IP-Adresse von Panorama als Ziel verweist. Weitere Informationen zum Konfigurieren dieses Setups finden Sie unter Configure VPN gateway transit for virtual network peering.
- **Öffentlicher IP-Zugriff auf Panorama über das Internet** – Wenn zwischen Panorama und Ihrem Cloud NGFW-Hub-VNet keine VNet-Peering-, VPN- oder VWAN-Konnektivität besteht, können Ihre Cloud NGFW-Ressourcen über das Internet eine Verbindung mit der öffentlichen IP-Adresse von Panorama herstellen. Um diese Konnektivität zuzulassen, müssen Sie in Azure eine Netzwerksicherheitsgruppenregel erstellen, um eingehenden Datenverkehr von der öffentlichen IP-Adresse der Cloud NGFW zu den von Panorama verwendeten Ports zuzulassen.
- **Von überall auf Panorama zugreifen (VWAN)** – Cloud NGFW für Azure wird als verwalteter SaaS-Dienst im Azure VWAN bereitgestellt und kann daher den gesamten Datenverkehr sichern, der über den VWAN-Hub läuft. Ihre Cloud NGFW-Ressourcen können eine Verbindung mit der privaten IP-Adresse einer Panorama-Instanz herstellen, die an einem beliebigen Standort bereitgestellt wird, der mit Ihrem VWAN-Hub verbunden ist.

  Wenn Ihre Azure VWAN-Bereitstellung über eine Netzwerksicherheitsgruppe für Ost-West-Datenverkehr verfügt, müssen Sie eine Netzwerksicherheitsgruppenregel erstellen, die eingehenden Datenverkehr von der privaten IP-Adresse der Cloud NGFW-Ressource zur privaten IP-Adresse von Panorama zulässt.

Verknüpfen von Cloud NGFW mit Palo Alto Networks Management

Erstellen einer Cloud-Gerätegruppe

Nachdem Sie die Umgebung für die Integration vorbereitet haben, können Sie Cloud NGFW mit der virtuellen Panorama-Appliance verknüpfen und mit der Richtlinienverwaltung beginnen. Sie beginnen mit der Erstellung einer Cloud-Gerätegruppe.

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 gerätegruppenspezifische Regeln und Objekte 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.

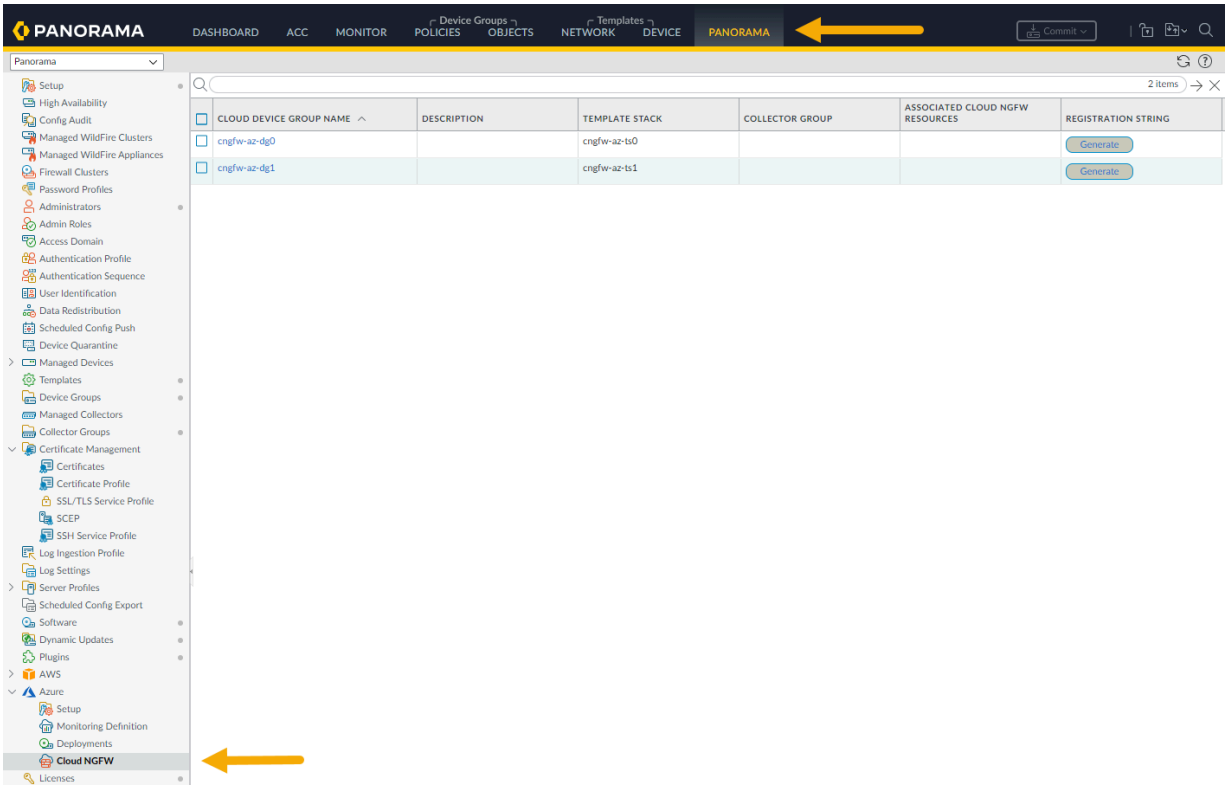
So fügen Sie mithilfe der Panorama-Konsole eine Cloud-Gerätegruppe und einen Vorlagenstapel hinzu:

STEP 1 | Wählen Sie in der Panoramakonsole **Panorama** aus.

STEP 2 | Wählen Sie im Navigationsbaum das **Azure**-Plug-in aus.

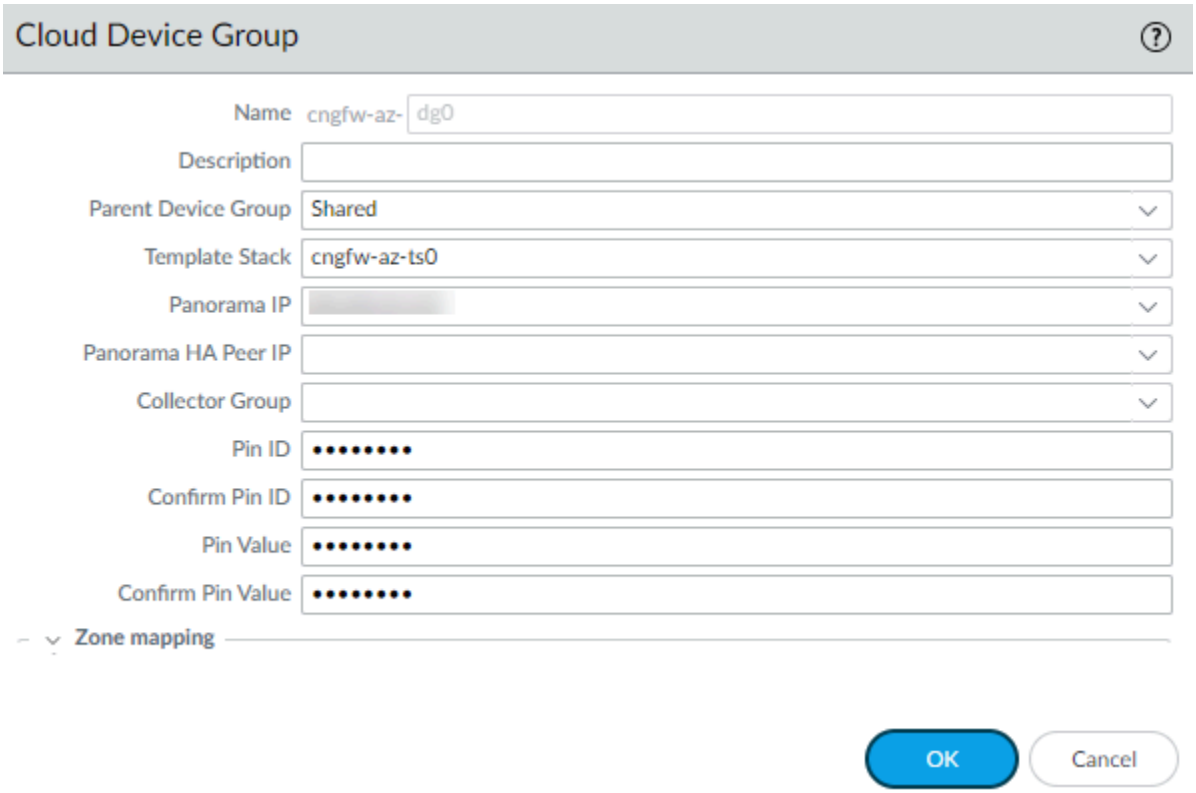
STEP 3 | Erweitern Sie das Azure-Plug-in, um Konfigurationsoptionen anzuzeigen. Wählen Sie **Cloud NGFW** aus, um den Bildschirm für die Cloud-Gerätegruppe anzuzeigen. Wenn die Option „Cloud NGFW“

nicht angezeigt wird, überprüfen Sie, ob Sie das Azure-Plug-in erfolgreich installiert haben. Wählen Sie **Panorama** > **Plugins**, um die Liste der installierten Plug-ins anzuzeigen.



STEP 4 | Klicken Sie im unteren linken Bereich der Panorama-Konsole auf **Add**, um eine neue Cloud-Gerätegruppe zu erstellen.

STEP 5 | Im Bildschirm „Cloud Device Group“:

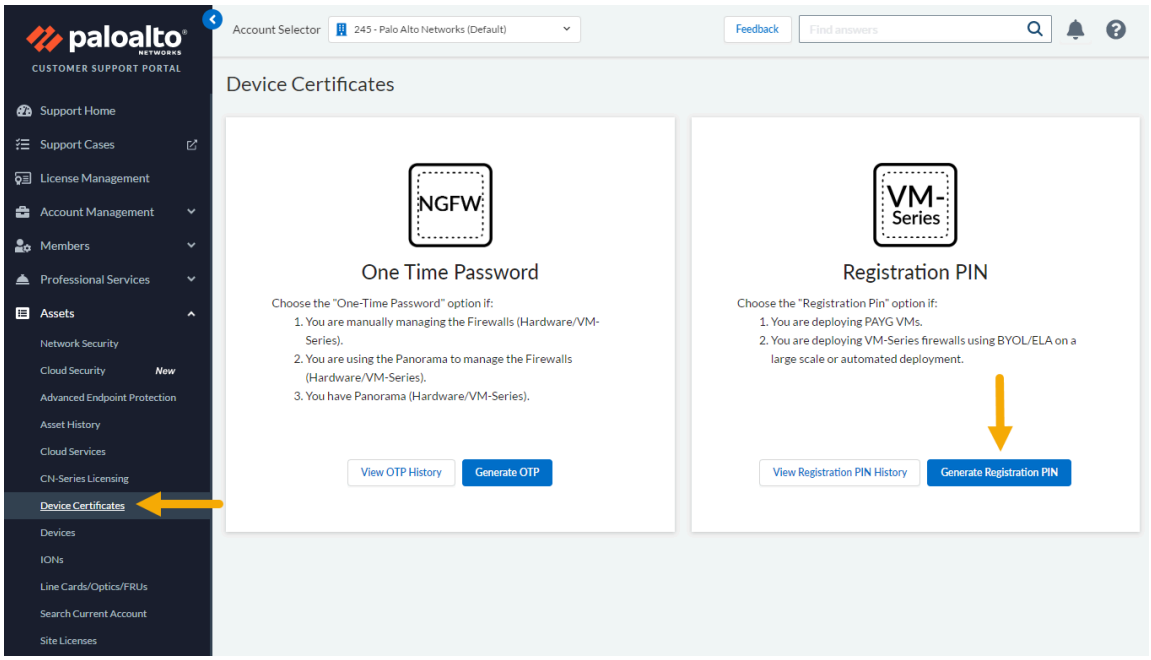


1. Geben Sie einen eindeutigen **Namen** für die Cloud-Gerätegruppe ein.
2. Geben Sie eine **Beschreibung** ein.
3. Wählen Sie im Drop-down-Menü die **Übergeordnete Gerätegruppe** aus. Standardmäßig wird dieser Wert freigegeben.
4. Wählen Sie im Drop-down-Menü den Vorlagenstapel aus. Oder klicken Sie auf **Add**, um einen neuen zu erstellen. Sie können den Namen des Vorlagenstapels nach der Bereitstellung der Cloud NGFW nicht ändern.
5. Wählen Sie die von der Bereitstellung verwendete **Panorama IP**-Adresse aus. Im Drop-down-Menü können Sie entweder die *private* oder *öffentliche* IP-Adresse auswählen.
6. Wählen Sie optional die Panorama HA **Peer IP**-Adresse.
7. Wählen Sie optional im Drop-down-Menü die Kollektorgruppe aus.
8. Geben Sie die **PIN-ID** an. Dieser Wert wird vom Customer Support Portal bereitgestellt.

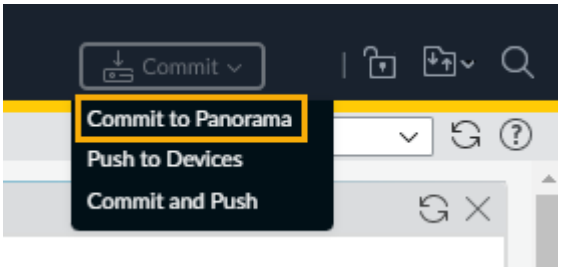
   Um die PIN abzurufen, benötigen Sie ein Konto im Palo Alto Networks Customer Support Portal (CSP).

   Die PIN-ID läuft nach einem Jahr ab. Dies ist optional, wenn Sie die Cloud NGFW-Seriennummer bereits registriert haben. Wenn sie noch nicht registriert ist, registrieren Sie Ihre Cloud NGFW unter Verwendung der Seriennummer für dasselbe CSP-Konto, in dem Sie Ihre virtuelle Panorama-Appliance registriert haben.
9. Um die PIN-ID und den PIN-Wert abzurufen, melden Sie sich als registrierter Benutzer im **Customer Support Portal** an.

10. Wählen Sie auf der Customer Support Portal-Seite **Assets** > **Device Certificates** aus.
11. Wählen Sie auf der Seite **Device Certificate** für die Firewall der VM-Serie die Option **Generate Registration PIN** aus.



12. Kopieren Sie die neu erstellten Registrierungs-IDs und fügen Sie sie in das Feld **PIN ID** und **PIN Value** im Bildschirm „Cloud Device Group“ ein.
13. Bestätigen Sie die PIN-ID und den PIN-Wert.
14. Konfigurieren Sie optional die Zonenzuordnung für die Cloud-Gerätegruppe. Es werden nur 2 Zonen unterstützt: *öffentlich* und *privat*.
15. Klicken Sie auf **OK**.
16. Übernehmen Sie Ihre Änderung in der Panorama-Konsole, um die Cloud-Gerätegruppe zu erstellen. Generieren Sie als Nächstes die Registrierungszeichenfolge, um die Cloud NGFW-Ressource zu erstellen und in Azure bereitzustellen.



In einigen Fällen kann beim Konfigurieren einer Cloud-Gerätegruppe ein Validierungsfehler auftreten. Um dieses Problem zu beheben, stellen Sie sicher, dass das Azure Plug-in für Panorama mithilfe von Administratoranmeldeinformationen ordnungsgemäß installiert ist. Installieren Sie das Plug-in für HA-Umgebungen auf dem Sekundärknoten und dann auf dem Primärknoten.

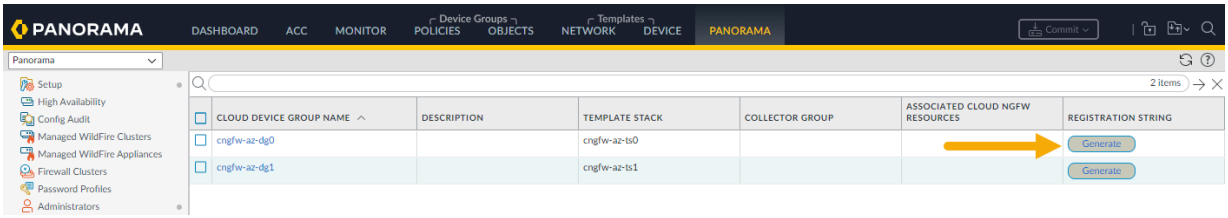
Erstellen der Registrierungszeichenfolge zum Erstellen der Cloud NGFW und Bereitstellen in Azure

Nachdem Sie die Änderung zum Erstellen der Cloud-Gerätegruppe übernommen haben, können Sie die Registrierungszeichenfolge generieren. Diese Zeichenfolge wird zum Erstellen und Bereitstellen der Cloud NGFW in Azure verwendet.

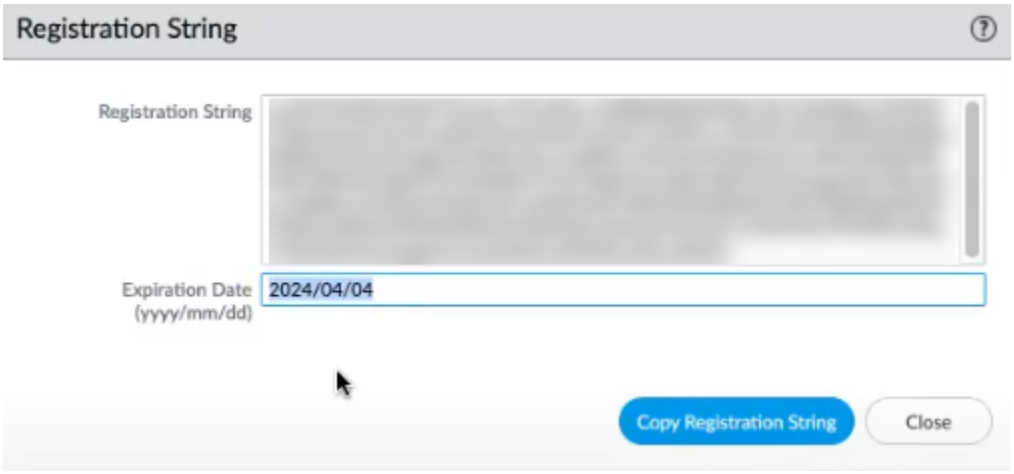
So rufen Sie die PIN ab:

STEP 1 | Suchen Sie in der Panorama-Konsole nach der Cloud-Gerätegruppe, die Sie im vorherigen Abschnitt erstellt haben.

STEP 2 | Klicken Sie im Feld „Registration String“ auf **Generate**.

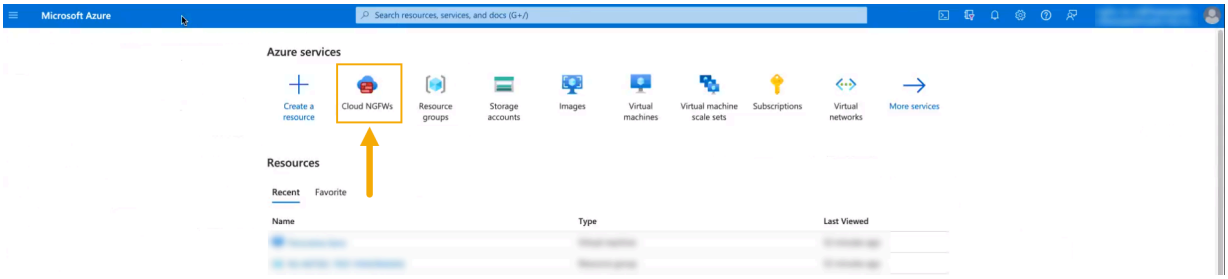


STEP 3 | Wählen Sie **Copy Registration String** aus.

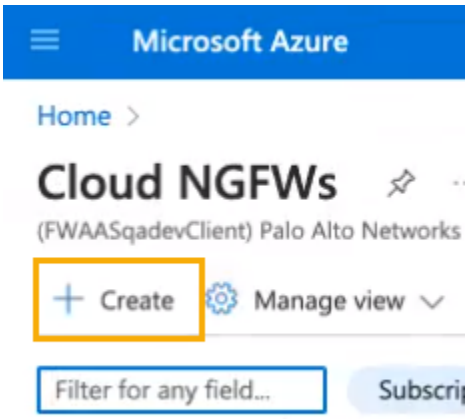


Greifen Sie nach dem Kopieren der Registrierungszeichenfolge auf Azure Marketplace zu, um eine Cloud NGFW-Ressource zu erstellen.

STEP 4 | Wählen Sie im Azure Marketplace **Cloud NGFWs** aus.

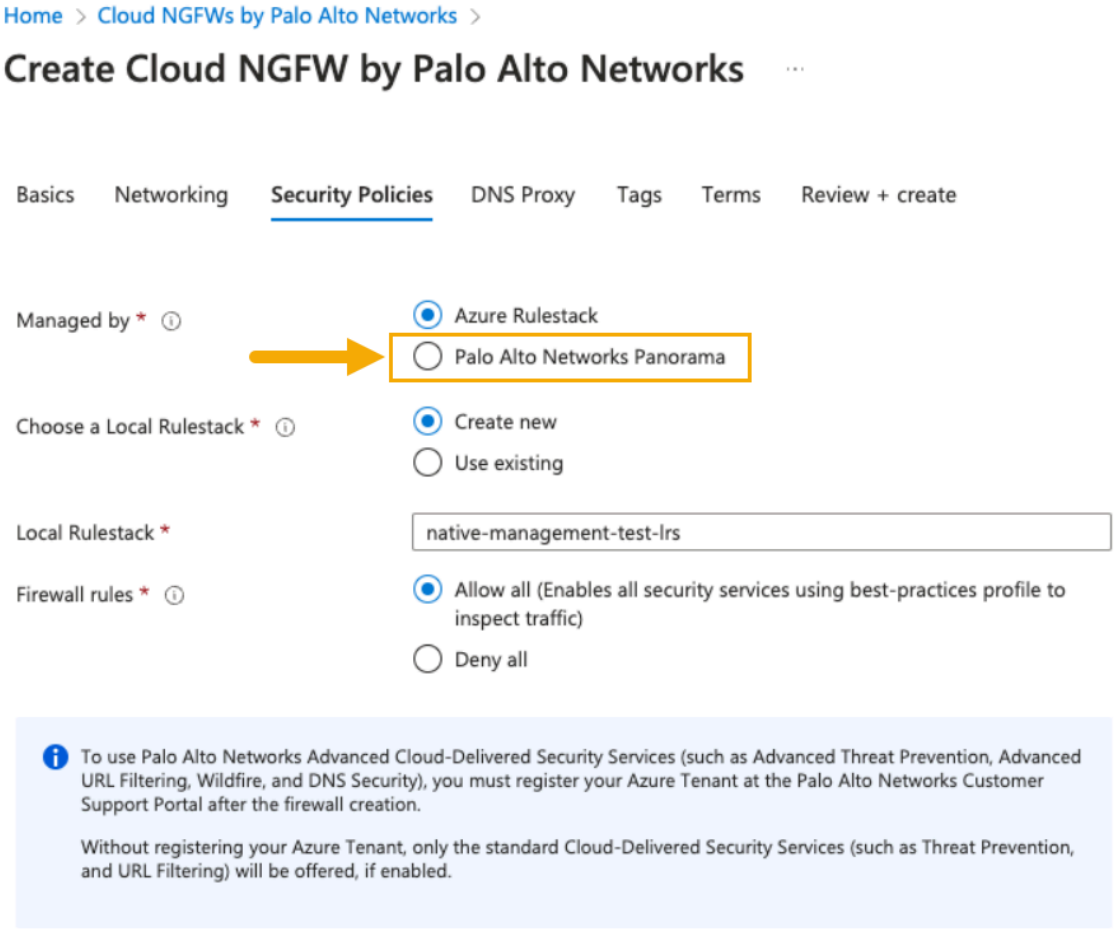


STEP 5 | Klicken Sie auf **+ Create**, um eine neue Cloud NGFW-Ressource zu erstellen.

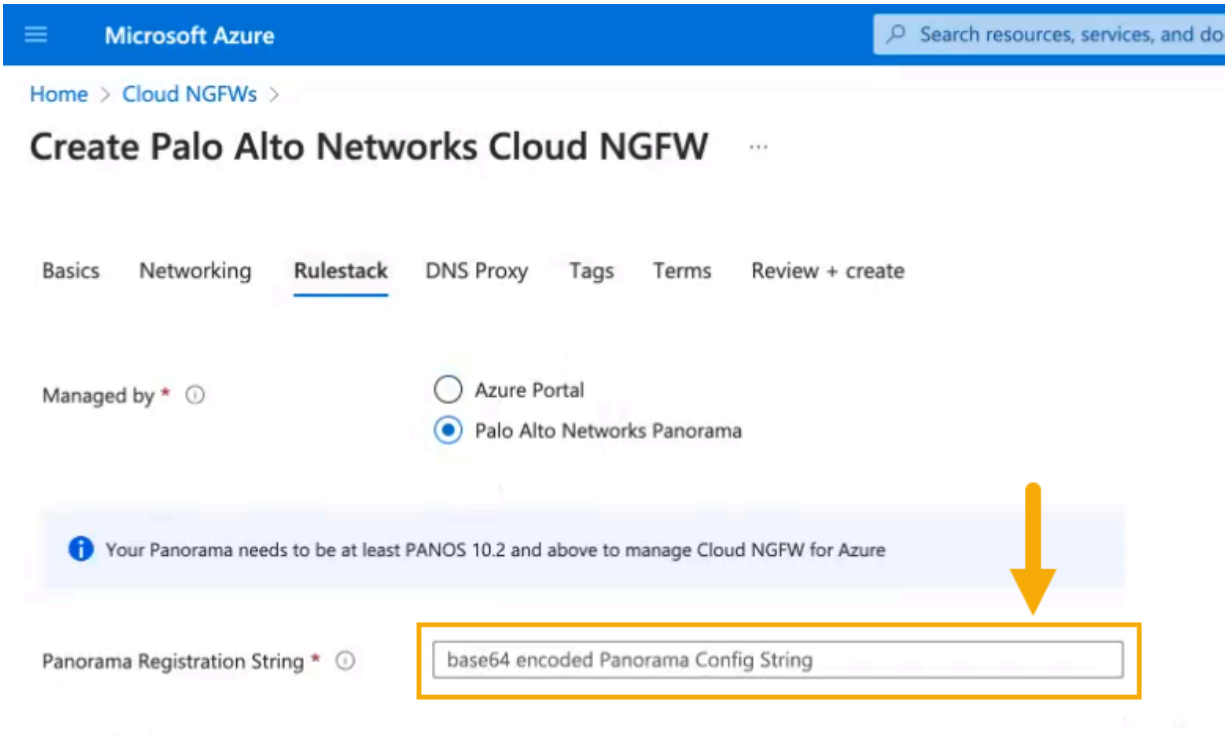


STEP 6 | Folgen Sie den Installationsanweisungen zum **Erstellen von Palo Alto Networks Cloud NGFW**.

1. Konfigurieren Sie grundlegende Informationen.
2. Konfigurieren Sie das Netzwerk.
3. Konfigurieren Sie die Sicherheitsrichtlinien. Wählen Sie im Abschnitt **Managed by Palo Alto Networks Panorama**.



STEP 7 | Nachdem Sie **Managed by Palo Alto Networks Panorama** ausgewählt haben, wird auf der Seite für die Sicherheitsrichtlinien das Feld **Panorama Registration String** hinzugefügt. Geben Sie die Registrierungszeichenfolge ein, die Sie in Schritt 3 kopiert haben.



STEP 8 | Setzen Sie die Erstellung der Cloud NGFW-Ressource fort, indem Sie Informationen für DNS-Proxy, Tags und Bedingungen angeben. Überprüfen Sie Ihre Konfiguration und klicken Sie dann auf **Create**.

Das Erstellen einer Cloud NGFW-Ressource kann etwa 10–15 Minuten dauern.

Die Panorama-Konsole ist nun mit der Cloud NGFW-Ressource verknüpft.

Panorama für die Richtlinienverwaltung in Cloud NGFW verwenden

Hinzufügen einer Cloud-Gerätegruppe

Nachdem Sie Ihre Cloud NGFW-Ressource mit der virtuellen Panorama-Appliance verknüpft haben, können Sie die Integration für Richtlinienverwaltungsaufgaben verwenden, wie das Hinzufügen von Gerätegruppen und das Anwenden von Richtlinienregeln auf die Gerätegruppe.

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.

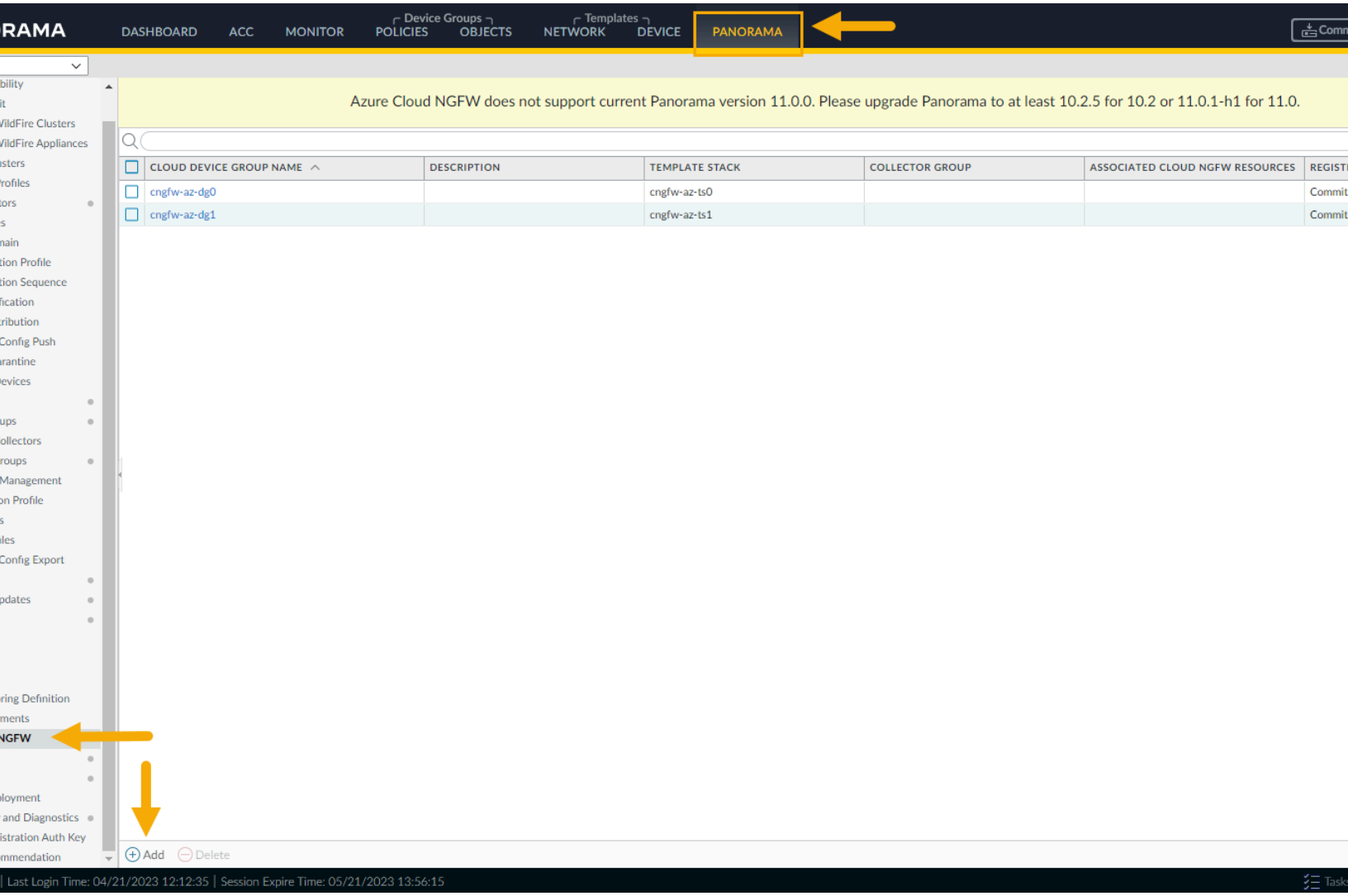
Mithilfe von Gerätegruppen können Sie Richtlinienregeln und die von ihnen referenzierten Objekte konfigurieren. Organisieren Sie Gerätegruppen hierarchisch mit gemeinsamen Regeln und Objekten an der Spitze und gerätegruppenspezifische Regeln und Objekte auf nachfolgenden Ebenen. So können Sie eine Hierarchie 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:

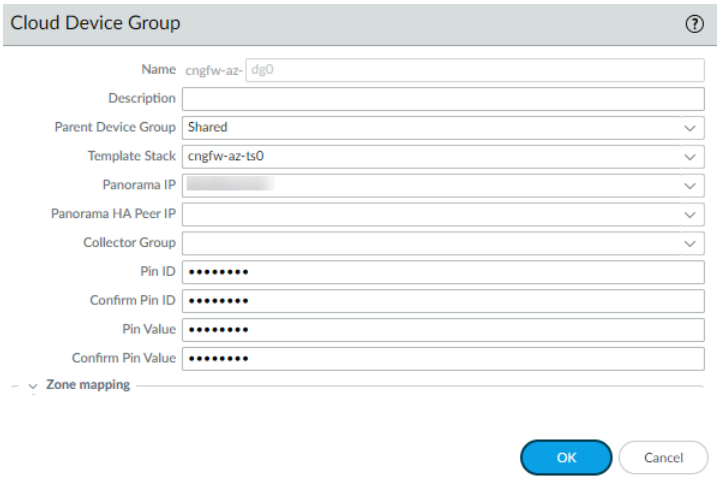
STEP 1 | Wählen Sie im **Azure**-Plug-in **Cloud NGFW** aus.

Wenn Sie die Tabelle „Cloud Device Group“ (Cloud-Gerätegruppe) zum ersten Mal auswählen, ist sie leer. Zuvor erstellte Cloud-Gerätegruppen werden angezeigt, wenn sie für die Cloud NGFW-Ressource mit Azure eingerichtet wurden.

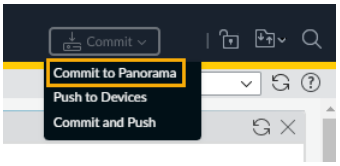


STEP 2 | Klicken Sie unten links auf **Add**.

STEP 3 | Im Bildschirm **Cloud Device Group**:



1. Geben Sie einen eindeutigen **Namen** für die Cloud-Gerätegruppe ein.
2. Geben Sie eine **Beschreibung** ein.
3. Wählen Sie im Drop-down-Menü die **Übergeordnete Gerätegruppe** aus. Standardmäßig wird dieser Wert freigegeben.
4. Wählen Sie im Drop-down-Menü den Vorlagenstapel aus. Oder klicken Sie auf **Add**, um einen neuen zu erstellen.
5. Wählen Sie die von der Bereitstellung verwendete **Panorama IP**-Adresse aus. Im Drop-down-Menü können Sie entweder die *private* oder *öffentliche* IP-Adresse auswählen.
6. Wählen Sie optional die Panorama HA **Peer IP**-Adresse aus.
7. Verwenden Sie optional das Drop-down-Menü, um die Kollektorgruppe auszuwählen.
8. Konfigurieren Sie optional die Zonenzuordnung für die Cloud-Gerätegruppe. Es werden nur zwei Zonen unterstützt: *öffentlich oder privat*.
9. Klicken Sie auf **OK**.
10. Übernehmen Sie Ihre Änderung in der Panorama-Konsole, um die Cloud-Gerätegruppe zu erstellen. Generieren Sie als Nächstes die Registrierungszeichenfolge, um die Cloud NGFW-Ressource zu erstellen und in Azure bereitzustellen.



Löschen einer Cloud-Gerätegruppe

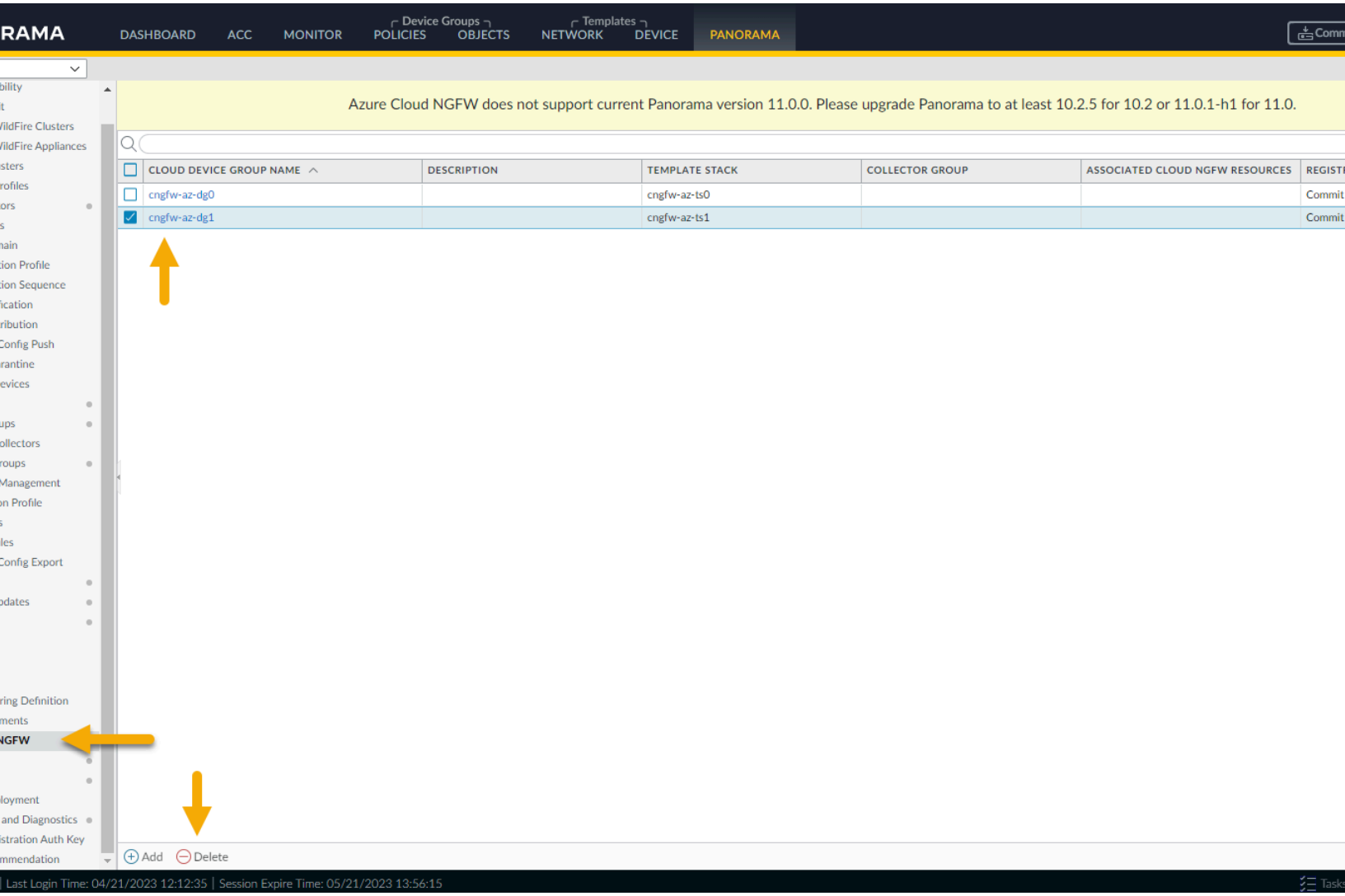
Verwenden Sie die Panorama-Konsole, um eine Cloud-Gerätegruppe zu löschen. Sie können eine Cloud-Gerätegruppe nur löschen, wenn ihr keine Firewalls zugeordnet sind.

So löschen Sie eine Cloud-Gerätegruppe aus einer Ressource 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**.



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

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

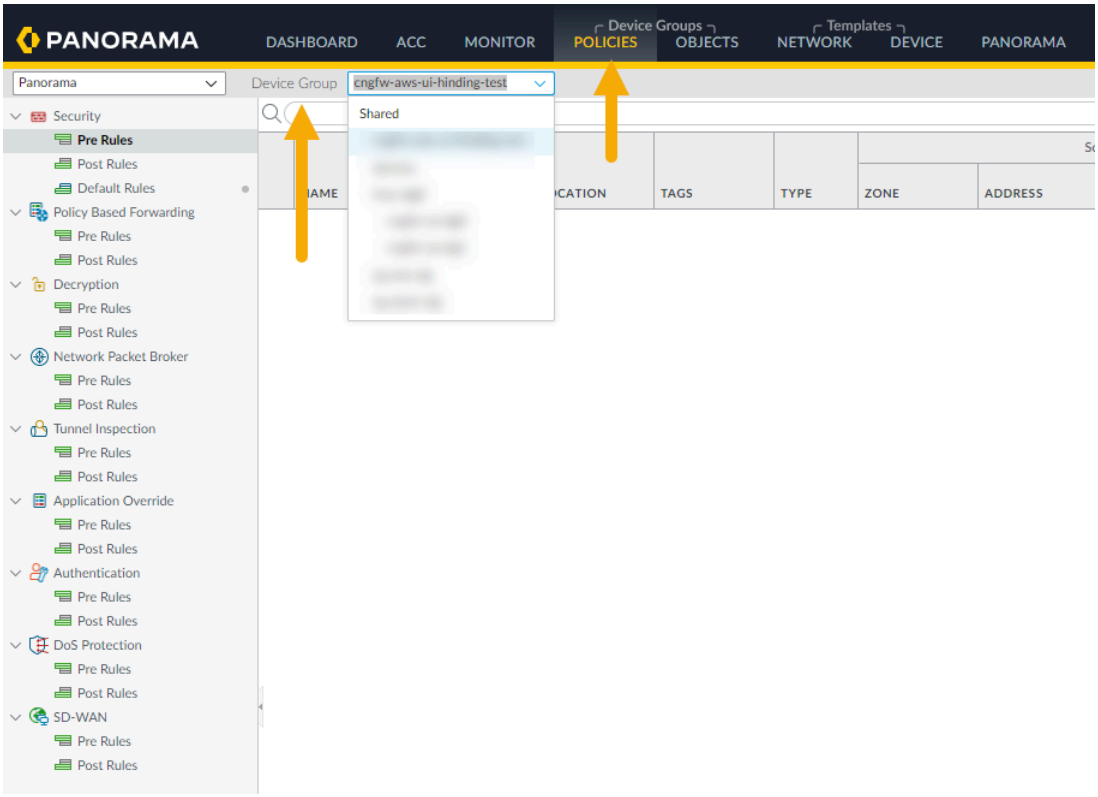
Anwenden der Richtlinie

Cloud-Gerätegruppen auf Panorama ermöglichen Ihnen die zentrale Verwaltung von Firewall-Richtlinienregeln. Sie erstellen Richtlinienregeln auf Panorama entweder als Vor- oder Nachregel. Mit diesen Regeln können Sie einen mehrschichtigen Ansatz für die Umsetzung von Richtlinien erstellen. Weitere Informationen finden Sie unter Definieren von Richtlinien auf Panorama.

So konfigurieren Sie Richtlinienregeln für die Cloud-Gerätegruppe in Panorama:

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

STEP 2 | Wählen Sie im Abschnitt **Device Group** über das Drop-down-Menü die zuvor erstellte **Cloud-Gerätegruppe** aus.

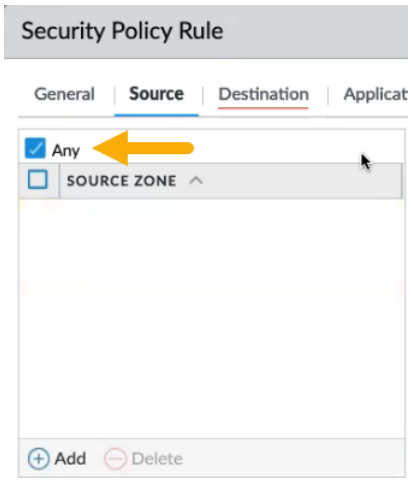


Wenn Sie eine Gerätegruppe für Cloud NGFW erstellen, beginnt der Name mit *cngfw*. Zum Beispiel *cngfw-azure-demo*

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

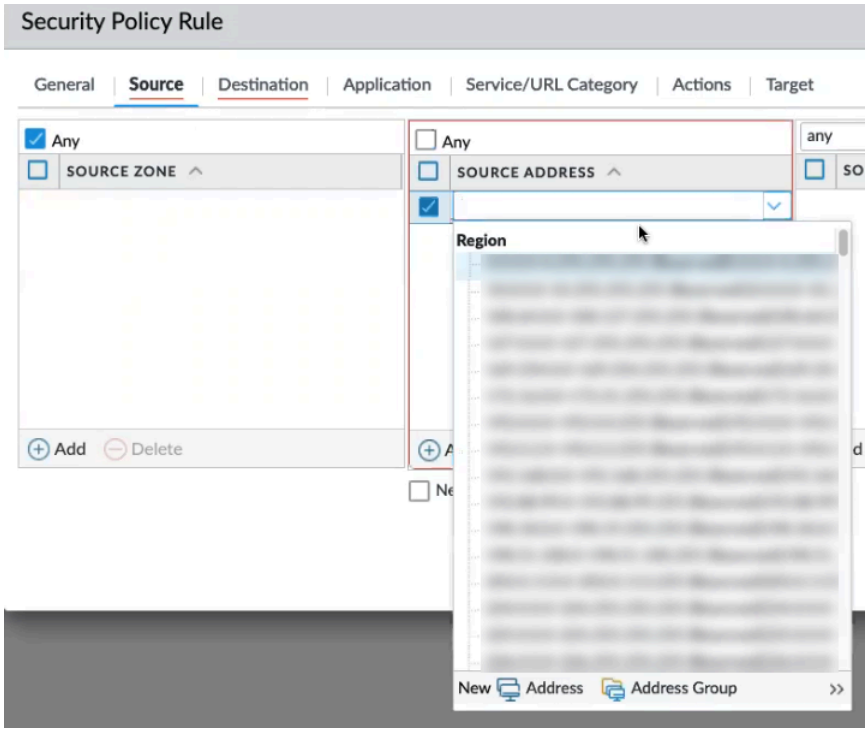
STEP 4 | Konfigurieren Sie im Bildschirm Security Policy Rule die Elemente der Richtlinie, die Sie auf die Gerätegruppe anwenden möchten.

1. Geben Sie auf der Registerkarte **General** einen Namen für die Richtlinie ein. Geben Sie optional zusätzliche Informationen an.
2. Die **Quellrichtlinie** definiert die Quellzone oder Quelladresse, von der der Datenverkehr ausgeht. Klicken Sie für **Source Zone** auf **Any**. Sie können keine spezifische Quellzone hinzufügen.



Fahren Sie mit der Anwendung der **Quellrichtlinien** fort, indem Sie die **Quelladresse** einschließen. Klicken Sie auf **Any** oder verwenden Sie das Drop-down-Menü, um eine

vorhandene Adresse auszuwählen, oder verwenden Sie die entsprechenden Optionen, um eine neue Adresse oder Adressgruppe hinzuzufügen.



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.

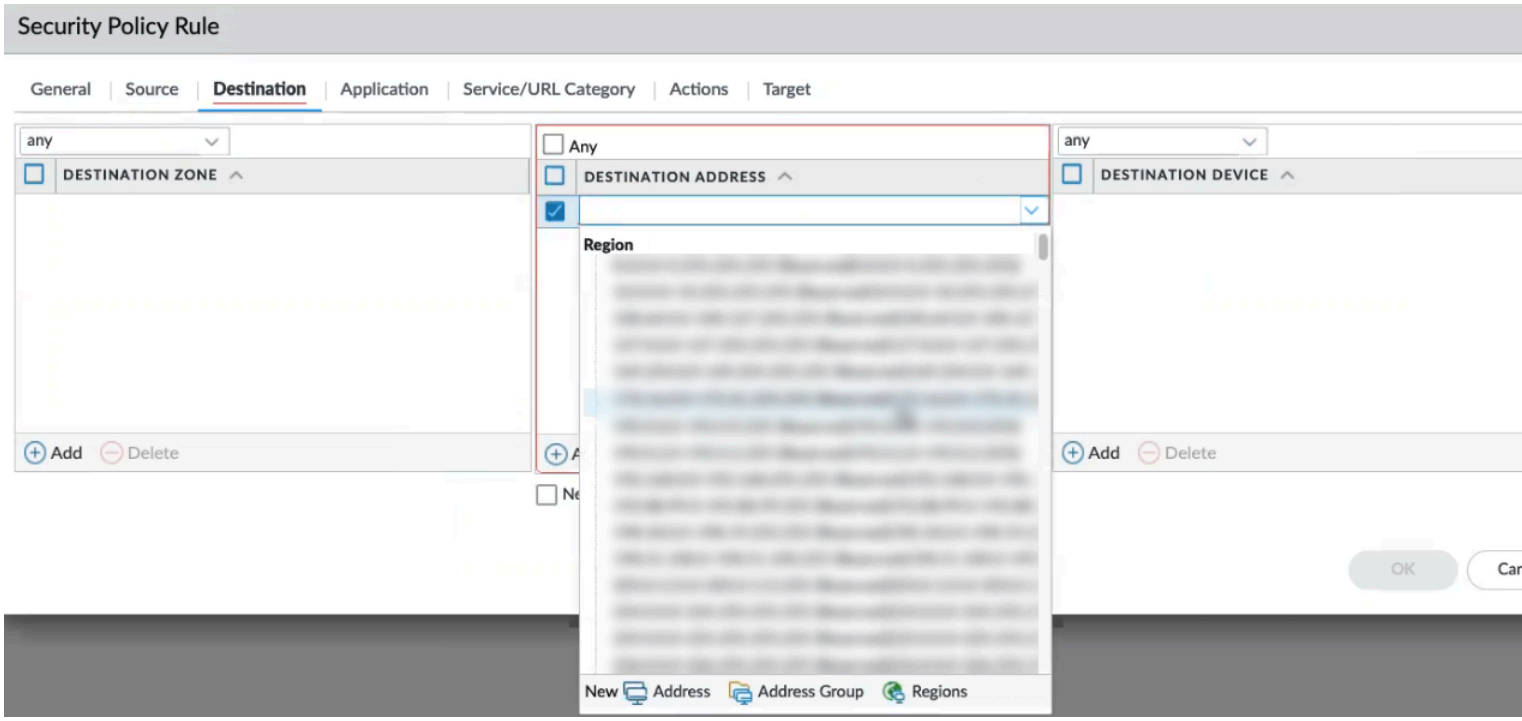
3. Die **Zielrichtlinie** definiert die Zielzone oder Zieladresse für den Datenverkehr. Verwenden Sie das Drop-down-Menü, um eine vorhandene Adresse auszuwählen, oder verwenden Sie die

Optionen, um eine neue Adresse oder Adressgruppe hinzuzufügen. Die Zielrichtlinie umfasst Felder für Zone, Adresse und Gerät.

Klicken Sie für **Destination Zone (Zielzone)** auf **Any (Beliebig)**. Cloud NGFW unterstützt das Hinzufügen einzelner Zielzonen nicht.

Klicken Sie für **Destination Address** auf **Any** oder verwenden Sie das Drop-down-Menü, um eine vorhandene Zone auszuwählen. Klicken Sie auf **New**, um eine neue Adresse, Adressgruppe oder Region hinzuzufügen.

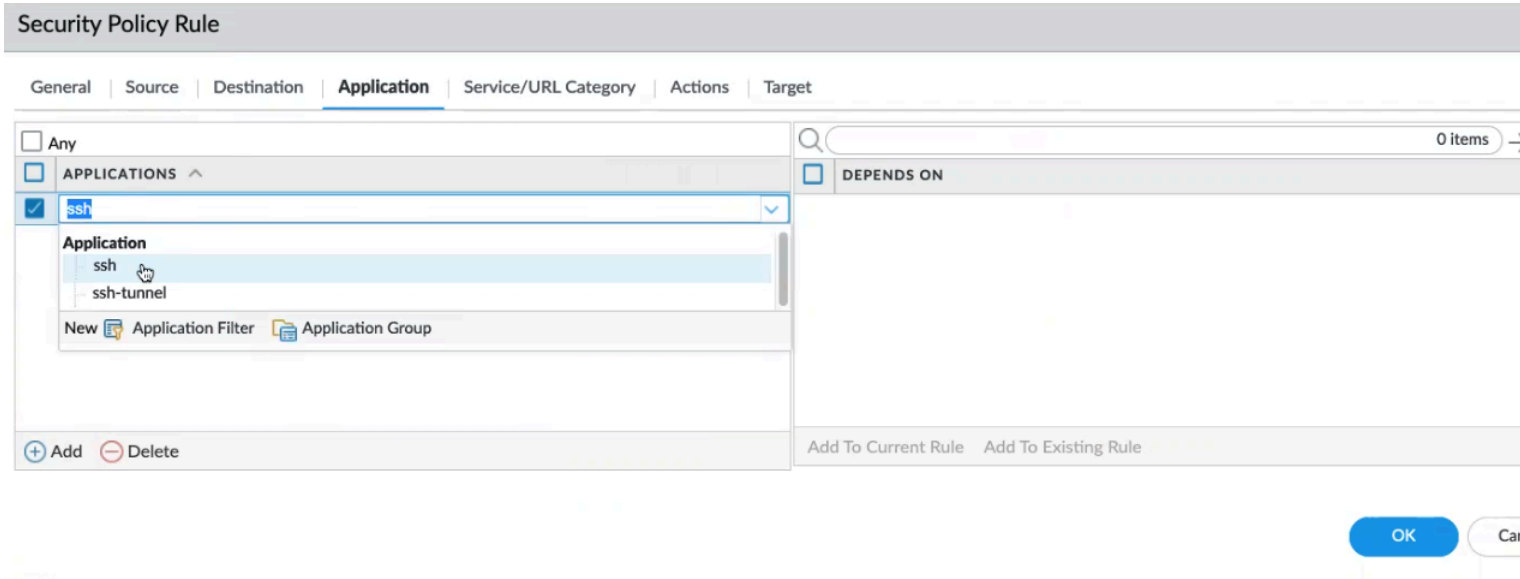
Klicken Sie für **Destination Device** auf **Any**. Cloud NGFW unterstützt das Hinzufügen einzelner Zielgeräte nicht.



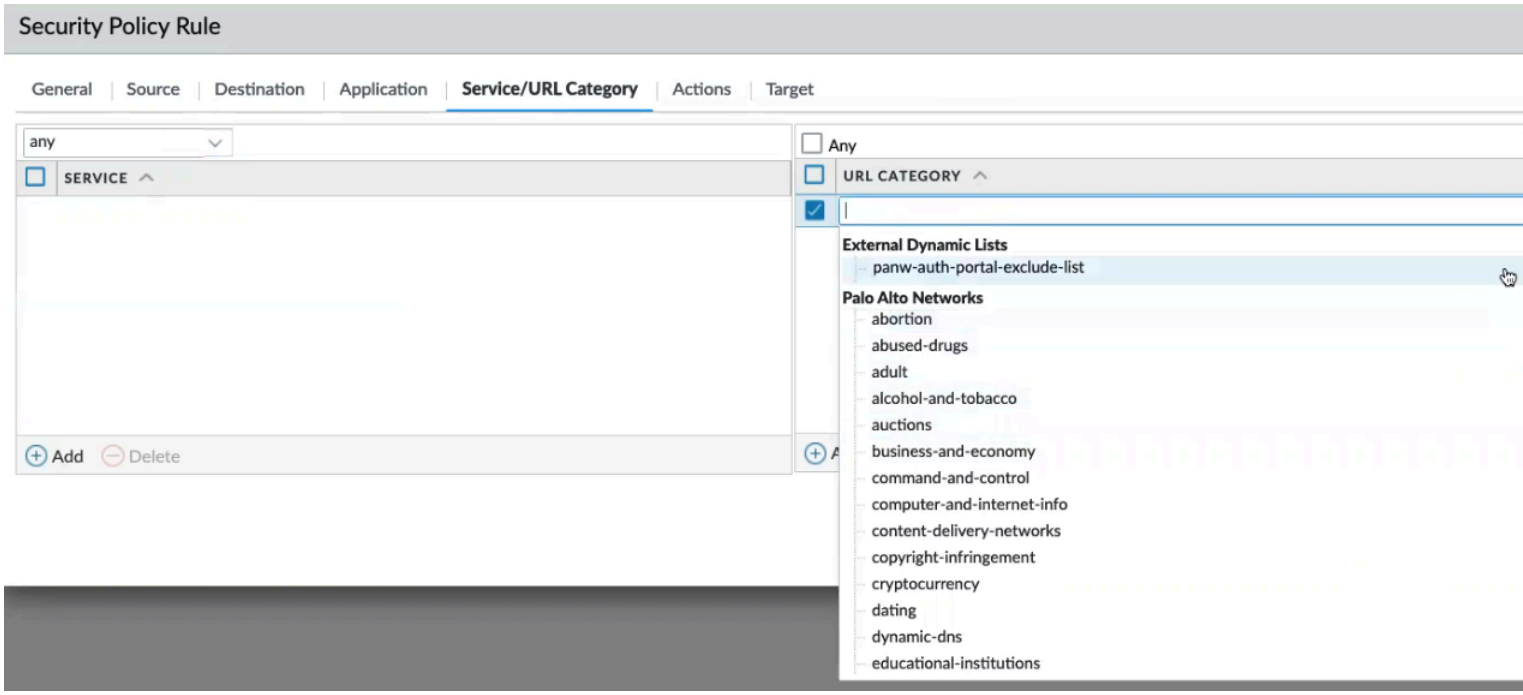
4. Konfigurieren Sie eine Richtlinie vom Typ **Application** so, dass die Richtlinienaktion basierend auf einer Anwendung oder Anwendungsgruppe ausgeführt wird. Ein Administrator kann auch eine vorhandene App-ID-Signatur verwenden und sie anpassen, um proprietäre Anwendungen

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

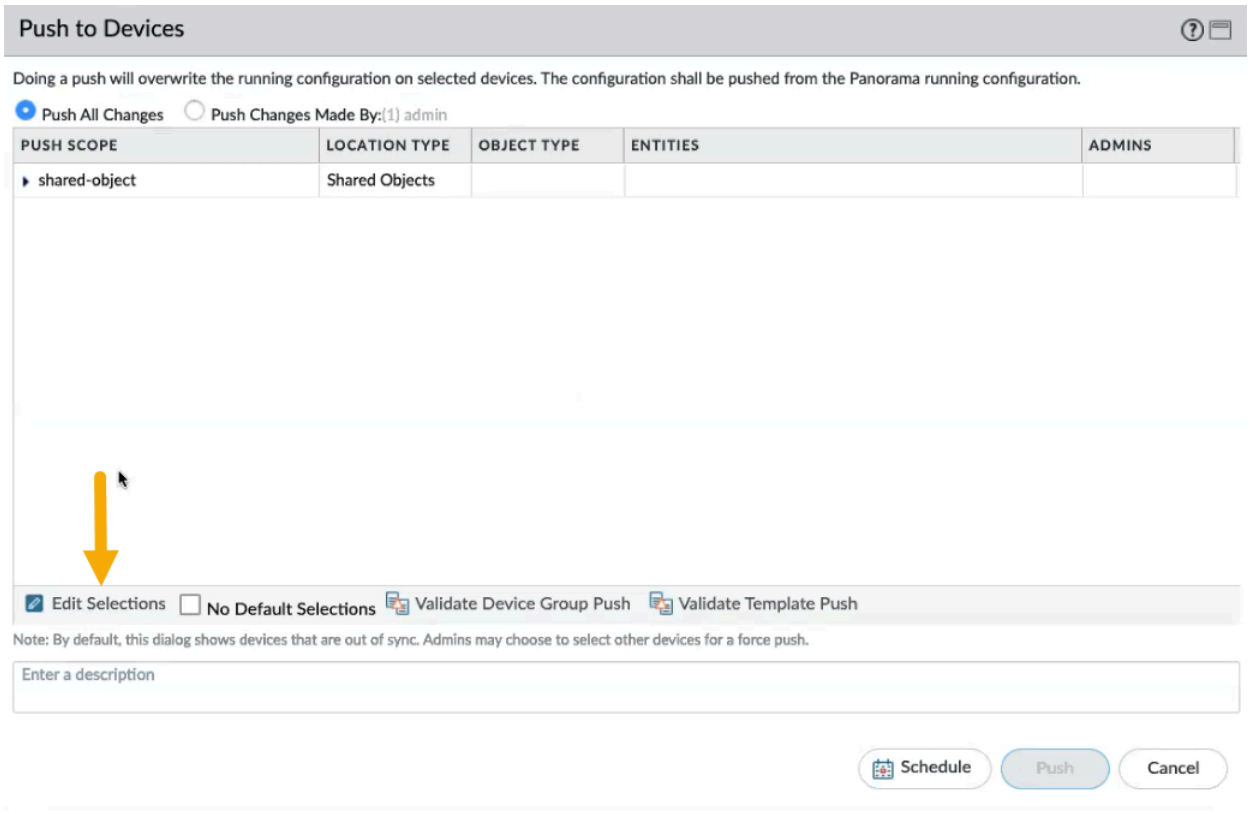
Klicken Sie im Bildschirm **Application** auf „Any“ oder geben Sie eine bestimmte Anwendung an, beispielsweise SSH. Klicken Sie auf **Add**, um eine neue Anwendungsrichtlinie einzuschließen.



5. Konfigurieren Sie unter **Service/URL Category** Dienst-/URL-Kategorie-Richtlinien für die Firewall, um eine bestimmte TCP- oder UDP-Portnummer oder eine URL-Kategorie als Übereinstimmungskriterium in der Richtlinie anzugeben. Geben Sie Richtlinienregeln auf **Dienstebene** oder **URL-Kategorie**-Richtlinienregeln an, indem Sie **Any** auswählen, oder verwenden Sie die Drop-down-Optionen, um die Richtlinienelemente, die Sie anwenden möchten, einzeln auszuwählen. Klicken Sie auf **Add**, um neue Richtlinienregeln für den Dienst oder die URL/Kategorie zu erstellen.



STEP 5 | Nachdem Sie Richtlinienregeln auf die Cloud-Gerätegruppe für die Cloud NGFW-Ressource angewendet haben, übertragen Sie die Änderungen per Push in die Panorama-Konsole. Klicken Sie im Bildschirm **Push to Devices (Per Push auf Geräte übertragen)** auf **Edit Selections (Auswahl bearbeiten)**.



STEP 6 | 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)**.

Benutzer-ID in der Cloud NGFW für Azure aktivieren

Die Benutzeridentität ist im Gegensatz zu einer IP-Adresse ein integraler Bestandteil einer effektiven Sicherheitsinfrastruktur. Wenn Sie wissen, wer welche Anwendungen in Ihrem Netzwerk verwendet und wer möglicherweise eine Bedrohung übermittelt oder Dateien überträgt, können Sie Ihre Sicherheitsrichtlinien stärken und die Reaktionszeit bei Vorfällen verkürzen. User-ID™, eine Standardfunktion der Firewall von Palo Alto Networks, ermöglicht Ihnen die Nutzung von Benutzerinformationen, die in einer Vielzahl von Repositories gespeichert sind. Weitere Informationen zu Benutzer-ID-Konzepten finden Sie in der PAN-OS-Dokumentation.

So erzwingen Sie Richtlinien anhand von Benutzer-IDs oder Gruppen:

- Die Firewall muss in der Lage sein, die IP-Adressen den Benutzernamen zuzuordnen.
- Die Benutzeridentifikation bietet verschiedene Mechanismen zum Sammeln der Benutzerzuordnungsinformationen. Um mehr zu erfahren, klicken Sie hier.
- Wenn die Zuordnungsmethoden die Zuordnung nicht erfassen können, können Sie die Authentifizierungsrichtlinie so konfigurieren, dass Benutzer zu einer Anmeldung beim Authentifizierungsportal umgeleitet werden. Benutzer können Anmeldeinformationen angeben, die mit dem Identitätsanbieter abgeglichen werden, und den Zugriff entsprechend erzwingen. Erfahren Sie hier mehr über die Authentifizierungsrichtlinie.

Cloud NGFW unterstützt die Serverüberwachungszuordnung aktuell nur über die Agenteninstallation.

So aktivieren Sie die benutzer- und gruppenbasierte Richtlinie:

- Die Firewall benötigt eine Liste aller verfügbaren Benutzer und ihrer entsprechenden Gruppenmitgliedschaften.
- Panorama sammelt Gruppenzuordnungsinformationen, indem eine direkte Verbindung mit dem LDAP-Server hergestellt und diese dann an die Cloud NGFW verteilt wird.

Für die Cloud NGFW-Bereitstellung empfehlen wir die Verwendung der Serverüberwachung mit dem Terminalserver-Agenten von Palo Alto Networks oder einem auf Windows basierten Agenten, der auf einem Domänenserver im Netzwerk ausgeführt wird.

STEP 1 | Die Benutzer-ID aktivieren.

1. Melden Sie sich bei Panorama an.
2. Wählen Sie **Network** > **Zones** aus und klicken Sie auf die Zone **Name**.
3. **Enable User Identification** und klicken Sie auf **OK**.

STEP 2 | Erstellen Sie ein dediziertes Dienstkonto für den Benutzer-ID-Agent.

STEP 3 | Ordnen Sie Benutzern Gruppen zu.

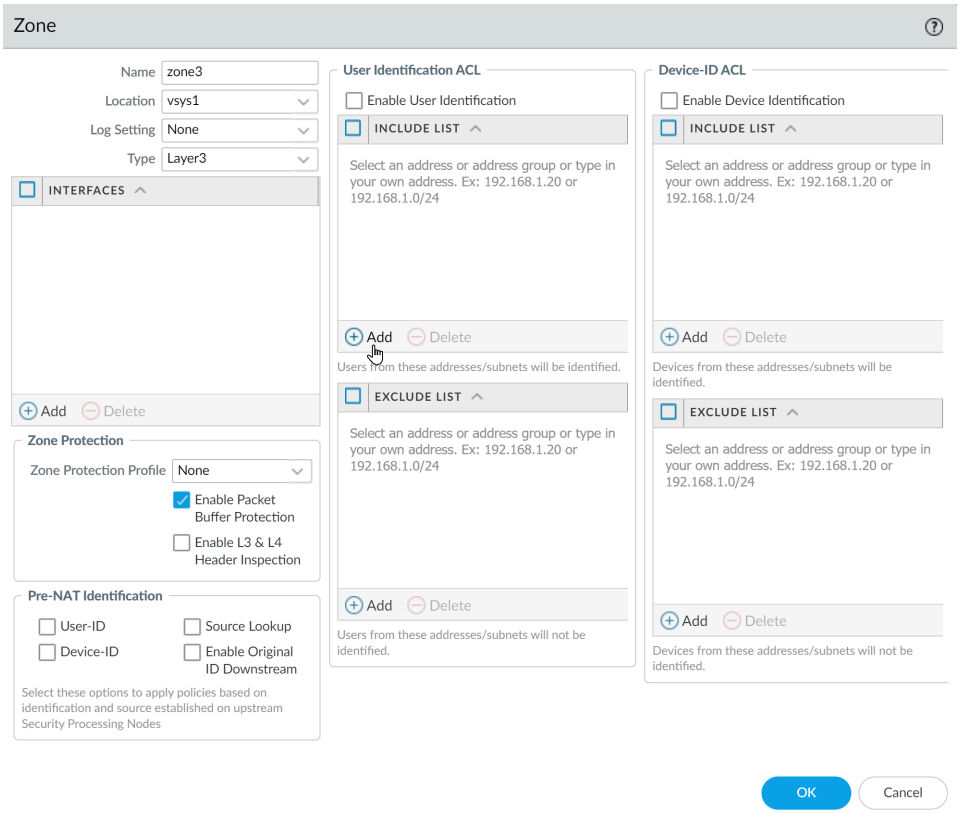
STEP 4 | Konfigurieren Sie die IP-Adresszuordnung von Benutzern. Die Cloud NGFW für Azure unterstützt die IP-zu-Benutzer-Zuordnung mithilfe des Windows Benutzer-ID-Agenten oder des Terminalserver-Agenten.

- Konfigurieren von Benutzerzuordnungen mit dem Windows Benutzer-ID-Agenten
- Konfigurieren von Benutzerzuordnungen für Terminalserver-Benutzer

STEP 5 | Geben Sie die Netzwerke an, die in die Benutzerzuordnung einbezogen bzw. davon ausgeschlossen werden sollen.

Geben Sie als bewährte Methode immer an, welche Netzwerke in die Benutzer-ID einbezogen und welche davon ausgeschlossen werden sollen. Dadurch können Sie sicherstellen, dass nur Ihre vertrauenswürdigen Assets geprüft und nicht unerwartet unerwünschte Benutzerzuordnungen erstellt werden.

1. Wählen Sie **Network** > **Zones** und die Zone aus, in der Sie die Benutzer-ID konfigurieren.
2. Fügen Sie Ihre Netzwerke nach Bedarf zu **Include**- und **Exclude**-Listen hinzu.
3. Klicken Sie auf **OK**.



STEP 6 | Aktivieren Sie die benutzer- und gruppenbasierte Richtliniendurchsetzung.

Nachdem Sie die Benutzer-ID auf Ihrer Cloud NGFW aktiviert haben, können Sie einen Benutzernamen oder Gruppennamen als Quelle oder Ziel einer Sicherheitsrichtlinienregel verwenden.

1. Wählen Sie **Policies** > **Security** aus und klicken Sie auf **Add**, um eine neue Sicherheitsrichtlinienregel zu erstellen. Oder klicken Sie auf den Namen einer Sicherheitsrichtlinie, um eine vorhandene Regel zu ändern.
2. Wählen Sie „User“ aus und geben Sie auf eine der folgenden Arten an, welche Benutzer und Gruppen mit der Regel übereinstimmen sollen.
   - Wenn Sie bestimmte Benutzer oder Gruppen als Übereinstimmungskriterien auswählen möchten, klicken Sie im Abschnitt „Source User“ auf **Add**, um eine Liste der von der Gruppenzuordnungsfunktion der Firewall erkannten Benutzer und Gruppen anzuzeigen. Wählen Sie die Benutzer oder Gruppen aus, die der Regel hinzugefügt werden sollen.

- Wenn Sie alle Benutzer abgleichen möchten, die sich authentifiziert haben bzw. die sich nicht authentifiziert haben, und Sie den spezifischen Benutzer- oder Gruppennamen nicht wissen müssen, wählen Sie aus der Drop-down-Liste über der Liste „Source User“ **known-user** oder **unknown** aus.

3. Konfigurieren Sie den Rest der Regel nach Bedarf und klicken Sie dann auf **OK**, um sie zu speichern. Einzelheiten zu anderen Feldern in der Sicherheitsregel finden Sie unter Einrichten einer grundlegenden Sicherheitsrichtlinie.

Erstellen Sie nach Möglichkeit gruppenbasierte statt benutzerbasierte Regeln. Dadurch wird verhindert, dass Sie Ihre Regeln ständig aktualisieren müssen (was ein Commit erfordert), wenn sich Ihre Benutzerbasis ändert.

STEP 7 | Erstellen Sie die Sicherheitsrichtlinienregeln, um die Benutzer-ID innerhalb Ihrer vertrauenswürdigen Zonen sicher zu aktivieren und zu verhindern, dass Benutzer-ID-Datenverkehr Ihr Netzwerk verlässt.

Befolgen Sie die Best Practice Internet Gateway-Sicherheitsrichtlinie, um sicherzustellen, dass die Benutzer-ID-Anwendung (`paloalto-userid-agent`) nur in den Zonen zulässig ist, in denen Ihre Agenten (sowohl Ihre Windows-Agenten als auch Ihre in PAN-OS integrierten Agenten) Dienste überwachen und Zuordnungen an Firewalls verteilen. Im Besonderen:

- Erlauben Sie die Anwendung `paloalto-userid-agent` zwischen den Zonen, in denen sich Ihre Agenten befinden, und den Zonen, in denen sich die überwachten Server befinden (oder noch besser, zwischen den spezifischen Systemen, die den Agenten hosten, und den überwachten Servern).
- Erlauben Sie die Anwendung `paloalto-userid-agent` zwischen den Agenten und den Firewalls, die die Benutzerzuordnungen benötigen, und zwischen Firewalls, die Benutzerzuordnungen neu verteilen, und den Firewalls, an die sie die Informationen neu verteilen.

Verweigern Sie der `paloalto-userid-agent`-Anwendung den Zugriff auf alle externen Zonen, z. B. Ihre Internetzone.

*Als bewährte Methode aktivieren Sie immer die Option **Enable Config Sync** für eine HA-Konfiguration, um sicherzustellen, dass die Gruppenzuordnungen und Benutzerzuordnungen zwischen der aktiven und passiven Firewall synchronisiert werden.*

STEP 8 | Übernehmen Sie mit **Commit** die Änderungen.

Einschränkungen

- Bei einem großen Netzwerk können Sie die Ressourcennutzung optimieren, indem nicht alle Firewalls so konfiguriert werden, dass die Zuordnungsinformationsquellen direkt abgefragt werden, sondern einige Firewalls so konfiguriert werden, dass die Zuordnungsinformationen durch Umverteilung erfasst werden. Für Cloud NGFW in Azure wird die Funktionalität zur Umverteilung von Benutzerzuordnungsinformationen nicht unterstützt.
- Authentifizierungs- und Autorisierungsrichtlinie wird nicht unterstützt.
- Die PAN-OS-basierte Agentenmethode für die Benutzer-ID-Zuordnung wird nicht unterstützt.
- Die XML-API-Methode zur Benutzer-ID-Zuordnung wird nicht unterstützt.

Konfigurieren von Service-Routen für lokale Dienste

Sie können Cloud NGFW für Azure für den Zugriff auf lokale, gehostete Dienste wie DNS-Server, externe dynamische Listen, Log Collector, Syslog, dynamische Inhaltsupdates, LDAP, MFA usw. konfigurieren. Standardmäßig greift eine Cloud NGFW-Firewall über die Verwaltungsschnittstelle auf diese Arten von Diensten zu. In einigen Anwendungsfällen wird die Verwendung der Verwaltungsschnittstelle jedoch nicht empfohlen. Stattdessen empfiehlt Palo Alto Networks, dass Sie eine **Service-Route** auf der Firewall konfigurieren, um auf diese Dienste zuzugreifen. Wenn Sie eine Service-Route verwenden, verlassen Dienstpakete die Firewall über einen Datenport, den Sie dem jeweiligen Dienst zugewiesen haben. Im Gegenzug sendet der Dienst seine Antwort an die konfigurierte Quell-IP und die Quellschnittstelle.

Panorama und das Panorama-Plug-in für Azure 5.1.1 oder höher sind erforderlich, um eine Service-Route in Cloud NGFW für Azure zu konfigurieren.

In den folgenden Szenarien sollten Sie eine Service-Route verwenden.

- Dienste, die in Ihrem lokalen Netzwerk mit einer privaten IP-Adresse gehostet werden. Da die Cloud NGFW-Verwaltungsschnittstelle nicht mit Ihrem lokalen Netzwerk verbunden ist, kann sie nicht auf die private IP-Adresse des Diensts zugreifen.
- Auf Dienste kann über eine öffentliche IP-Adresse über das Internet zugegriffen werden, in einer Zulassungslistenkonfiguration ist jedoch eine statische Quell-IP erforderlich. Die Cloud NGFW-Verwaltungsschnittstelle verwendet eine Quell-IP-Adresse, die per Source-NAT in eine dynamische öffentliche IP-Adresse übersetzt wird, um auf das Internet zuzugreifen, was nicht mit einer Zulassungsliste funktioniert. Sie können die Service-Route so konfigurieren, dass sie über eine öffentliche Datenschnittstelle auf den lokalen Dienst zugreift. Die IP-Adresse der Datenverkehrsquelle wird per Source-NAT in die öffentliche IP-Adresse der Cloud NGFW übersetzt.

Standardmäßig enthält jede Cloud NGFW-Panorama-Vorlage drei Zonen: privat, öffentlich und loopback. Die loopback-Zone verwendet eine Schnittstelle (loopback.3), die für die Service-Route verwendet wird.

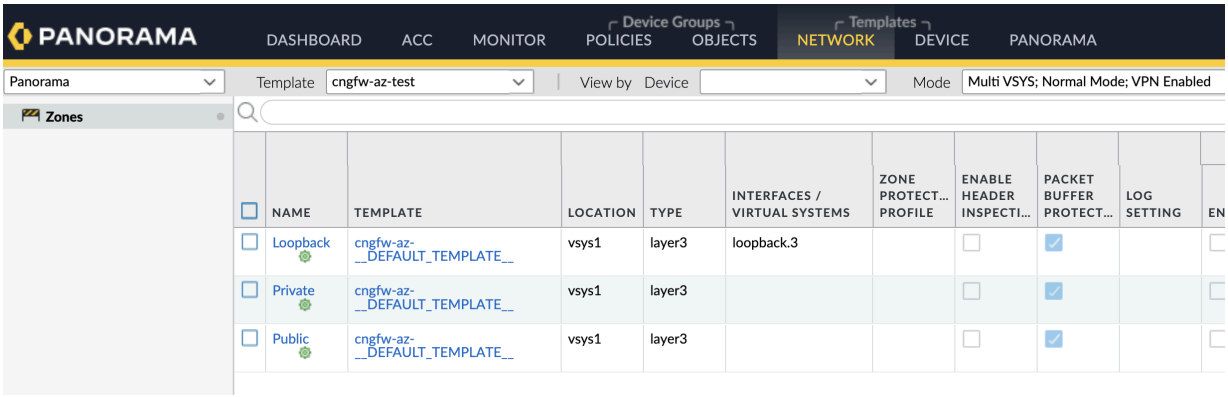
Führen Sie das folgende Verfahren aus, um eine Dienstroute in Cloud NGFW für Azure zu konfigurieren.

STEP 1 | Melden Sie sich bei Panorama an.

STEP 2 | Stellen Sie sicher, dass das Panorama-Plug-in für Azure 5.1.1 oder höher installiert ist.

STEP 3 | Navigieren Sie zu **Templates** > **Device** und wählen Sie Ihre Cloud NGFW-Vorlage aus dem Vorlage-Drop-down-Menü aus.

cngfw-az-_DEFAULT_TEMPLATE_ *ist erst sichtbar, nachdem der Vorlagenstapel im Panorama-Plug-in für Azure unter Cloud NGFW erstellt wurde.*



STEP 4 | Navigieren Sie zu **Setup** > **Services** und klicken Sie auf **Service Route Configuration**.

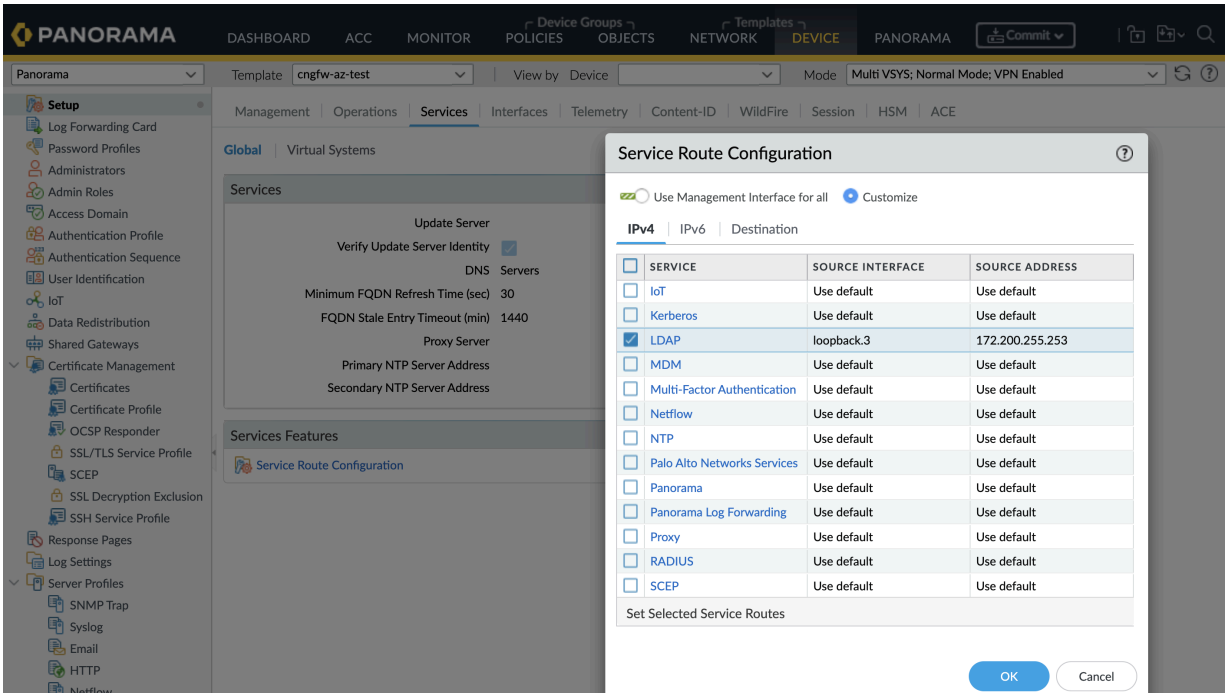
STEP 5 | Wählen Sie **Customize** aus und führen Sie eine der folgenden Aktionen aus, um eine Service-Route zu erstellen:

- Für einen vordefinierten Dienst:
  1. Wählen Sie **IPv4** oder **IPv6** aus und klicken Sie auf den Link für den Service, für den Sie die Service-Route anpassen möchten.

     *Wenn Sie dieselbe Quelladresse für mehrere Dienste verwenden möchten, aktivieren Sie das Kontrollkästchen für die Dienste, klicken Sie auf **Set Selected Routes** und fahren Sie mit dem nächsten Schritt fort.*
  2. Um die Liste für **Quelladresse** einzuschränken, wählen Sie loopback.3 als **Quellschnittstelle**. Wählen Sie dann eine **Quelladresse** (von dieser Schnittstelle) als Service-Route. Ein Adressobjekt kann auch als Quelladresse referenziert werden, wenn es bereits auf der ausgewählten Schnittstelle konfiguriert ist. Bei der Auswahl von **Any** als Quellschnittstelle werden alle IP-Adressen auf allen Schnittstellen in der Liste der Quelladressen zur Verfügung gestellt, aus der Sie eine Adresse auswählen. Nicht die Option **Use default** auswählen, denn dadurch wird die Firewall angewiesen, die Verwaltungsschnittstelle für die Service-Route zu verwenden.

     Die Quelladresse der Service-Route erbt keine Konfigurationsänderungen von der referenzierten Schnittstelle und umgekehrt. Durch die Änderung einer Schnittstellen-IP-Adresse in eine andere IP-Adresse oder ein anderes Adressobjekt wird eine entsprechende Service-Routen-Quelladresse nicht aktualisiert. Dies kann zu einem Commit-Fehler führen und erfordert, dass Sie die Service-Route(n) auf einen gültigen Quelladresswert aktualisieren.
  3. Klicken Sie auf **OK**, um die Konfiguration zu speichern.
  4. Wiederholen Sie diesen Schritt, wenn Sie sowohl eine **IPv4**- als auch eine **IPv6**-Adresse für einen Service angeben möchten.
- Wenn der Dienst nicht aufgeführt ist, wählen Sie die Registerkarte „Destination“ aus, um den Zieldienst nach IP-Adressen anzugeben:
  1. Wählen Sie **Destination** aus und **fügen** Sie eine **Ziel-IP**-Adresse hinzu. Wenn in diesem Fall ein Paket mit einer Ziel-IP-Adresse eintrifft, die mit der konfigurierten **Ziel-Adresse** übereinstimmt, wird die Quell-IP-Adresse des Pakets auf die im nächsten Schritt konfigurierte **Quelladresse** festgelegt.
  2. Um die Liste für die **Quelladresse** einzuschränken, wählen Sie die **loopback.3**-Schnittstelle und dann eine Quelladresse (von dieser Schnittstelle) als Service-Route aus. Bei der Auswahl von **Any** als Quellschnittstelle werden alle IP-Adressen auf allen Schnittstellen in der Liste der Quelladressen zur Verfügung gestellt, aus der Sie eine Adresse auswählen. Wenn Sie MGT auswählen, verwendet die Firewall die MGT-Schnittstelle für die Service-Route.

3. Klicken Sie auf **OK**, um die Konfiguration zu speichern.



STEP 6 | **Bestätigen** Sie die Änderungen.

STEP 7 | Mit einer Sicherheitsrichtlinienregel kann die Cloud NGFW den lokalen Dienst erreichen.

Die Sicherheitsrichtlinienregel kann mit dem Service-Routen-Datenverkehr wie folgt übereinstimmen:

- Von einer beliebigen Zone in die öffentliche Zone oder die private Zone, je nachdem, ob der Server über eine öffentliche oder private IP-Adresse verfügt.
- Quell-IP-Adresse (172.200.255.253) an Ziel-IP-Adresse (IP-Adresse des Dienstes).

XFF-IP-Adresswerte in der Richtlinie verwenden

Wenn Sie zwischen den Benutzern in Ihrem Netzwerk und Ihrer Cloud NGFW-Instanz ein Upstream-Gerät, beispielsweise einen Load Balancer, bereitgestellt haben, erkennt die Cloud NGFW im HTTP/HTTPS-Datenverkehr, den der Proxy weiterleitet, möglicherweise die IP-Adresse des Upstream-Geräts als Quell-IP-Adresse und nicht die IP-Adresse des Clients, der den Inhalt angefordert hat. In vielen Fällen fügt das Upstream-Gerät HTTP-Anfragen einen X-Forwarded-For-Header (XFF-Header) hinzu, der die tatsächliche IPv4- oder IPv6-Adresse des Clients enthält, der den Inhalt angefordert hat oder von dem die Anfrage stammt.

In Microsoft Azure fügt ein Anwendungsgateway standardmäßig die ursprüngliche Quell-IP-Adresse und den Port in den XFF-Header ein. Um XFF-Header in der Richtlinie Ihrer Firewall zu verwenden, müssen Sie das Anwendungsgateway so konfigurieren, dass der Port aus dem XFF-Header weggelassen wird. Informationen zum Konfigurieren des Anwendungsgateways finden Sie in der Azure-Dokumentation.

Diese Funktion wird nur auf Panorama-verwalteter Cloud NGFW für Azure unterstützt.

Wenn Sie Sicherheitsrichtlinienregeln auf Panorama konfigurieren, können Sie Cloud NGFW aktivieren, um die Quell-IP-Adresse in einem XFF-HTTP-Headerfeld zu verwenden, um die Sicherheitsrichtlinie durchzusetzen. Wenn ein Paket einen einzelnen Proxyserver passiert, bevor es die Firewall erreicht, enthält das XFF-Feld die IP-Adresse des ursprünglichen Endpunkts. Wenn das Paket jedoch mehrere Upstream-Geräte durchläuft, verwendet die Firewall die zuletzt hinzugefügte IP-Adresse, um die Richtlinie durchzusetzen oder andere Funktionen zu nutzen, die auf IP-Informationen basieren.

STEP 1 | Melden Sie sich bei Panorama an.

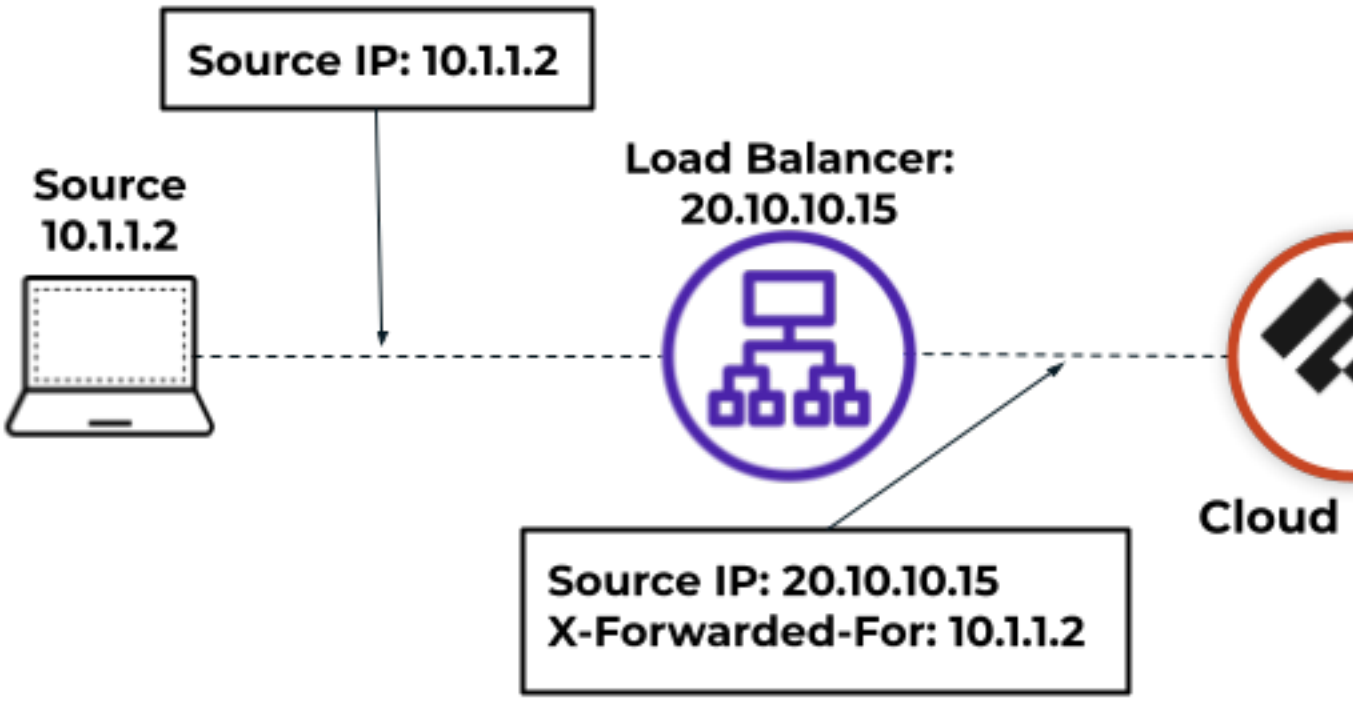
STEP 2 | Wählen Sie Ihre Cloud NGFW für die Azure-Cloud-Gerätegruppe aus.

STEP 3 | Wählen Sie **Device** > **Setup** > **Content ID** > **X-Forwarded-For Headers** aus.

STEP 4 | Klicken Sie auf das Bearbeitungssymbol.

STEP 5 | Wählen Sie **Enabled for Security Policy** aus dem Drop-down-Menü **Use X-Forwarded-For Header**.

*Die Option **Use X-Forwarded-For Header** kann nicht gleichzeitig für Sicherheitsrichtlinie und Benutzer-ID aktiviert werden.*



STEP 6 | Optional Wählen Sie **Strip X-Forwarded-For Header**, um das XFF-Feld aus ausgehenden HTTP-Anfragen zu entfernen.

Durch Auswahl dieser Option wird die Verwendung von XFF-Headern in der Richtlinie nicht deaktiviert. Die Cloud NGFW für Azure entfernt das XFF-Feld aus Clientanforderungen, nachdem es zur Durchsetzung der Richtlinie verwendet wurde.

STEP 7 | Klicken Sie auf **OK**.

STEP 8 | Übernehmen Sie mit **Commit** die Änderungen.

Anzeigen von Cloud NGFW-Protokollen und -Aktivitäten in Panorama

Anzeigen von Cloud NGFW-Protokollen in Panorama

Wenn Ihre Cloud NGFW-Ressourcen in Panorama integriert sind, werden Protokolle und Aktivitäten erfasst und in Panorama auf den Registerkarten „Monitoring and Application Command Center (ACC)“ angezeigt. Panorama sammelt Protokolle, die von der Cloud NGFW generiert wurden, und zeigt sie auf der Registerkarte **Monitor (Überwachen)** an. Sie können aus den Datenverkehrs-, Bedrohungs-, URL-Filter- und Entschlüsselungsprotokollen auswählen und diese nach ID oder Name filtern. Beschreibungen der Protokollfelder finden Sie in der Dokumentation zur Protokollierung von Cloud NGFW.

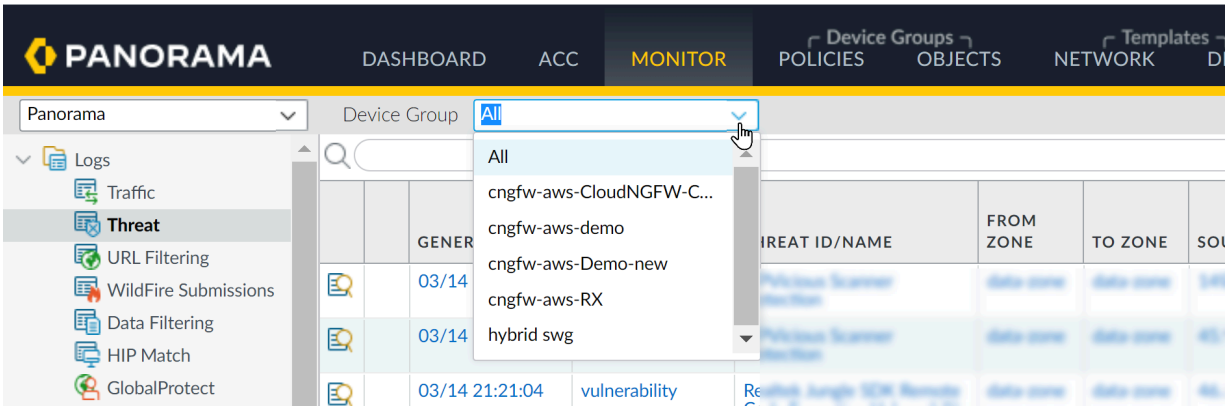
STEP 1 | Melden Sie sich bei Panorama an.

STEP 2 | Wählen Sie **Monitor** aus.

STEP 3 | Wählen Sie aus der Drop-down-Liste **Device Group** die **Cloud Device Group** aus, um die Aktivität anzuzeigen.

STEP 4 | Sie können einen Panorama-Filter verwenden, um das Protokoll einer einzelnen Cloud-Gerätegruppe anzuzeigen. Suchen Sie die Schaltfläche **Device Name**. Klicken Sie auf das Symbol + im oberen rechten Bereich der Panorama-Benutzeroberfläche, um einen neuen Filter hinzuzufügen. Geben Sie den Namen für den Filter ein und klicken Sie dann auf **Save**. Klicken Sie auf das Symbol **Load Filter**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

STEP 5 | Im Menü **Logs** auf der linken Seite der Panorama-Konsole können Sie einen bestimmten Protokolltyp auswählen, der angezeigt werden soll.



Anzeigen der Cloud NGFW-Aktivität im ACC

Das ACC ist ein Analysetool, das verwertbare Informationen über die Aktivitäten in Ihrem Netzwerk liefert. Das ACC verwendet die Cloud NGFW-Protokolle, um die Datenverkehrstrends in Ihrem Netzwerk grafisch darzustellen. Die grafische Darstellung ermöglicht es Ihnen, mit den Daten zu

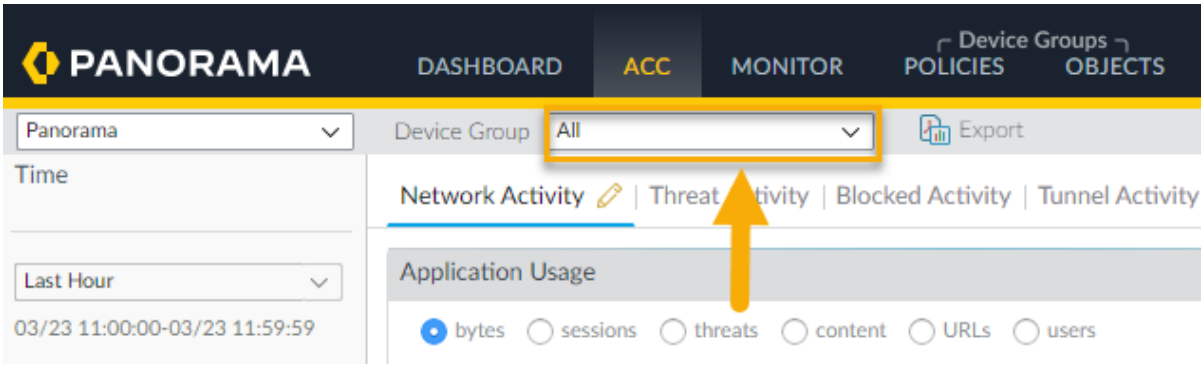
interagieren und die Beziehungen zwischen Ereignissen im Netzwerk zu visualisieren, einschließlich Netzwerknutzungsmustern, Datenverkehrsmustern sowie verdächtigen Aktivitäten und Anomalien.

In Panorama können Sie ACC-Inhalte basierend auf der Cloud-Gerätegruppe filtern. Weitere Informationen zum Filtern und Anzeigen bestimmter Informationen zu Aktivitäten in Ihren Cloud NGFW-Ressourcen finden Sie in der ACC-Dokumentation für PAN-OS.

STEP 1 | Melden Sie sich bei Panorama an.

STEP 2 | Wählen Sie **ACC** aus.

STEP 3 | Wählen Sie aus der Drop-down-Liste **Device Group** die **Cloud Device Group** aus, um die Aktivität anzuzeigen.



STEP 4 | Sie können einen Panorama-Filter verwenden, um das Protokoll einer einzelnen Cloud-Gerätegruppe anzuzeigen. Suchen Sie die Schaltfläche **Device Name**. Klicken Sie auf das Symbol **+** im oberen rechten Bereich der Panorama-Benutzeroberfläche, um einen neuen Filter hinzuzufügen. Geben Sie den Namen für den Filter ein und klicken Sie dann auf **Save**. Klicken Sie auf das Symbol **Load Filter**. Wählen Sie den neu erstellten Filter aus, um die Protokolle für die einzelnen Cloud-Gerätegruppen anzuzeigen.

Protokollierung

Die Cloud NGFW kann Datenverkehrs-, Bedrohungs- und Entschlüsselungsprotokolle an einen Azure Log Analytics Workspace senden, der im Azure-Portal erstellt wird.

Protokollierung in Cloud NGFW für Azure 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 Azure Log Analytics Workspace senden, der im Azure-Portal erstellt wird. Der Log Analytics Workspace ist mit einer Arbeitsbereichs-ID, einem Primärschlüssel und einem Sekundärschlüssel verknüpft, die von der Steuerebene über die Protokollierungs-API abgerufen werden.

Protokolltypen

Cloud NGFW kann drei Arten von Protokollen erfassen und speichern.

- **Datenverkehr**: Datenverkehrsprotokolle enthalten einen Eintrag für den Beginn und das Ende jeder Sitzung. Weitere Informationen finden Sie unter Datenverkehrsprotokollfelder in Cloud NGFW für Azure.
- **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 Azure.

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 auszunutzen sein, nicht zu erhöhten Rechten führen oder keinen großen Opferpool haben.

Severity (Schweregrad)	Beschreibung
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 Azure.

Datenverkehrsprotokollfelder in Cloud NGFW für Azure

Feldname	Beschreibung
Quelladresse (src_ip)	Ursprüngliche IP-Adresse der Sitzungsquelle.
Quellport (sport)	Quellport, der von der Sitzung verwendet wird.
Zieladresse (dst)	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_received)	Anzahl der Bytes in Server-zu-Client-Richtung der Sitzung.
Gesendete Bytes (bytes_sent)	Anzahl der Bytes in Client-zu-Server-Richtung der Sitzung.
Empfangene Pakete (pkts_received)	Anzahl der Server-zu-Client-Pakete für die Sitzung.
Gesendete Pakete (pkts_sent)	Anzahl der Client-zu-Server-Pakete für die Sitzung.
Startzeit (start)	Startzeit der Sitzung.
Verstrichene Zeit (elapsed)	Verstrichene Zeit der Sitzung.
Wiederholungsanzahl (repeatcnt)	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).

Feldname	Beschreibung
Quellland (srcloc)	Quellland oder interne Region für private Adressen. Die maximale Länge beträgt 32 Byte.
Zielland (dstloc)	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 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

Feldname	Beschreibung
	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)	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 Azure

Feldname	Beschreibung
Quelladresse (src_ip)	Ursprüngliche IP-Adresse der Sitzungsquelle.
Quellport (sport)	Quellport, der von der Sitzung verwendet wird.
Zieladresse (dst)	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 • 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

Feldname	Beschreibung
	• 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 protokollieren) im WildFire-Übermittlungsprotokoll protokolliert wird. • wildfire-virus: Virus, der über ein Antivirus-Profil erkannt wurde.

Feldname	Beschreibung
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 Bedrohungs-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)	Die IP-Adresse des Benutzers, der die Webseite angefordert hat, oder die IP-Adresse des vorletzten Geräts, über das die Anforderung geleitet wurde. Wenn die Anforderung durch einen oder mehrere Proxys, Load Balancer oder andere Upstream-Geräte geleitet wird, zeigt die Firewall die IP-Adresse des neuesten Geräts an.
Inhaltsversion (contentver)	Anwendungs- und Bedrohungsversion auf Ihrer Firewall, als das Protokoll generiert wurde.

Entschlüsselungsprotokollfelder in Cloud NGFW für Azure

Feldname	Beschreibung
Quell-IP-Adresse (src_ip)	Ursprüngliche IP-Adresse der Sitzungsquelle.
Quellport (sport)	Quellport, der von der Sitzung verwendet wird.
Zieladresse (dst)	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
TLS-Version (tls_version)	Die Version des TLS-Protokolls, die für die Sitzung verwendet wird.
Schlüsselaustauschalgorithmus (tls_keyxchg)	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 (tls_auth)	Authentifizierungsalgorithmus, der für die Sitzung verwendet wird, z. B. SHA, SHA256, SHA384.
Elliptische Kurve (ec_curve)	Die elliptische Kryptografiekurve, die Client und Server aushandeln und für Verbindungen verwenden, die ECDHE-Verschlüsselungssammlungen nutzen.

Feldname	Beschreibung
Angabe des Servernamens (server_name_indication)	Die Angabe des Servernamens.
Länge von der Angabe des Servernamens (server_name_indication_length)	Die Länge von der Angabe des Servernamens (hostname).
Proxytyp (proxy_type)	Der Entschlüsselungsproxytyp, z. B. „Forward“ für Forward-Proxy, „Inbound“ für eingehende Prüfung, „No Decrypt“ für unverschlüsselten Datenverkehr, „GlobalProtect“.
Kettenstatus (chain_status)	Legt fest, ob der Kette vertraut wird. Werte sind: • Nicht geprüft • Nicht vertrauenswürdig • Vertrauenswürdig • Unvollständig

Protokolleinstellungen aktivieren

So aktivieren Sie die Protokolleinstellungen:

STEP 1 | Navigieren Sie auf der Startseite zur Cloud NGFW-Firewall, auf der Sie die Protokolleinstellungen aktivieren möchten.

STEP 2 | Klicken Sie auf **Log Settings**.

STEP 3 | Markieren Sie die Option **Enable Log Settings**.

STEP 4 | Wählen Sie in der Drop-down-Liste **Log Settings** den gewünschten Log Analytics Workspace aus, für den Sie die Protokolleinstellungen aktivieren möchten.

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

Protokolleinstellungen deaktivieren

Um die Protokolleinstellungen zu deaktivieren:

STEP 1 | Navigieren Sie auf der Startseite zur Cloud NGFW-Firewall, auf der Sie die Protokolleinstellungen aktivieren möchten.

STEP 2 | Klicken Sie auf **Log Settings**.

STEP 3 | Markieren Sie die Option **Disable Log Settings**.

STEP 4 | Wählen Sie in der Drop-down-Liste **Log Settings** den gewünschten Log Analytics Workspace aus, für den Sie die Protokolleinstellungen deaktivieren möchten.

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

Aktivitätsprotokollierung in Cloud NGFW für Azure aktivieren

Verfolgen Sie Administratoraktivitäten in Cloud NGFW für Azure, 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 Aktivitätsprotokoll 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.

Mehrere Protokollierungsziele in Cloud NGFW für Azure

Sie können Protokolle verwalten und Einblicke in die Cloud-Sicherheit Ihrer Cloud NGFW-Ressourcen gewinnen. Senden Sie Ihre von Cloud NGFW für Azure generierten Protokolle an einen Azure Log Analytics Workspace oder an Panorama an mehrere Ziele gleichzeitig. Diese Protokolle umfassen sowohl Datenverkehrs- als auch Bedrohungsprotokolle (URL-Filterung, WildFire-Übermittlungen, Dateiblockierung, Datenblockierung und Entschlüsselung)

Aktivieren des Datenverkehrsprotokolls in Log Analytics Workspace und Panorama

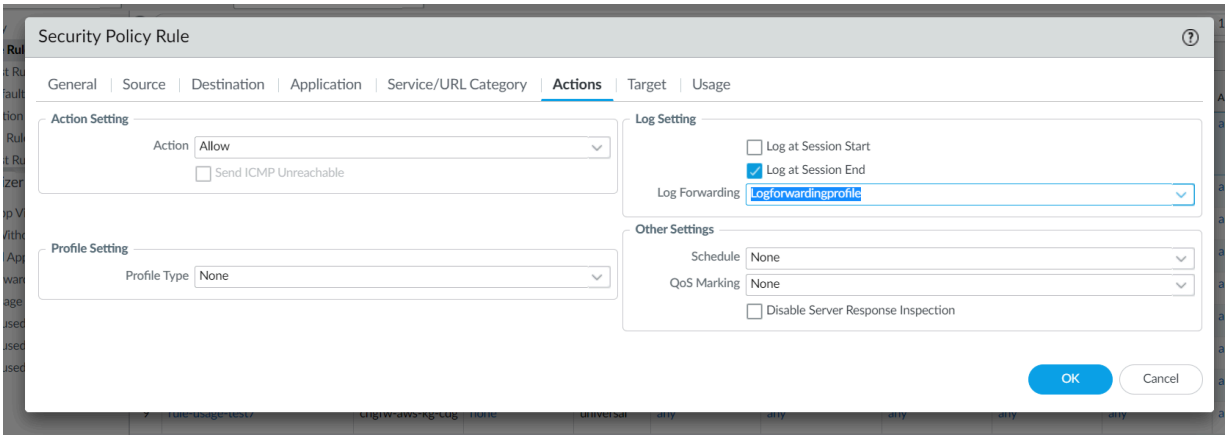
Im Folgenden finden Sie die Schritte zum Aktivieren des Datenverkehrsprotokolls im Log Analytics Workspace und in Panorama:

STEP 1 | Enable Log Settings in der Cloud NGFW für Azure-Konsole.

STEP 2 | Gehen Sie in Panorama zu **Policies**.

STEP 3 | Wählen Sie die Richtlinienregel für Ihre Cloud-Gerätegruppe aus.

STEP 4 | Gehen Sie zur Registerkarte **Actions** und wählen Sie dann das Profil **Log Forwarding** aus.



STEP 5 | Klicken Sie auf **OK**.

STEP 6 | **Legen Sie die Änderungen fest** und übertragen Sie sie an die Panorama-Konsole.

Nachdem der Datenverkehr gesendet wurde, können Sie die Cloud NGFW-Protokolle in Log Analytics Workspace und Panorama anzeigen**.** Weitere Informationen finden Sie unter View the Logs und View Cloud NGFW Logs in Panorama.

Aktivieren des Datenverkehrsprotokolls in Log Analytics Workspace und Deaktivieren in Panorama

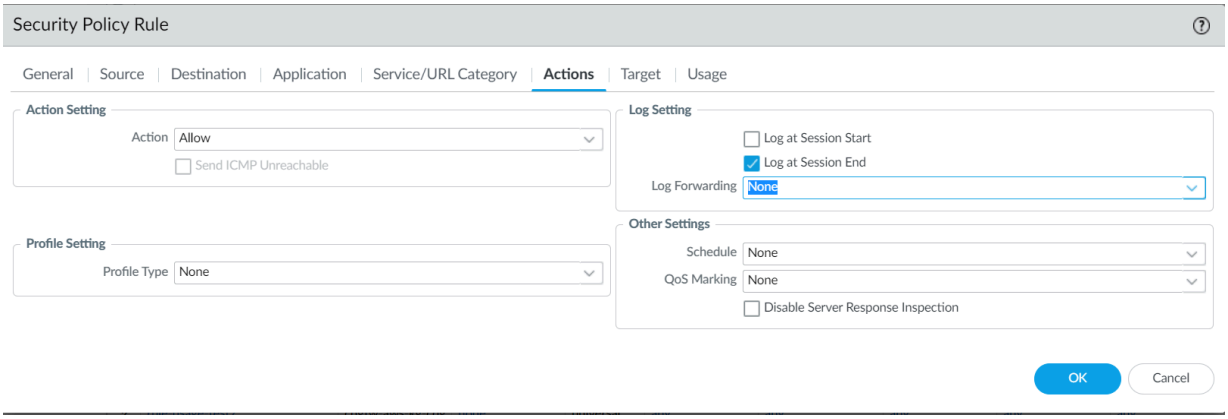
Im Folgenden finden Sie die Schritte zum Aktivieren des Datenverkehrsprotokolls im Log Analytics Workspace und zum Deaktivieren des Protokolls in Panorama:

STEP 1 | Enable Log Settings in der Cloud NGFW für Azure-Konsole.

STEP 2 | Gehen Sie in Panorama zu **Policies**.

STEP 3 | Wählen Sie die Richtlinienregel für Ihre Cloud-Gerätegruppe aus.

STEP 4 | Gehen Sie zur Registerkarte **Actions** und wählen Sie dann **None** im Profil „Log Forwarding“ aus.



STEP 5 | Klicken Sie auf **OK**.

STEP 6 | **Legen Sie die Änderungen fest** und übertragen Sie sie an die Panorama-Konsole.

Nachdem der Datenverkehr gesendet wurde, können Sie die Cloud NGFW-Protokolle in Log Analytics Workspace und Panorama anzeigen**.** Weitere Informationen finden Sie unter View the Logs und View Cloud NGFW Logs in Panorama.

Deaktivieren des Datenverkehrsprotokolls in Log Analytics Workspace und Aktivieren in Panorama

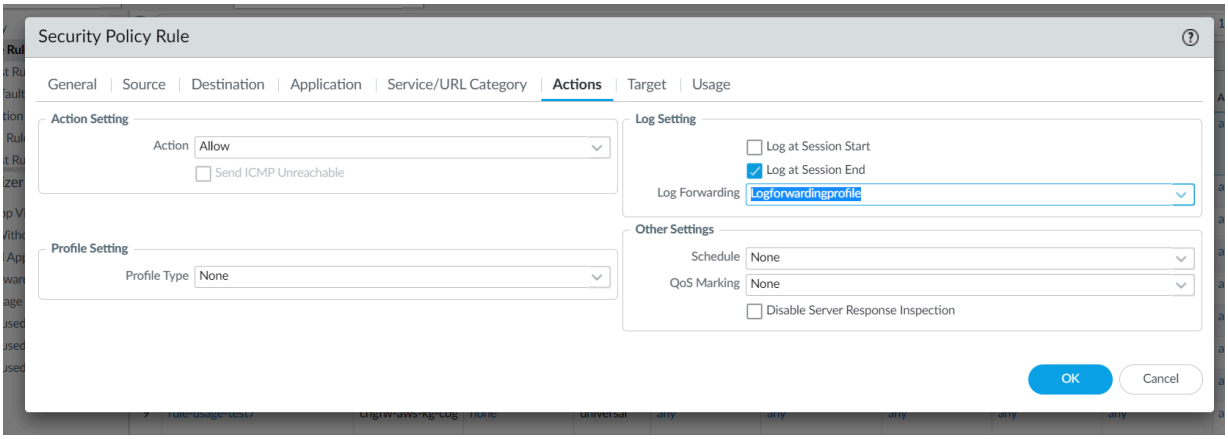
Im Folgenden finden Sie die Schritte zum Deaktivieren von Protokollen im Log Analytics Workspace und zum Aktivieren von Protokollen in Panorama:

STEP 1 | Disable Log Settings in der Cloud NGFW für Azure-Konsole.

STEP 2 | Gehen Sie in Panorama zu **Policies**.

STEP 3 | Wählen Sie die Richtlinienregel für Ihre Cloud-Gerätegruppe aus.

STEP 4 | Gehen Sie zur Registerkarte **Actions** und wählen Sie dann das Profil **Log Forwarding** aus.



STEP 5 | Klicken Sie auf **OK**.

STEP 6 | **Legen Sie die Änderungen fest** und übertragen Sie sie an die Panorama-Konsole.

Nachdem der Datenverkehr gesendet wurde, können Sie die Cloud NGFW-Protokolle in Log Analytics Workspace und Panorama anzeigen**.** Weitere Informationen finden Sie unter View the Logs und View Cloud NGFW Logs in Panorama.

Deaktivieren des Datenverkehrsprotokolls in Log Analytics Workspace und Panorama

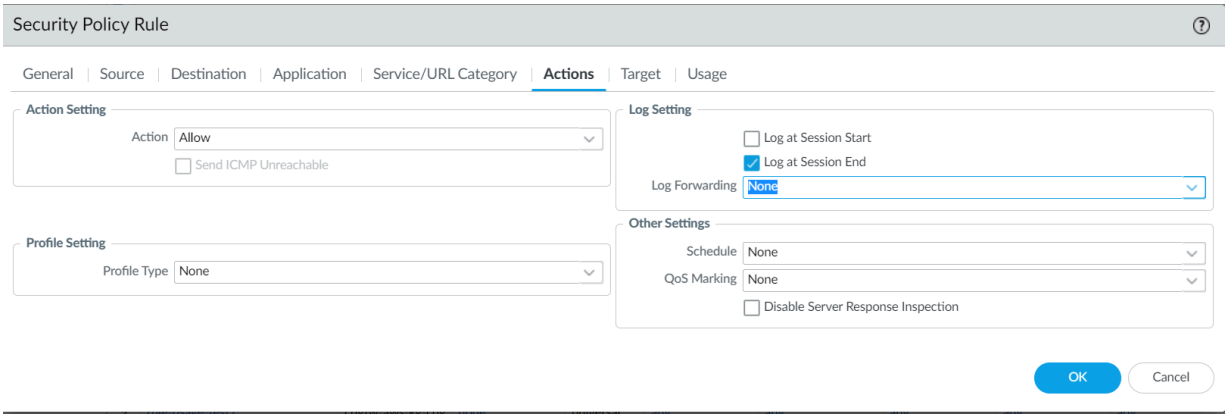
Im Folgenden finden Sie die Schritte zum Deaktivieren von Protokollen in Log Analytics Workspace und Panorama:

STEP 1 | Disable Log Settings in der Cloud NGFW für Azure-Konsole.

STEP 2 | Gehen Sie in Panorama zu **Policies**.

STEP 3 | Wählen Sie die Richtlinienregel für Ihre Cloud-Gerätegruppe aus.

STEP 4 | Gehen Sie zur Registerkarte **Actions** und wählen Sie dann **None** im Profil „Log Forwarding“ aus.



STEP 5 | Klicken Sie auf **OK**.

STEP 6 | **Legen Sie die Änderungen fest** und übertragen Sie sie an die Panorama-Konsole.

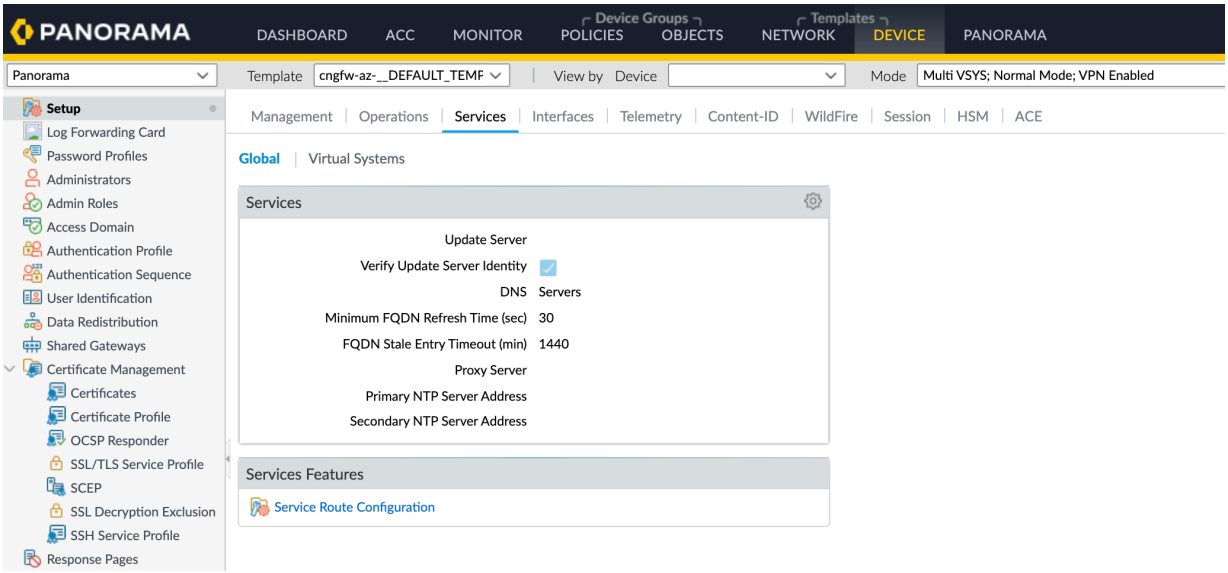
Die Cloud NGFW-Protokolle werden nicht mehr in Log Analytics Workspace und Panorama angezeigt.

Deaktivieren des Datenverkehrsprotokolls in Log Analytics Workspace und Aktivieren in Panorama und Syslog

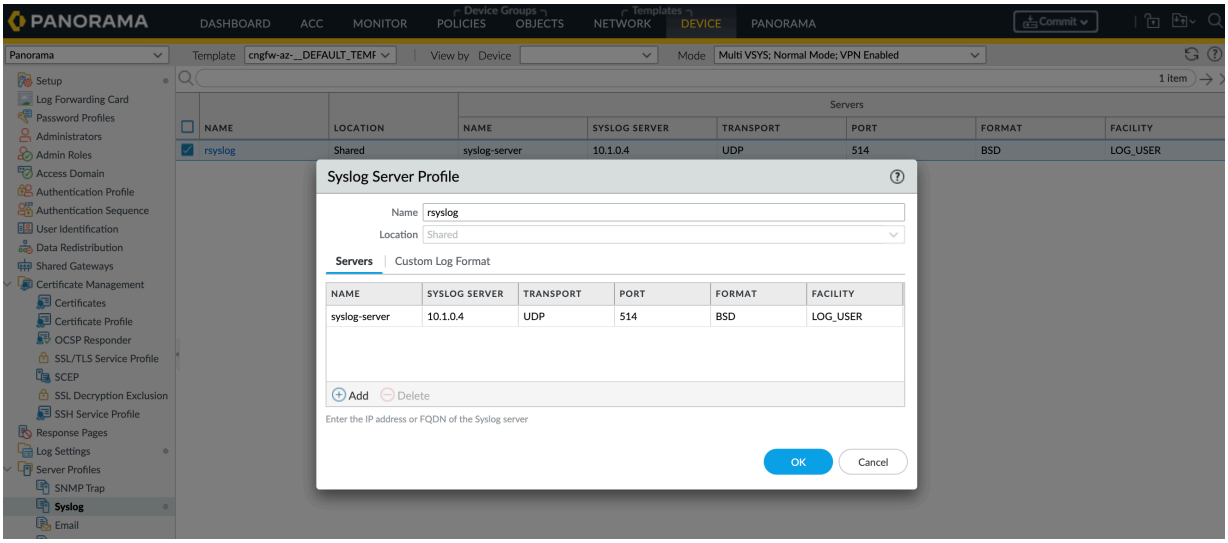
Im Folgenden finden Sie die Schritte zum Deaktivieren von Protokollen im Log Analytics Workspace und zum Aktivieren von Protokollen in Panorama und auf dem Syslog-Server:

STEP 1 | Disable Log Settings in der Cloud NGFW für Azure-Konsole.

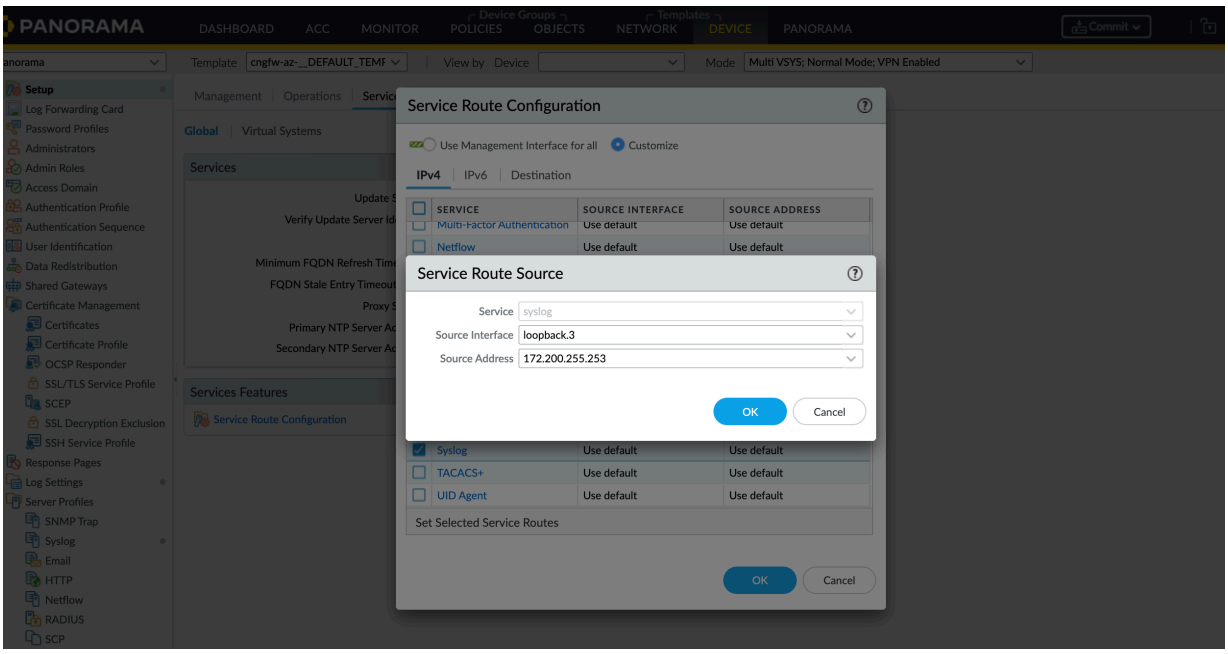
STEP 2 | Wechseln Sie in Panorama zur Registerkarte **Device** und wählen Sie dann die Azure NGFWAAS-Standardvorlage (`cngfw-az-__DEFAULT_TEMPLATE__`) aus.



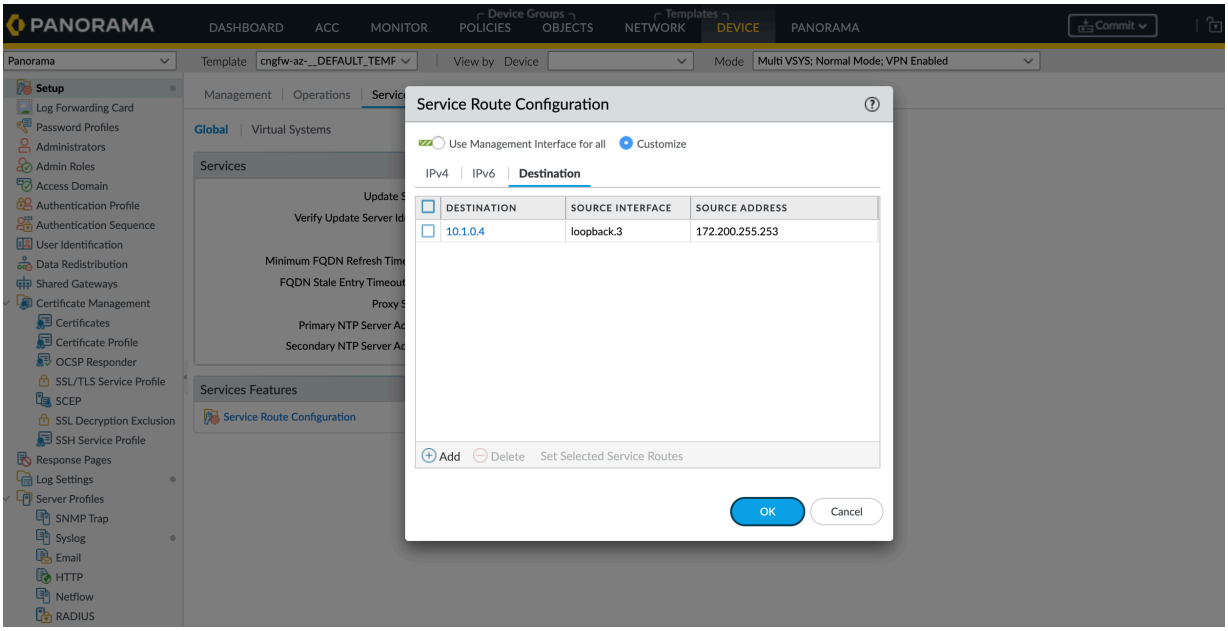
STEP 3 | Gehen Sie zu **Server profiles** -> **Syslog** und fügen Sie dann die private IP-Adresse Ihres Syslog-Servers hinzu.



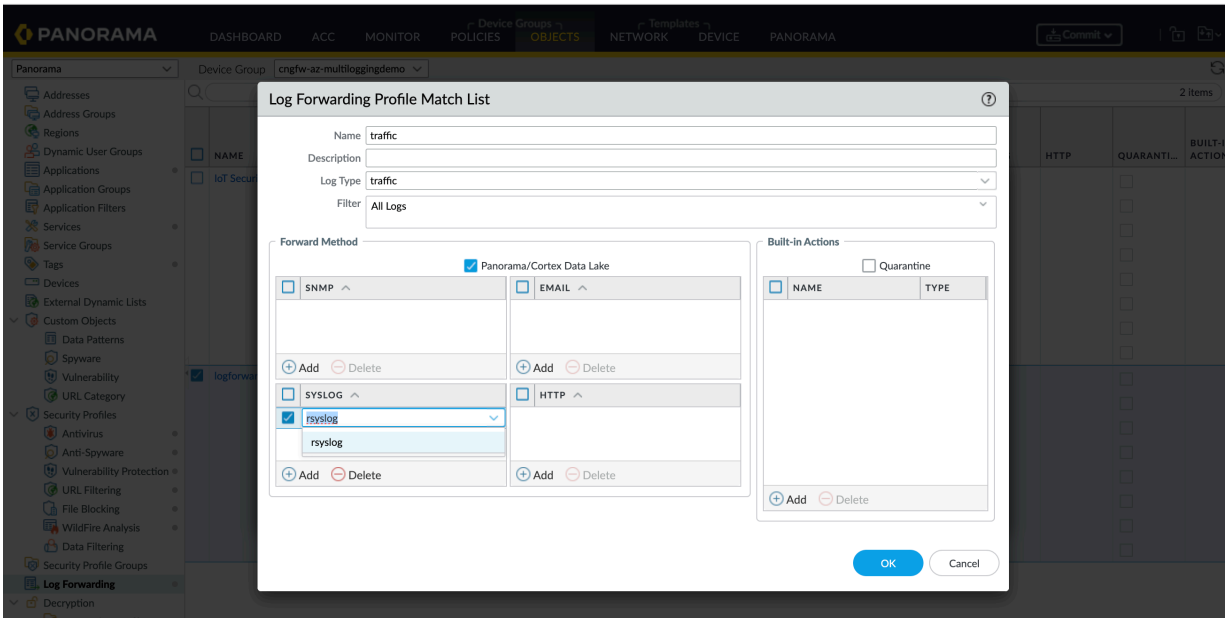
STEP 4 | Gehen Sie zur Registerkarte „Device“, klicken Sie auf **Setup** und dann auf **Service Route Configuration**.



- Für die Konfiguration des **servicebasierten Routings** wählen Sie **IPv4** und **Syslog**-Dienst aus. Sie müssen sicherstellen, dass **loopback.3** als Quellschnittstelle ausgewählt ist.
- Wählen Sie für die Konfiguration des **zielbasierten Routings** das Ziel aus, fügen Sie die private IP Ihres Syslog-Servers hinzu und wählen Sie dann **Loopback.3** als Quellschnittstelle aus.



STEP 5 | Fügen Sie im **Log Forwarding Profile** Ihren Syslog-Server hinzu.



STEP 6 | Wechseln Sie in Panorama zu **Policies** und wählen Sie dann die Richtlinienregel für Ihre Cloud-Gerätegruppe aus.

STEP 7 | Gehen Sie zur Registerkarte **Actions** und wählen Sie dann das **Log Forwarding Profile** aus.

STEP 8 | Klicken Sie auf **OK**.

STEP 9 | **Legen** Sie Ihre Änderungen fest und **übergeben** Sie sie an die Panorama-Konsole.

Das VNET-Peering muss zwischen dem Syslog-Server VNET und dem Firewall Hub VNET abgeschlossen werden, um Datenverkehr auf dem Syslog-Server zu empfangen. Nachdem der Datenverkehr gesendet wurde, können Sie die Cloud NGFW-Protokolle in Panorama und auf dem Syslog-Server anzeigen.

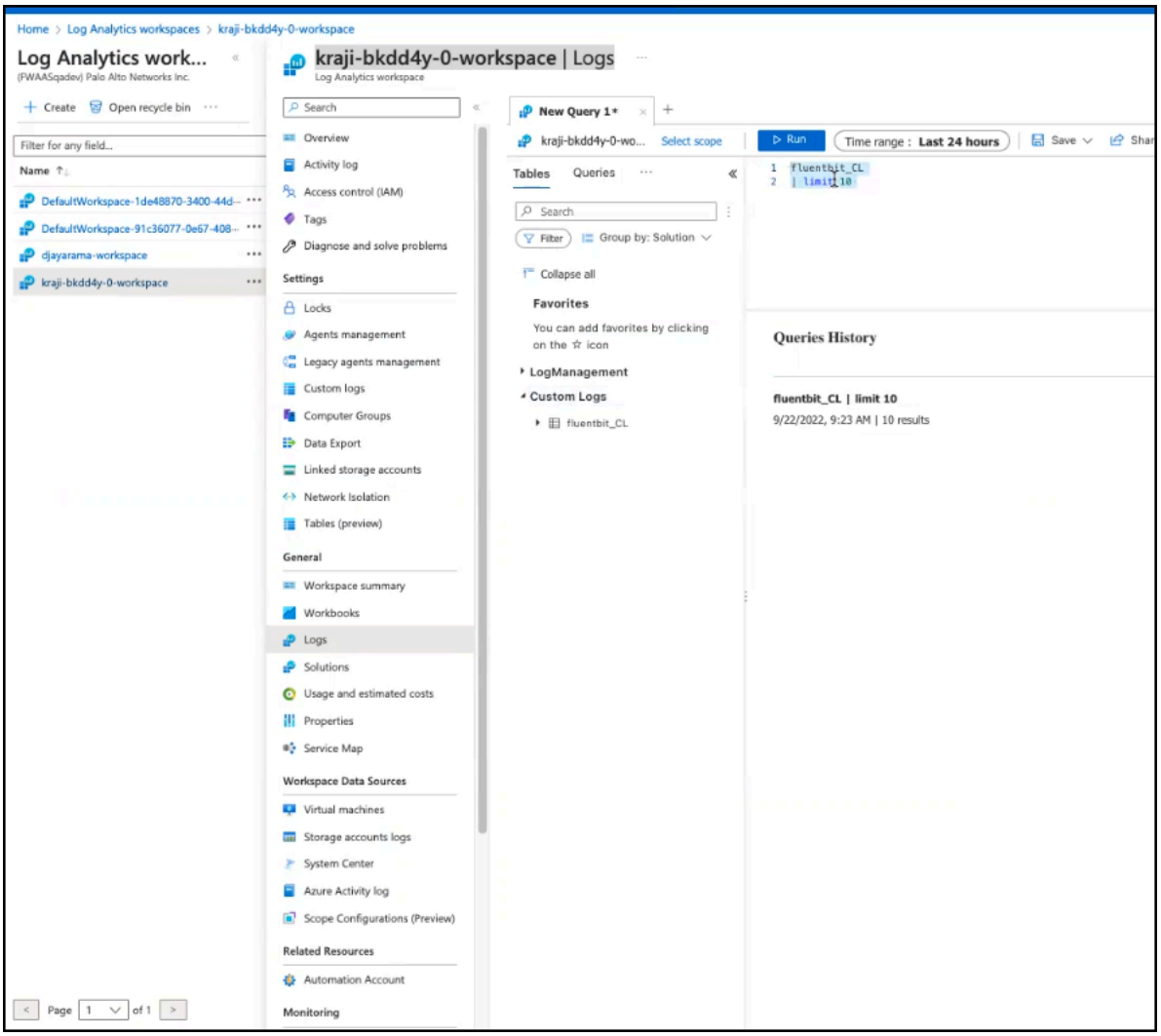
Anzeigen der Protokolle

Nachdem Sie den Log Analytics Workspace erstellt haben, aktualisieren Sie die Protokolleinstellungen der Firewall und beginnen mit dem Senden des Datenverkehrs. Sobald der Datenverkehr gesendet wurde, können Sie die Protokolle wie in den folgenden Schritten beschrieben anzeigen:

STEP 1 | Klicken Sie auf den **Log Analytics Workspace**, für den Sie die Protokolle anzeigen möchten.

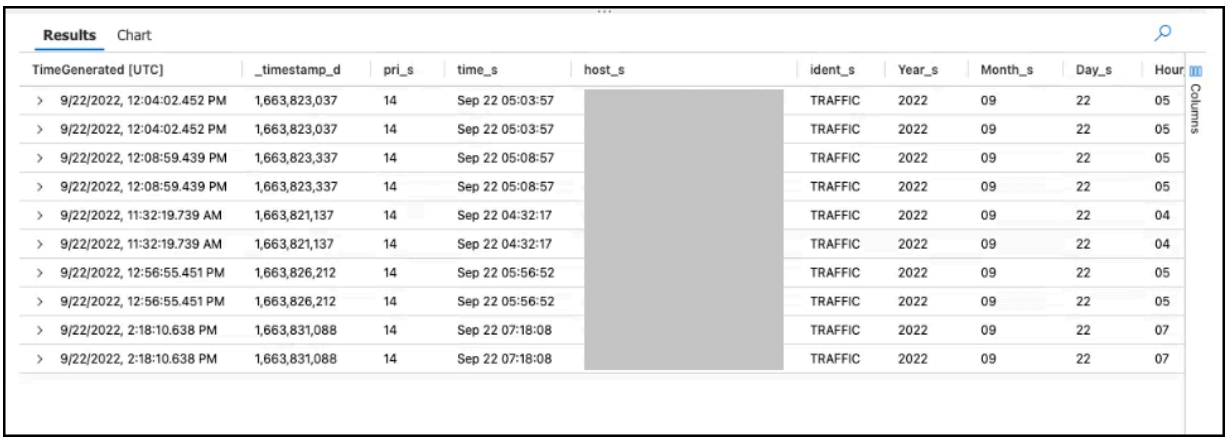
STEP 2 | Klicken Sie auf **Logs**.

STEP 3 | Klicken Sie im Abfragefenster auf **Custom Logs** und führen Sie eine von Ihnen erstellte **Abfrage** aus.



Sie können eine benutzerdefinierte Abfrage mit Parametern wie Anzahl der Protokolle, Zeitbereich usw. erstellen. Zum Beispiel – Eine einfache Abfrage

```
fluentbit_CL | limit 10
```

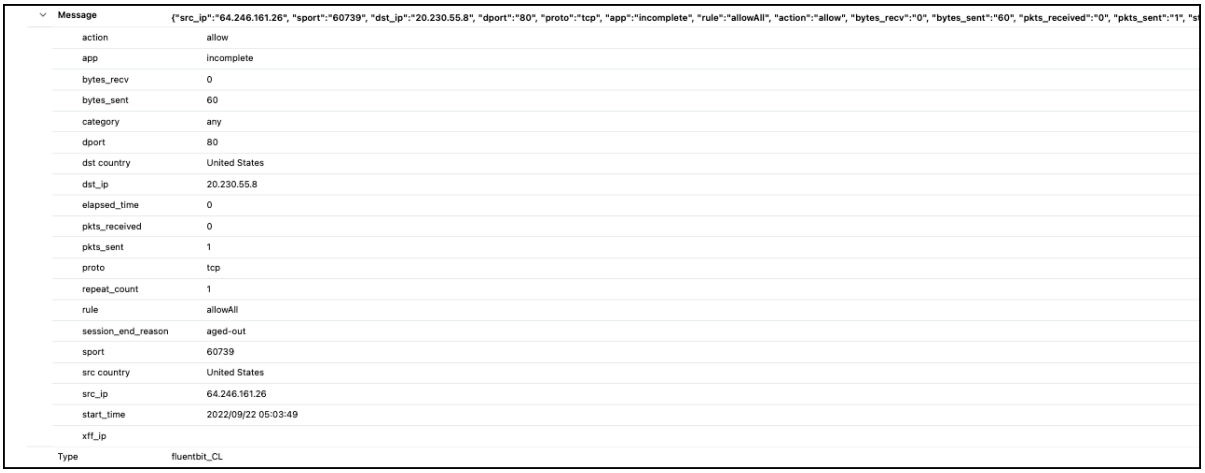



Results Chart

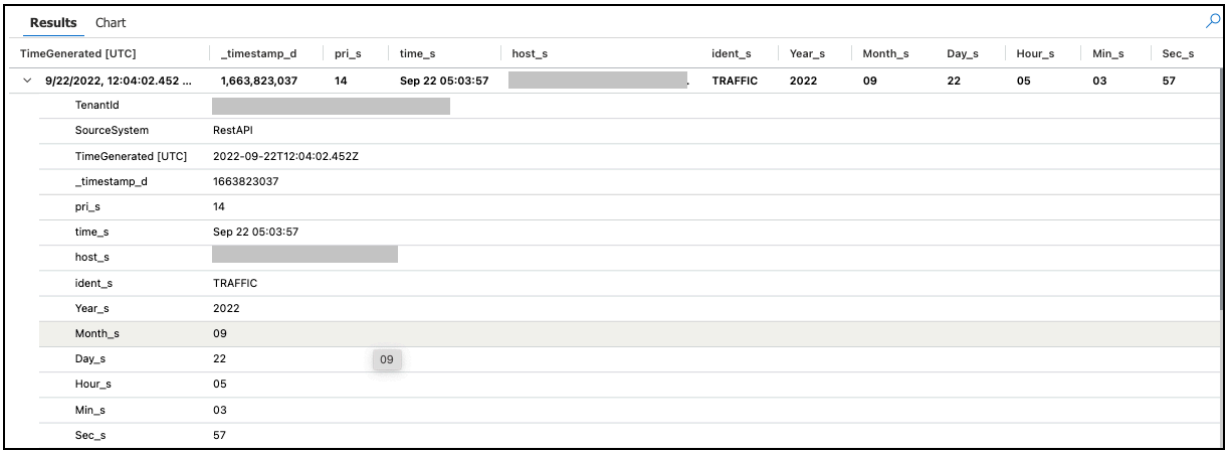
TimeGenerated [UTC]	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	Hour
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07

Columns

STEP 4 | Klicken Sie auf das gewünschte Abfrageergebnis, für das Sie detaillierte Protokolle anzeigen möchten.



Message	{"src_ip":"64.246.161.26", "sport":"60739", "dst_ip":"20.230.55.8", "dport":"80", "proto":"tcp", "app":"incomplete", "rule":"allowAll", "action":"allow", "bytes_recv":"0", "bytes_sent":"60", "pkts_received":"0", "pkts_sent":"1", "s
action	allow
app	incomplete
bytes_recv	0
bytes_sent	60
category	any
dport	80
dst country	United States
dst_ip	20.230.55.8
elapsed_time	0
pkts_received	0
pkts_sent	1
proto	tcp
repeat_count	1
rule	allowAll
session_end_reason	aged-out
sport	60739
src country	United States
src_ip	64.246.161.26
start_time	2022/09/22 05:03:49
xff_ip	
Type	fluentbit_CL



Results | Chart

TimeGenerated [UTC]	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	Hour_s	Min_s	Sec_s
9/22/2022, 12:04:02.452 ...	1,663,823,037	14	Sep 22 05:03:57	[redacted]	TRAFFIC	2022	09	22	05	03	57

TenantId	[redacted]
SourceSystem	RestAPI
TimeGenerated [UTC]	2022-09-22T12:04:02.452Z
_timestamp_d	1663823037
pri_s	14
time_s	Sep 22 05:03:57
host_s	[redacted]
ident_s	TRAFFIC
Year_s	2022
Month_s	09
Day_s	22
Hour_s	05
Min_s	03
Sec_s	57

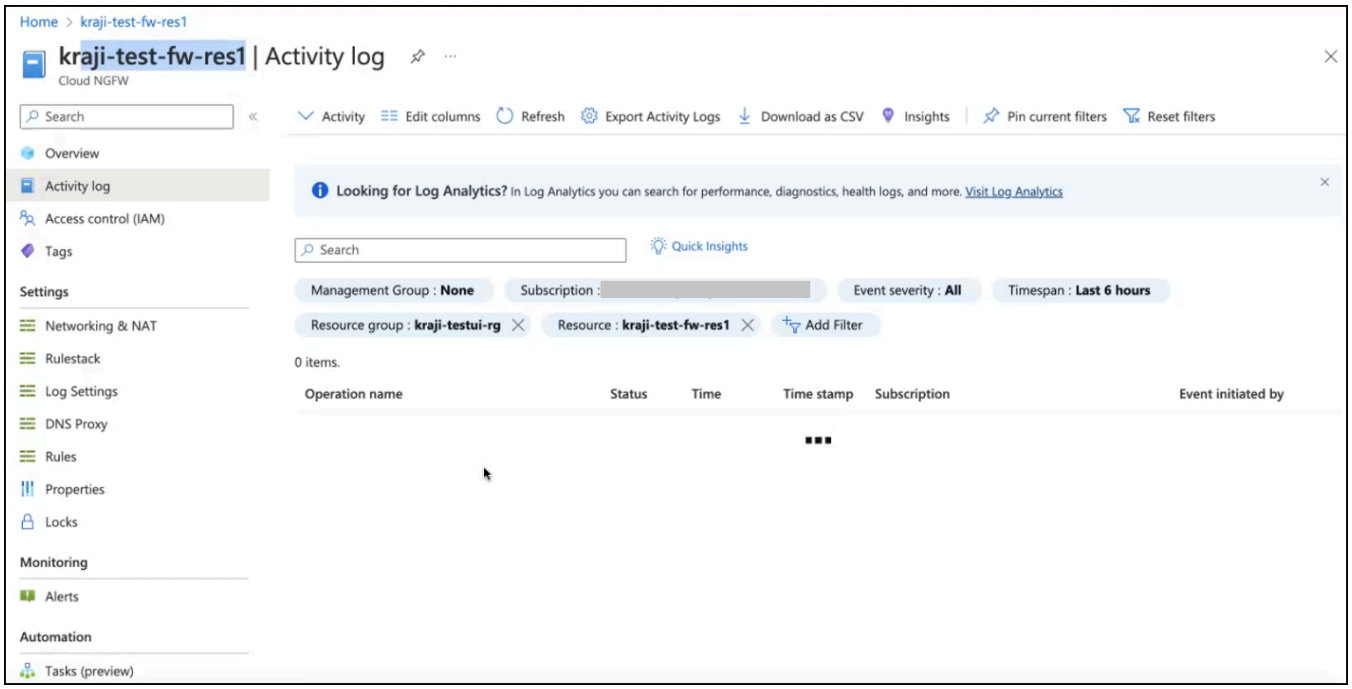
Anzeigen von Überwachungsprotokollen für eine Firewall-Ressource

So zeigen Sie Überwachungsprotokolle der Firewall-Ressource an, die in einer Ressourcengruppe bereitgestellt ist:

STEP 1 | Navigieren Sie von der Homepage zu der Cloud NGFW-Firewall-Ressource, deren Protokolle Sie anzeigen möchten.

STEP 2 | Klicken Sie im linken Bereich auf **Activity Log**, wählen Sie den gewünschten **Zeitraum** aus, für den Sie die Protokolle anzeigen möchten, und klicken Sie auf **Apply**. Die Liste der Protokolle für den ausgewählten Zeitraum wird angezeigt.

STEP 3 | Klicken Sie auf das gewünschte Protokoll, um die **Zusammenfassung** und **JSON** des Protokolls anzuzeigen.



Anzeigen von Überwachungsprotokollen für Ressourcengruppen

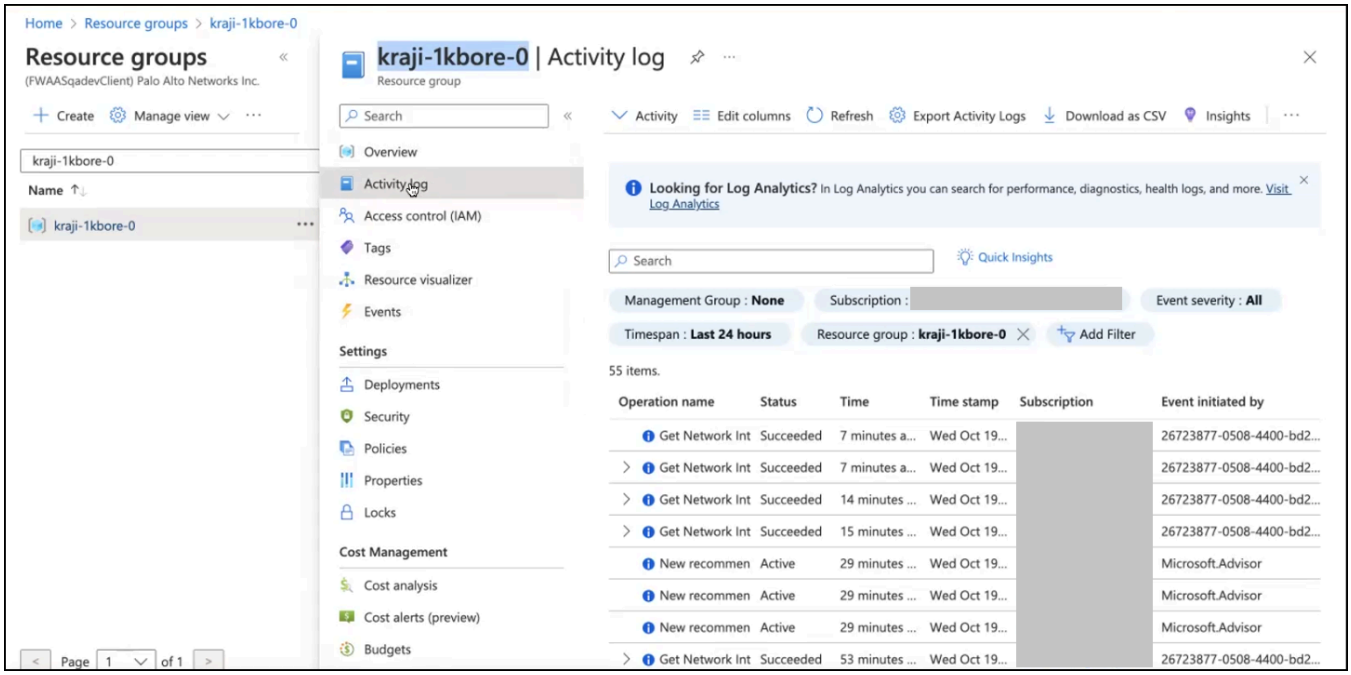
So zeigen Sie Überwachungsprotokolle für Ressourcengruppen an:

STEP 1 | Navigieren Sie von der Homepage zu **Resource Groups**.

STEP 2 | Klicken Sie auf die **Resource group**, für die Sie das Aktivitätsprotokoll erfassen möchten.

STEP 3 | Klicken Sie im linken Bereich auf **Activity Log**, wählen Sie den gewünschten **Zeitraum** aus, für den Sie die Protokolle anzeigen möchten, und klicken Sie auf **Apply**. Die Liste der Protokolle für den ausgewählten Zeitraum wird angezeigt.

STEP 4 | Klicken Sie auf das gewünschte Protokoll, um die **Zusammenfassung** und **JSON** des Protokolls anzuzeigen.



Neuigkeiten

Hier erfahren Sie, was neu in Cloud NGFW für Azure ist.

Was ist neu im Juni 2024

Neu	Beschreibung
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Japan West (Osaka) • Schweden Zentral (Gävle) • Italien Nord (Mailand) • Südafrika Nord (Johannesburg) • Israel Zentral • West Zentralamerika (Wyoming) • VAE Nord (Dubai) Eine vollständige Liste der unterstützten Regionen finden Sie unter Cloud NGFW für Azure – unterstützte Regionen und Zonen.

Was ist neu im Mai 2024

Neu	Beschreibung
Verwenden von XFF-Headerwert zur Durchsetzung von Sicherheitsrichtlinien	Cloud NGFW for Azure kann nun eine IP-Adresse in einem X-Forwarded-For-Header (XFF-Header) verwenden, um auf Panorama erstellte Sicherheitsrichtlinien durchzusetzen.
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Kanada Ost Eine vollständige Liste der unterstützten Regionen finden Sie unter Cloud NGFW für Azure – unterstützte Regionen und Zonen.
Sichtbarkeit von Verbrauch und Nutzung von Credits	Sie können Credits jetzt für die Nutzung von Cloud NGFW für langfristige Verträge verwenden, die Sie für Ihre Firewallressourcen in Azure-Cloudumgebungen auf Mandantenebene zuweisen können. Weitere Informationen finden Sie unter Sichtbarkeit der Nutzung von Credits.

Was ist neu im März 2024

Neu	Beschreibung
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Norwegen Ost • Deutschland West Zentral • Zentralindien • Schweiz Nord Eine vollständige Liste der unterstützten Regionen finden Sie unter Cloud NGFW für Azure – unterstützte Regionen und Zonen.
Gebühren für Azure-Netzwerk	Cloud NGFW für Azure berechnet Peering-Gebühren für virtuelle Netzwerke gemäß Azure Networking-Gebührendimension. Die Verbrauchsdetails werden im Azure Marketplace freigegeben. Die Nutzung wird für eingehenden (vom Internet zu VNET), ausgehenden (zum Internet von VNET) und Ost-West-Datenverkehr (über VNETs hinweg) verfolgt. Weitere Informationen zu den Gebühren finden Sie unter Preise für Cloud NGFW für Azure.
Unterstützung für eingehende Entschlüsselung	Cloud NGFW für Azure verwendet die eingehende SSL-Entschlüsselung, um eingehenden SSL/TLS-Datenverkehr von einem Client zu einem Zielnetzwerkserver zu untersuchen, zu entschlüsseln und verdächtige Sitzungen zu blockieren. Weitere Informationen finden Sie unter Eingehende Entschlüsselung in Cloud NGFW für Azure einrichten.

Was ist neu im Februar 2024

Neu	Beschreibung
Mehrere Protokollziele	Sie können jetzt Protokolle von Ihrer Panorama-verwalteten Cloud NGFW für Azure-Ressource an Azure Log Analytics Workspace, Syslog-Server und Panorama senden. Weitere Informationen finden Sie unter Mehrere Protokollziele in Cloud NGFW für Azure.
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Frankreich Zentral • Süd Zentral US Siehe Cloud NGFW für Azure – unterstützte Regionen und Zonen für eine vollständige Liste der unterstützten Regionen.

Was ist neu im Januar 2024

Neu	Beschreibung
Unterstützung für 100 Gbit/s	Diese Version ermöglicht es Cloud NGFW für Azure, automatisch bis zu 100 Gbit/s für vNET- und vWAN-Bereitstellungen zu skalieren. Weitere Informationen finden Sie unter Bereitstellen der Cloud NGFW in einem vNET und Bereitstellen der Cloud NGFW in einem vWAN.

Was ist neu im Dezember 2023

Neu	Beschreibung
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Nord-Zentral-USA • Südostasien Siehe Cloud NGFW für Azure – unterstützte Regionen und Zonen für eine vollständige Liste der unterstützten Regionen.
Unterstützung für private Quell-NAT	Ab dieser Version ist die Unterstützung für die private Quell-NAT verfügbar. Mit dieser Unterstützung können Sie ein privates NAT-Gateway erstellen, um eine Übersetzung der Netzwerkadresse (NAT, Network Address Translation) durchzuführen. Weitere Informationen finden Sie unter Bearbeiten einer vorhandenen Firewall, um private Quell-NAT zu aktivieren.

Was ist neu im November 2023

Neu	Beschreibung
Weitere unterstützte Azure-Regionen	Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar: • Japan Ost • Brasilien Süd Siehe Cloud NGFW für Azure – unterstützte Regionen und Zonen für eine vollständige Liste der unterstützten Regionen.
Regelstapel-Erweiterungen	Diese Version unterstützt implizite Regellöschungen in einem Regelstapel. Mit dieser Erweiterung ist Folgendes möglich: • Sie können nicht zugeordnete Regelstapel, die nicht leer sind, löschen, ohne Regeln und Objekte zu löschen. • Sie können Ressourcengruppen unter Beibehaltung leerer oder nicht leerer, nicht zugeordneter Regelstapel löschen. • Sie können nicht zugeordnete Regelstapel, die nicht leer sind, mit Azure CLI, CDK, PowerShell und Terraform löschen. *Diese Löschfunktion gilt für nicht gebundene und nicht leere Regelstapel.*
Unterstützung für DNS-Sicherheitsdienst	Cloud NGFW für Azure fügt Unterstützung für den Palo Alto Networks DNS-Sicherheitsdienst hinzu. Mit diesem Dienst können Sie vNET- und vWAN-Datenverkehr vor erweiterten DNS-basierten Bedrohungen schützen, indem die Domänen überwacht und gesteuert werden, die von Ihren Netzwerkressourcen abgefragt werden. Für weitere Informationen siehe DNS-Sicherheit in Cloud NGFW für Azure aktivieren.
Unterstützung für Nicht-RFC 1918	Diese Version unterstützt zusätzliche private IP-Bereiche neben den in RFC 1918 angegebenen Adressen für vNET- und vWAN-Bereitstellungen. Mit dieser Unterstützung können Sie öffentliche IP-Adressblöcke (z. B. 40.0.0.0/24) als Ihr privates Netzwerk verwenden, ohne den Datenverkehr ins Internet umzuleiten. Weitere Informationen zu dieser Funktion in vNET-Bereitstellungen finden Sie in den Informationen im Abschnitt **Networking** (Schritt 5) Zusätzliche Präfixe für privaten Datenverkehrsbereich.

Was ist neu im Oktober 2023

<table>
<tr><th>Neu</th><th>Beschreibung</th></tr>
<tr><td>Weitere unterstützte Azure-Regionen</td><td>Cloud NGFW für Azure ist jetzt in den folgenden Azure-Regionen verfügbar:
US West 2
Nordeuropa
Siehe Cloud NGFW für Azure – unterstützte Regionen und Zonen für eine vollständige Liste der unterstützten Regionen.</td></tr>
<tr><td>Programmgesteuerter Zugriff</td><td>Der programmgesteuerte Zugriff ermöglicht Ihnen das Erstellen und Verwalten von NGFWs und Regelstapeln mithilfe von APIs. Mit diesen APIs können Sie Aktionen für Cloud NGFW-Ressourcen über eine Anwendung oder ein Drittanbieter-Tool aufrufen. Die folgende Tabelle enthält Informationen zu unterstützten Tools:<table><tr><td>Terraform</td><td>Verwenden Sie den Azure Provider zum Konfigurieren der Infrastruktur mithilfe von Azure Resource Manager-APIs.</td></tr><tr><td>PowerShell</td><td>Verwenden Sie Microsoft Azure PowerShell cmdlets zum Konfigurieren von Cloud NGFW für Azure.</td></tr><tr><td>CLI</td><td>Verwenden Sie diese Befehle, um Ihre Cloud NGFW für Azure-Ressourcen zu verwalten</td></tr><tr><td>SDK</td><td>SDK Paket für Python wird unterstützt.</td></tr></table></td></tr>
</table>

Was ist neu im September 2023

Neu	Beschreibung
SSO-Anmeldung in Ihr Support Portal-Konto integrieren	Integrieren Sie den SSO-Anmeldefluss Ihres Unternehmens mit Ihrem Palo Alto Networks Customer Support Portal-Konto in Ihr Cloud NGFW für Azure-Abonnement. Weitere Informationen finden Sie unter Single Sign-on integrieren.
Unterstützung für öffentliche Domänen-E-Mail-Adressen	In dieser Version wurde die Unterstützung für öffentliche Domänen-E-Mail-Adressen für Customer Support Portal-Konten hinzugefügt. Bisher benötigten Benutzer, die Cloud NGFW-Assets und zugehörige Supportfälle verwalteten, eine Unternehmens-E-Mail-Adresse, um sich bei dem Konto anzumelden. Mit dieser zusätzlichen Funktionalität ist Folgendes möglich: • Öffentliche Domänenbenutzer greifen auf Assets zu und unterstützen Fälle in Konten, in denen sie Mitglieder sind. • RBAC-Zugriffskontrollen können Benutzern mit öffentlichen Domänen-E-Mails zugewiesen und auf sie angewendet werden. • Ein Benutzer mit einer öffentlichen Domänen-E-Mail-Adresse in einem Konto kann nicht auf Assets zugreifen und Fälle in einem anderen Konto unterstützen. Beheben Sie dieses Problem, indem Sie den Benutzer mit der öffentlichen Domänen-E-Mail-Adresse dem Konto hinzufügen, auf das er zugreifen muss. • Einem Benutzer mit einer öffentlichen Domänen-E-Mail-Adresse wird eine beliebige Rolle zugewiesen, einschließlich Superuser und Domänenadministrator. • Ein Konto kann einen oder mehrere Benutzer mit einer öffentlichen Domänen-E-Mail-Adresse haben. Wenn ein Konto von einem Benutzer mit einer öffentlichen Domänen-E-Mail-Adresse erstellt wurde, gilt das Konto als *öffentlich*. *Ein Konto kann keine Mischung aus Benutzern mit Unternehmens- und öffentlichen E-Mail-Adressen aufweisen.* Die folgenden öffentlichen Domänen-E-Mail-Adressen werden unterstützt: gmail.com, yahoo.*, hotmail.* live.*, outlook.com, aol.com gms.* (gmx.de, gmx.net, gmx.us), icloud.com, msn.com comcast.net**, att.net

Was ist neu im August 2023

Neu	Beschreibung
Allgemeine Verfügbarkeit	Cloud NGFW für Azure hat die allgemeine Verfügbarkeit erreicht. Diese Version enthält zahlreiche Korrekturen, Unterstützung für zusätzliche Regionen und Verbesserungen am Abonnementmodell Pay-as-you-go (PAYG).

Was ist neu im Juni 2023

Neu	Beschreibung
Zustandsüberwachung	Anzeigen von Gesamtzustand der Cloud NGFW-Firewall, Verbindungsstatus und Diagnoseinformationen. Verwenden Sie diese Informationen, um die Ursache für einen fehlerhaften Firewallzustand zu ermitteln. Weitere Informationen finden Sie unter Überwachen des Cloud NGFW-Zustands.

Was ist neu im Mai 2023

Neu	Beschreibung
Erstveröffentlichung von Cloud NGFW für Azure	Die erste Version von Cloud NGFW für Azure enthält die folgenden Funktionen: • vNET- und vWAN-basierte Firewall-Bereitstellungen • Single und Multihub für vWAN. Weitere Informationen finden Sie unter Konfigurieren von Palo Alto Networks Cloud NGFW in virtuellem WAN. • Anwendungsfälle für eingehenden, ausgehenden und Ost-West-Datenverkehr • Richtlinienverwaltung für Regelstapel, Präfixobjekte, FQDN-Objekte und Zertifikatobjekte • Unterstützung der Protokollierung • Autoscale-Unterstützung • Ausgehende Entschlüsselung • Inhalts- und Virenschutzupgrades • Rollende Upgrades für Firewallressourcen • Unterstützung durch das Customer Support Portal • Unterstützung für integrierte Rollen (LocalNGFirewall und LocalRuleStacksAdministrator)

Bekannte Probleme bei Cloud NGFW für Azure

Die folgenden bekannten Probleme wurden in der Cloud NGFW für Azure von Palo Alto Networks erkannt.

ID	Beschreibung
FWAAS-10519	Wenn das Multilogging-Ziel aktiviert ist, werden die Protokolle in Panorama und dem Syslog-Server angezeigt, aber im Log Analytics Workspace werden keine Protokolle angezeigt. Problemumgehung: Wenn Sie Syslog zusammen mit Log Analytics Workspace verwenden möchten, ändern Sie die Service-Route auf eine zielbasierte statt auf eine dienstbasierte Route. Wählen Sie für die Konfiguration des **zielbasierten Routings** das Ziel aus, fügen Sie die private IP Ihres Syslog-Servers hinzu und wählen Sie dann **loopback.3** als Quellschnittstelle aus.
FWAAS-9688	Standardregeln in Panorama werden von der Cloud NGFW-Ressource außer Kraft gesetzt. Parameter wie **Profile** und **Action** werden nicht beibehalten. Wenn Sie beispielsweise eine Aktion mit **Allow** konfigurieren, wird sie auf **Deny** zurückgesetzt; wenn Sie ein Protokollierungsprofil konfigurieren, wird es auf **None** zurückgesetzt.
FWAAS-7531	Ein selbstsigniertes Zertifikat kann fälschlicherweise einem Regelstapel zugeordnet werden, obwohl kein Ressourcenname vorhanden ist.
FWAAS-7542	Panorama überträgt Inhalts- und Antivirenupdates nicht immer automatisch für neu erstellte Cloud NGFW für Azure-Ressourcen.
FWAAS-7547	QoS-Profile (von einer Gerätevorlage bereitgestellt) werden nicht entfernt, wenn sie in der virtuellen Panorama-Appliance angezeigt werden.
FWAAS-7956	Ein Regelstapel zeigt falsche Informationen an, wenn er denselben Namen wie die Firewall hat.
FWAAS-8642	Das Erstellen einer großen Anzahl lokaler Regeln kann zu einem HTTP-Fehler führen (503 Serverfehler: Dienst nicht verfügbar).
FWAAS-9086	Die Informationen zum Bereitstellungsstatus im Azure-Portal werden gekürzt, ohne dass vollständige Informationen angezeigt werden.
FWAAS-10195	Die Firewallerstellung schlägt fehl, wenn Sie Nicht-RFC 1918-Adressen aktivieren, ohne den DNS-Proxy zu aktivieren.

ID	Beschreibung
PAN-217954	Wenn eine Cloud NGFW für Azure-Ressource zum ersten Mal eine Verbindung zu Panorama herstellt, ist der Vorlagenstapel, der der Cloud-Gerätegruppe der Ressource zugeordnet ist, nicht synchron.
PAN-217459	Cloud NGFW-Ressourcen, die von einem Panorama HA-Paar verwaltet werden, werden in der Cloud-Gerätegruppe möglicherweise mit der Seriennummer (statt des Gerätenamens) auf dem sekundären Panorama aufgeführt. Im primären Panorama wird die Cloud NGFW-Ressource jedoch mit ihrem Gerätenamen aufgeführt.
PAN-217966	Konfigurierte dynamische Adressgruppen-Tags und IP-Adressen werden nicht in untergeordneten Cloud-Gerätegruppen aufgeführt, wenn für die übergeordnete Gerätegruppe keine dynamische Adressgruppe konfiguriert ist.

Behobene Probleme in Cloud NGFW für Azure

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

ID	Beschreibung
FWAAS-3919	Es wurde festgestellt, dass in lokalen Regelstapeln ungültige Regelnamen generiert werden könnten, die Commit-Fehler verursachen könnten.
FWAAS-4546	DB-Einträge des Regeltrefferzählers werden nach dem Löschen der Regel nicht gelöscht, sodass beim erneuten Erstellen einer Regel mit demselben Namen alte Werte zurückbleiben.
FWAAS-4767	Der DNS-Proxy wird nach einem Firewall-Update-Aufruf nicht gleichzeitig mit der Firewall aktualisiert.
FWAAS-4805	Firewall-Hostnamen werden in Protokollen fälschlicherweise angezeigt.
FWAAS-7430	Wenn Sie versuchen, eine neue Cloud NGFW-Ressource zu löschen, bevor die Erstellung abgeschlossen ist, schlägt der Löschvorgang fehl.
FWAAS-7542	Panorama überträgt Inhalts- und Antivirenupdates nicht immer automatisch für neu erstellte Cloud NGFW für Azure-Ressourcen.
FWAAS-8696	Die Protokollweiterleitung an eine virtuelle Panorama-Appliance kann viel Zeit in Anspruch nehmen.
FWAAS-9041	Geräteserverprofile (z. B. LDAP, Syslog) werden in Panorama-Vorlagen, die für CNGFW-Geräte verwendet werden, fälschlicherweise als deaktiviert angezeigt.
FWAAS-9050	In einigen Fällen kann eine Lizenz einer Firewall der VM-Serie aus der virtuellen Panorama-Appliance entfernt werden.
FWAAS-9055	Wenn der Name der Cloud-Gerätegruppe geändert wird, gerät CNGFW in einen Fehlerzustand und verliert die Verbindung zu Panorama.
PAN-217460	Von einem Panorama HA-Paar verwaltete Cloud NGFW-Ressourcen werden auf dem sekundären Panorama möglicherweise als getrennt angezeigt. Im primären Panorama wird die Cloud NGFW-Ressource jedoch als verbunden angezeigt.

