VM-SERIES FÜR AMAZON WEB SERVICES

Amazon Web Services (AWS) bieten Ihnen die Möglichkeit, neue Anwendungen für moderne Rechenzentren zügig und in globalem Umfang zu entwickeln, bereitzustellen und zu verwalten. Mit der VM-Series für AWS können Sie Ihre Anwendungen und Daten in AWS mit innovativen Firewall- und Abwehrfunktionen vor Bedrohungen schützen.

Anwendungsfälle der VM-Series für AWS in der hybriden Cloud

Hybrid-Cloud

- Stellen Sie mit unseren umfassenden innovativen Firewall- und Bedrohungsschutzfunktionen auf sichere Weise eine hybride Cloud bereit.
- Verschieben Sie Anwendungen und Daten über einen standardbasierten Site-to-Site IPsec VPN-Tunnel in und aus AWS.

Segmentierungsgateway

- Steuern Sie die Anwendungskommunikation in unterschiedlichen Subnetzen innerhalb und zwischen virtuellen privaten Clouds (VPCs) und blockieren Sie gleichzeitig laterale Bedrohungsbewegungen.
- Trennen Sie vertrauliche Daten aus Sicherheits- und Compliance-Gründen konsequent von anderem Datenverkehr.

Internetgateway

- Steuern Sie Anwendungen in AWS und verhindern Sie gleichzeitig, dass Angreifer mit fortschrittlichen Cyberattacken in Ihre Cloud gelangen und sich darin lateral bewegen.
- Erweitern Sie die Firewall- und Bedrohungsschutz-Richtlinien mit GlobalProtect auf Remote-Benutzer und Mobilgeräte.

Herausforderungen an die Sicherheit in der öffentlichen Cloud

AWS bietet die allseits bekannten Vorteile einer erhöhten Agilität, Skalierbarkeit und Flexibilität bei der Entwicklung und Bereitstellung von Anwendungen. Die Herausforderungen an die Sicherheit sind in AWS jedoch genau die gleichen wie beim Schutz eines physischen Netzwerks.

Zu den Problematiken zählen mangelnde Anwendungstransparenz und -steuerung, die Unfähigkeit hinsichtlich der Abwehr von Cyberattacken sowie mühsame Verfahren zur Richtlinienaktualisierung, die zu Verzögerungen zwischen der Bereitstellung von Arbeitslasten und der Aktualisierungen von Sicherheitsrichtlinien führen können. Die VM-Series für AWS löst diese Herausforderungen durch folgende Funktionsweisen:

- Identifizierung und Steuerung der Anwendungen, die Ihre AWS-Bereitstellung durchlaufen, ungeachtet des verwendeten Ports
- Ermittlung und Erteilung von Zugriffsrechten auf die Anforderungen basierend auf dem Bedarf und den Anmeldeinformationen
- Vermeidung der Einschleusung und lateralen (Ost-West-) Bewegung von Malware in der Cloud
- Erweiterung der Perimeterschutzmechanismen auf alle Benutzer und Geräte, ungeachtet ihres Standorts
- Vereinfachung des Managements und Minimierung von Verzögerungen durch Aktualisierungen von Sicherheitsrichtlinien aufgrund von Änderungen der virtuellen Arbeitslasten

Die VM-Series für AWS schützt Ihre Arbeitslasten und Daten mit denselben innovativen Firewall- und Bedrohungsschutzfunktionen, die Ihnen auch in unseren Sicherheits-Appliances zur Verfügung stehen, um Ihnen eine sichere Migration zur Cloud zu ermöglichen.

Sicherheitsgruppen, WAF oder innovative Firewall?

Im Rahmen seines Serviceportfolios bietet AWS Benutzern diverse grundlegende Sicherheitsfunktionen wie Zugangskontrolllisten (Access Control Lists, ACLs) von Sicherheitsgruppen sowie Web Application Firewalls (WAF). Diese Funktionen tragen zum Schutz Ihrer AWS-Bereitstellung bei. Sicherheitsgruppen und ACLs überprüfen den Datenverkehr jedoch nur hinsichtlich der verwendeten Ports und IP-Adressen. Sie sind nicht in der Lage, den AWS-Datenverkehr anhand der Anwendungsidentität zu identifizieren und zu steuern. WAFs überprüfen ausschließlich HTTP/HTTPS-Anwendungen. Diese Funktionen bieten somit nur einen Basisschutz, um Ihre Angriffsoberfläche zu reduzieren. Sie ermöglichen weder die umfassende Steuerung aller Anwendungen, noch schützen sie Ihre Umgebung vor eingehenden Bedrohungen oder unterbinden deren laterale Bewegung. Da Unternehmen die öffentliche Cloud zunehmend als Erweiterung ihrer Rechenzentren nutzen, sind die fortschrittlichen Sicherheitsfunktionen etwa einer innovativen Firewall unabdingbar.

VM-Series für AWS

Die VM-Series für AWS ermöglicht Ihnen die sichere Implementierung einer Cloud First-Methode. Gleichzeitig transformiert sie Ihr Rechenzentrum in eine hybride Architektur, welche die Skalierbarkeit und Agilität von AWS mit Ihren lokalen Ressourcen kombiniert. Sie können Ihre Anwendungen und Daten dadurch zu AWS migrieren und gleichzeitig die Sicherheitsaufstellung aufrechterhalten, die Sie in Ihrem physischen Netzwerk mithilfe von anwendungsbasierten Firewalls von Palo Alto Networks® etabliert haben.

Die VM-Series für AWS analysiert nativ den gesamten Datenverkehr in einer Single-Pass-Architektur, um die Identität der Anwendung und des Benutzers sowie des Inhalts zu ermitteln. Diese Komponenten sind wichtig, um Ihre Sicherheitsaufstellung zu definieren und die damit verbundenen Managementaufgaben hinsichtlich Transparenz, Richtliniensteuerung, Berichterstattung und Vorfalluntersuchung auszuführen.

Verbesserte Sicherheitsentscheidungen durch Anwendungstransparenz

Die VM-Series für AWS identifiziert Anwendungen ungeachtet des genutzten Ports. Sie erhalten dadurch äußerst relevante Informationen zu Ihrer AWS-Bereitstellung, etwa über die Anwendung, den Benutzer und die Quelle. Dieses erweiterte Wissen ermöglicht es Ihnen, informiertere Richtlinienentscheidungen zu treffen und schneller auf Vorfälle zu reagieren.

Reduzierung der Angriffsoberfläche durch Positivlisten-Richtlinien

Mit der VM-Series für AWS können Sie Ihre Richtlinien für die Zugriffssteuerung von Firewalls auf die Anwendungsebene erweitern. Setzen Sie die Ausführung von Anwendungen über bestimmte Ports durch, und nutzen Sie gleichzeitig die Voraussetzung „Alles andere ablehnen“, auf der Firewalls basieren, um alle anderen Anwendungen zu blockieren. Dieses zusätzliche Maß an Steuerung wird umso wichtiger, je mehr Ihrer Rechenzentrumsressourcen Sie zu AWS migrieren.

Verbesserte Sicherheitsaufstellung durch benutzerbasierte Steuerfunktionen

Durch die Integration in eine Vielzahl von Benutzerrepositories wie Microsoft® Active Directory®, LDAP und Microsoft Exchange wird die Benutzeridentität zum Bestandteil der Richtlinie, um Positivlisten von Anwendungen durch eine zusätzliche Zugriffssteuerungsfunktion zu ergänzen. Mithilfe von benutzerdefinierten Richtlinien können Sie Zugriff auf kritische Anwendungen und Daten, basierend auf den Anmeldeinformationen und dem jeweiligen Bedarf der Benutzer, erteilen. So kann das App-Team beispielsweise Vollzugriff auf die Entwicklungs-VPC erhalten, während Sie dem Betriebsteam RDP/SSH-Zugriff auf das Produktions-VPC gewähren.

Abwehr fortschrittlicher Angriffe auf der Anwendungsebene

Angreifer können ähnlich wie zahlreiche Anwendungen beliebige Ports nutzen, wodurch herkömmliche Schutzmechanismen wirkungslos werden. Die VM-Series für AWS bietet Ihnen die Möglichkeit, mithilfe der Threat Prevention- und WildFire™-Services anwendungsspezifische Richtlinien zur Abwehr von Bedrohungen anzuwenden um zu verhindern, dass Exploits, Malware und bislang unbekannte Bedrohungen (APTs) Ihre Cloud infizieren.

Erhöhte Datensicherheit durch Segmentierung

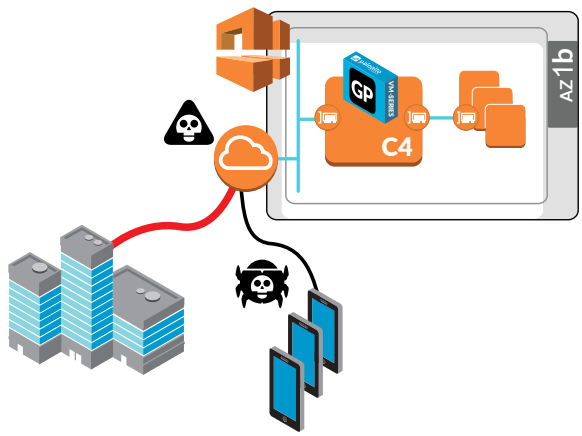
Moderne Cyberbedrohung gelangen in der Regel über eine einzelne Workstation oder einen einzelnen Benutzer in Ihr physisches oder virtualisiertes Netzwerk und bewegen sich anschließend lateral darin, wodurch sie Ihre unternehmenskritischen Anwendungen und Daten gefährden. Mithilfe von Sicherheitszonen und Positivlisten-Richtlinien können Sie Anwendungen segmentieren, die zwischen unterschiedlichen Subnetzen und VPCs kommunizieren, um behördliche Auflagen zu erfüllen. Indem Sie Ihre Segmentierungsrichtlinien durch Threat Prevention- und WildFire-Services ergänzen, können Sie sowohl bekannte als auch unbekannte Bedrohungen blockieren und verhindern, dass sich diese lateral zwischen Arbeitslasten bewegen.

Richtlinienkonsistenz durch zentrales Management

Neben Ihren physischen Sicherheits-Appliances können Sie mit Panorama™ Ihre VM-Series-Bereitstellungen in mehreren Cloud-Bereitstellungen verwalten. Sie stellen dadurch die Konsistenz und den Zusammenhang Ihrer Richtlinien sicher. Dank umfangreicher zentralisierter Protokollierungs- und Berichterstattungsfunktionen erhalten Sie einen transparenten Einblick in virtualisierte Anwendungen, Benutzer und Inhalte.

Automatisierte Sicherheitsbereitstellung und Richtlinienaktualisierungen

Die VM-Series für AWS beinhaltet native Managementfunktionen, mit denen Sie Ihre Cloud-First-Bereitstellungsprojekte schützen können. Bootstrapping stellt automatisch eine Firewall mit einer funktionierenden Konfiguration einschließlich Lizenzen und Abonnements bereit und registriert sich anschließend automatisch bei Panorama. Zur Automatisierung von Richtlinienaktualisierungen bei sich ändernden Arbeitslasten stehen der VM-Series eine vollständig dokumentierte XML API sowie Dynamic Address Groups (dynamische Adressgruppen, DAGs) zur Verfügung, um externe Daten in Form von Tags zu verarbeiten, die dynamische Richtlinienaktualisierungen ermöglichen können. Neue Anwendungen und Sicherheitsfunktionen der nächsten Generation lassen sich auf diese Weise gleichzeitig und automatisch bereitstellen.



Anwendungsfälle der VM-Series für AWS

Die VM-Series kann in einer Reihe unterschiedlicher Anwendungsfälle für AWS bereitgestellt werden.

Hybride Cloud: Sichere Erweiterung Ihres Rechenzentrums auf AWS

Eine der einfachsten Möglichkeiten, um neue Cloud First-Bereitstellungsinitiativen sicher zu bewerkstelligen, ist die hybride Bereitstellung, bei der Ihr vorhandenes Rechenzentrum über eine sichere Verbindung in AWS integriert wird. Mit diesem Ansatz können Sie klein beginnen und die Bereitstellung nach und nach entsprechend Ihren Anforderungen erweitern, während Sie konsequent eine starke Sicherheitsaufstellung aufrechterhalten. Durch die Bereitstellung in AWS kann die VM-Series als VPN-Endpunkt agieren, um Anwendungen und Daten sicher zu und von AWS zu bewegen. Richtlinien zur Anwendungssteuerung sowie zur Abwehr von Bedrohungen können als zusätzliche Sicherheitsebene des IPSec VPN-Tunnels genutzt werden.

Segmentierungsgateway: Trennung für Sicherheit und Compliance

Fortschrittliche Angriffe haben gezeigt, dass Cyberkriminelle sehr raffiniert sind, wenn es darum geht, Perimeterkontrollen unerkannt zu umgehen und sich frei in physischen und virtualisierten Netzwerken zu bewegen. Durch eine AWS VPC können Sie Ihre Arbeitslasten isolieren und schützen. Die VM-Series kann diese Trennung durch Segmentierungsrichtlinien auf Anwendungsebene erweitern, um den Datenverkehr zwischen VPCs zu steuern. Segmentierungskontrollen tragen in Verbindung mit Threat Prevention-Richtlinien dazu bei, laterale Bewegungen von Bedrohungen zu unterbinden. Datenverkehr, der über das Internet zwischen VPCs in unterschiedlichen Regionen fließt, kann für zusätzlichen Schutz verschlüsselt werden.

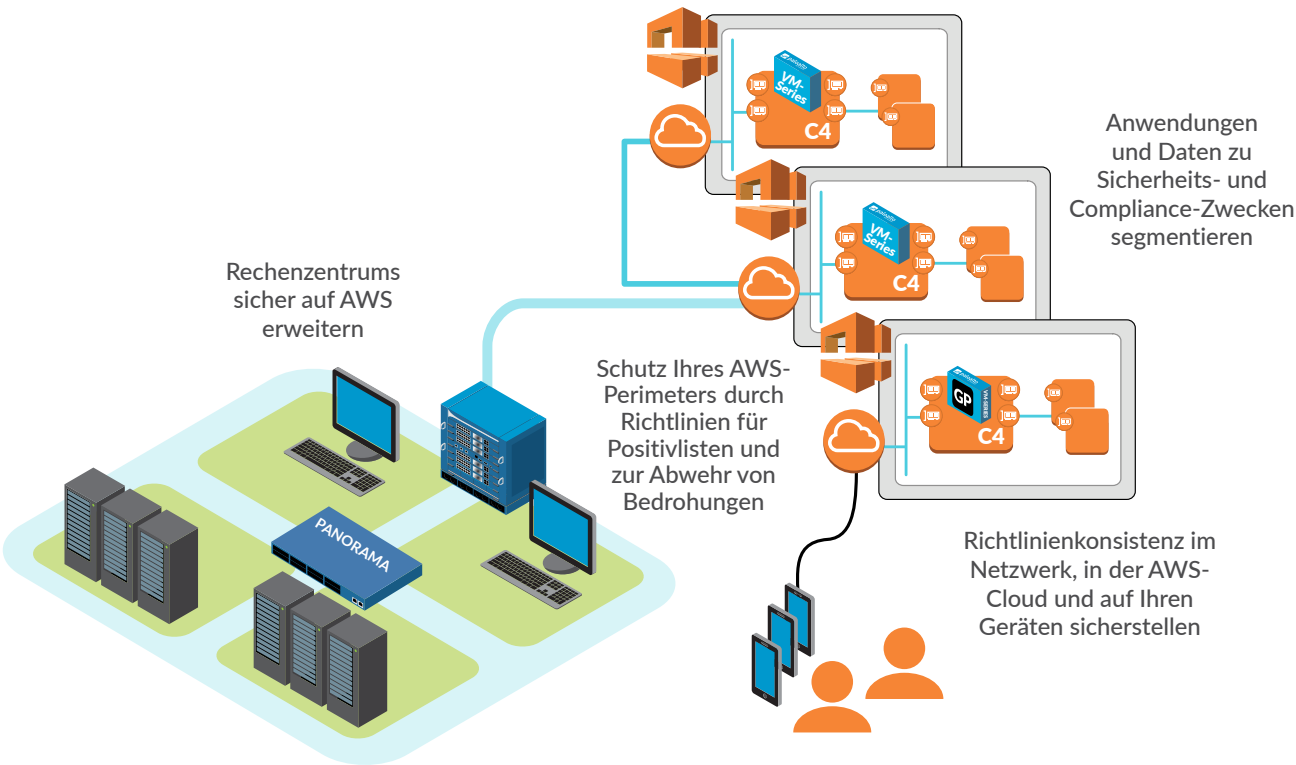
Internetgateway: Schutz von Netzwerk, Cloud und Geräten

Schützen Sie Ihre öffentlich zugänglichen (Web-)Anwendungen und stärken Sie Ihre Sicherheitsaufstellung durch Positivlisten-Richtlinien, um Zugriff auf Anwendungen entsprechend der Benutzeridentität und dem geschäftlichen Bedarf zu gewähren. Sie können als zusätzlichen Schutz vor Cyberbedrohungen auch anwendungsspezifische Richtlinien zur Abwehr von Bedrohungen anwenden um zu verhindern, dass Exploits, Malware und bislang unbekannte Bedrohungen (APTs) Ihre AWS-Bereitstellung infizieren.

GlobalProtect bietet Ihnen die Möglichkeit, die Sicherheitsrichtlinien Ihrer Internetgateways standortunabhängig auf Remote-Benutzer und Mobilgeräte zu erweitern. GlobalProtect stellt zunächst eine sichere Verbindung her und wendet anschließend die Sicherheitsrichtlinien Ihres Unternehmens an, um Benutzer vor fortschrittlichen Cyberattacken zu schützen.

VM-Series für AWS GovCloud

Für AWS GovCloud-Benutzer bietet sich die Möglichkeit, mithilfe der VM-Series Anwendungen und Daten vor Cyberattacken zu schützen. Indem GovCloud-Benutzer ihre eigenen Lizenzen verwenden (BYOL = Bring Your Own License), können sie die VM-Series in allen oben beschriebenen Anwendungsfällen nutzen. Zugriff auf die **VM-Series** erhalten Sie über Ihr AWS GovCloud-Konto.



Flexible Lizenzierungsmöglichkeiten

Die VM-Series für AWS unterstützt sowohl BYOL (Bring Your Own License) als auch nutzungsbasierte Lizenzierungsoptionen.

- **BYOL:** Alle VM-Series-Modelle sowie die zugehörigen Abonnements und Supportverträge sind über normale Palo Alto Networks-Vertriebskanäle erhältlich und werden über Ihre AWS-Verwaltungskonsole bereitgestellt.
- **Nutzungsbasierte Lizenzierung:** Sie kaufen die VM-Series im AWS Marketplace und wählen Abonnements und Premium-Supportpakete als Jahresabonnement oder auf Stundenbasis aus.
  - **Inhalt von Paket 1:** VM-300-Firewall-Lizenz, Threat Prevention-Abonnement (einschließlich IPS, AV und Malware-Schutz) sowie Premium-Support
  - **Inhalt von Paket 2:** VM-300-Firewall-Lizenz, Threat Prevention-Abonnement (einschließlich IPS, AV und Malware-Schutz), WildFire™ Threat Intelligence-Service, URL-Filterung, GlobalProtect-Abonnements und Premium-Support

4401 Great America Parkway
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com

vm-series-for-awsds-072816